Gabrielle Kaufmann-Kohler / Thomas Schultz

The Use of Information Technology in Arbitration

Information technology (IT) has invaded the legal profession. Very few are those who, today, do not work on a daily basis with electronic communication technologies. And dispute resolution is one of the most rapidly developing fields of IT usage. This special issue thus seeks to chart progress of the use of IT in offline arbitration.
This issue is not meant for specific niches of dispute resolution, but for standard procedures. In other words, it is not about online dispute resolution (ODR), but about how various IT solutions may be put to good use in traditional arbitral proceedings. Moreover, it is not meant for particularly computer-literate counsel or arbitrators, but for practitioners with a standard understanding of IT. Hence, its subject matter is centered on a discussion of the more commonplace IT solutions (e.g. e-mails, online filing, case-management websites, videoconferencing), and not of exotically sophisticated and rarely used technologies.
This issue is practice oriented, and thus includes practice guidelines and suggests standard forms for the use of IT. It also presents the services currently offered by arbitral institutions, such as NetCase, the ICC´s IT facility that has just become operational.
This work is the product of a multi-disciplinary research project carried out at Geneva University Law School and Center for Computer Science (MIRALab), financed by the Swiss National Research Fund. The text in its present form is the draft version of a book, to be published in the course of next year with Kluwer Law International. Hence, any comment or suggestion is welcome.

Index of Contents

Table of Contents

INTRODUCTION

[Rz 1] Disputes are becoming increasingly international, complex, and growingly include multiparty proceedings and mass claims, while cost constraints remain stringent and demands for speedy resolution increase. It is indeed commonplace nowadays to complain about the excessive duration and costs of the administration of justice. In the

international arena, the large majority of complex disputes, many of which include state parties, are settled by way of arbitration. One method of remedying the excessive duration and costs of arbitration is to resort to information technology (IT) tools to accelerate and facilitate the arbitration. IT tools have indeed the potential to reduce costs and time radically, and thereby maintain a necessary level of access to justice.

[Rz 2] In spite of its obvious advantages, many practitioners are reluctant to use IT in arbitration. Because arbitration is a quasi-judicial process, it must comply with procedural guarantees, which impose certain constraints on the process. In addition, in the last two decades, arbitration has evolved towards an increasingly formalistic, court-like procedure, which is often very antagonistic. Hence, parties and arbitrators fear that resorting to IT may jeopardize procedural rights and create grounds for useless procedural complications or even annulment of arbitral awards.

[Rz 3] Despite these reservations, it appears inevitable that the emergence and development of IT tools for dispute resolution will change the conduct of international commercial arbitration proceedings. The Internet has changed the way in which global commerce operates. The web has shaped business standards, time becomes increasingly shorter and delays are increasingly less tolerated. Users expect their disputes to be resolved according to the same standards as those under which they carry out the transactions giving rise to such disputes. As opposed to that, arbitration is becoming more formalistic—a manifestation of the so-called ´judicialization´ or ´legalization´ of international arbitration. This opposition may be significantly alleviated by the use of IT tools to accelerate the arbitral process, provided this is done in such a fashion that procedural guarantees are safeguarded and the quality of justice is not adversely affected.

[Rz 4] IT is indeed a very powerful toolbox for international arbitration. It may help accelerate the dispute resolution process. It may also facilitate the handling of the increasingly voluminous records that characterize present-day arbitrations. It is likely to significantly improve the administration of justice in complex, multiparty, or mass claims disputes if put to good use. IT can render arbitration more accessible, for instance making it possible for parties with less economic power to save certain costs that disadvantage them against more powerful ones.

[Rz 5] The use of IT in the arbitral process is in its infancy, but it is increasingly gathering a strong momentum. For instance, major arbitral institutions like the International Chamber of Commerce, the American Arbitration Association, and the World Intellectual Property Organization Arbitration and Mediation Center have recently launched projects offering case management websites, virtual case rooms, extranets, and other IT tools allowing multiparty communications.

[Rz 6] The present work is addressed to lawyers, not to computer scientists, nor to lawyers who are computer freaks in search of the latest trends in workflow technologies. Hence, the explanations and categories may not follow the traditional divisions used in computer science: they rather seek to present the most common technologies currently used in arbitration, addressed in a manner easily understandable to lawyers.

[Rz 7] This work addresses the following basic questions: why to use IT in arbitration? Which forms of IT (which tools or technologies) are available for use in arbitration? How should they be used? How can they be set up technically and legally? What are the main concerns related to their use, in terms of security and efficiency, but also in relation to the procedural rights of the parties?

[Rz 8] The text moves in five parts. First, it provides an introduction on standard technologies of electronic communication, reviewing their main potentials and limitations in the context of arbitration and suggesting, on this basis, a few basic recommendations. The second part is an analysis of the main legal issues that may arise in connection with the use of IT in arbitration, which relate to two areas: due process and confidentiality. Third, this work reviews the state of practice in the use of technology at the main arbitration institutions (ICC, AAA, WIPO), covering the IT services they offer and the recommendations the ICC suggests concerning IT usage in general. The fourth part presents, in analytical fashion, the two main IT tools (in addition to e-mail, which has been addressed in Part 1) that may be used in arbitration proceedings, i.e. case management websites and videoconferencing. The final part takes on a practical bent, suggesting guidelines, standard forms, and checklists for practitioners considering IT usage.

CHAPTER 1

INTRODUCTION ON INFORMATION TECHNOLOGY

[Rz 9] *Judex non calculat*, goes the saying; lawyers are not at home in mathematics. The same, unfortunately, often holds true in relation to the machines that calculate for us: computers. For many very diverse reasons, the use of information technology in the legal context is still very much below its potential. It is misunderstood, mistrusted, misused, and generally considered to be someone else´s problem—with the obvious exception of specific niches like e-commerce law and related matters.

[Rz 10] Nevertheless, technological changes have already profoundly affected legal practice. They have changed how legal information is created, how it is spread, and how it is accessed. Simple technologies like e-mail have also transformed the way people interact, and thus what people expect from each other—including what clients expect from their counsel and what parties expect from the arbitrators appointed to their case. Consequently, whatever the reason not to gain serious insight into information technology (lack of time, lack of interest, traditions, general delegation of tasks, past successes without computers, etc), most members of the legal community would be well-advised to take the necessary steps to enter the information age.

[Rz 11] Hence, this first chapter seeks to provide a global introduction on information technology, offering basic explanations and recommendations on standard technologies, their potentials, and the issues they most often raise in arbitration-related contexts. This chapter starts by telling the story of information technology, law, and dispute resolution: how they interact and how IT since the invention of computers has progressively become part and parcel of the manner in which law is practiced today (Section I). It thus provides a perspective on where we are and where we may go from here. After that, Section II suggests a list of functions IT may fulfill in relation to arbitration, i.e. the kinds of uses it may have; in other words, a conceptual categorization of the various uses of IT. Section III then takes the introduction further to pragmatic considerations, addressing the questions why, when, and how IT may be used in the context of arbitration: What are the advantages of resorting to IT? Which situations in arbitral proceedings call for such technologies? What are the golden rules in planning for the use of such tools? Section IV reviews the most common concerns in the face of relatively new technologies. Some of them are founded, while others are exaggerated and based on misunderstandings or unreasonable attitudes. All of them, however, constitute possible obstacles as they generate mistrust and must thus be understood and assessed correctly, and, where applicable, handled appropriately. Thereafter, Section V briefly presents five basic communication technologies that constitute either quantitatively important technical tools, or qualitatively significant components of more complex sets of communication systems. Finally, Section VI provides an analysis of a series of issues related to what still constitutes the main communication technology on the Internet: e-mail.

I. The story of information technology, law, and dispute resolution

[Rz 12] Computers, since their early development after World War II following Alan Turing´s work, have gradually changed the way we approach law, the way we practice it, the way we do business and, at the crossroad of these trends, computers have begun to change the way we resolve disputes. Setting up arbitration procedures that rely heavily on (IT) is in this regard not a spontaneous innovation, but merely a logical next step in the history of how computers penetrate the law. It simply follows the movement started some 20 years ago with the arrival of computers in offices.

[Rz 13] Consequently, before turning to a pragmatic approach of the use of IT in arbitration, a perspective that will be kept for most of this work, some considerations on the origin and development of the role of information technology in law and dispute resolution are in order. Such considerations may help understand the past failures and achievements of IT in arbitration, i.e. the lessons that can be drawn from its evolution, its current capabilities, the variety of its potential uses and objectives, as well the likely directions it may take in the future. The developments discussed below have shaped the context of the use of IT in arbitration.

[Rz 14] Beyond mere text editing, chronologically, research first focused on a general analysis of the effects computers have on the law: it inquired how independent or unconnected computers changed our relationship to legal

materials. The main topics of research, at the time, were information management and artificial intelligence. These topics, which are still the subject of much development in theory and practice, do not deserve a more detailed analysis here, as they do not relate to the subject matter of the present work beyond a chronological connection.

[Rz 15] The second relationship between information technology and the law that became the subject of interest dealt with the effects of networked computers, and in particular the Internet, on the circulation of information. IT caused legal information to flow differently, the most obvious example being online legal databases such as Lexis or WestLaw. This largely unrestrained, instantaneous, and global movement of information is of course not restricted to legal information, with the consequence that the Internet is often considered to be one of the main driving factors of economic globalization.[1] This form of globalization in turn increased the globalization of the law (e.g. the harmonization of legal regimes and extra-territorial effects) and of dispute resolution processes. Online dispute resolution (ODR) probably the epitome of a globalized dispute resolution process, is itself a product of computers and networks.[2]

[Rz 16] ODR represents the third main relationship between IT and the law. In fact, it probably embodies the heaviest reliance of legal processes on IT. The main advantage of ODR is the ease of its access, which is ubiquitous, and consequently the relatively low costs generated by the procedures. However, an important finding in the ODR field is that it is almost exclusively usable for small and medium size disputes raising factually simple issues. Large international disputes are still solved essentially by offline processes of dispute resolution. More precisely, the evolution of the ODR movement has gone through a series of phases that testify to the importance of the approach chosen for the present work; promoting the use of information technology in traditional arbitration procedures is a simple extension of the ODR movement.

[Rz 17] The first reason for the ODR movement was the lack of confidence that characterizes e-commerce. Internet shoppers are in need of a dispute resolution system that relies on the same communication means that were used to conclude the transaction in the first place: electronic means of communication. The electronic accessibility of the procedures allows these consumers to constitute points of reference, landmarks of justice in cyberspace: they may return to the place where the transaction was concluded—and thus where the dispute arose—and find a link to a dispute resolution process specifically adapted to their dispute.[3]

[Rz 18] After this first impulse, which corresponded (and still does) to a concern of consumer protection, it was soon realized that the advantages of ODR could be used to facilitate—and sometimes actually permit—access to justice not only for e-commerce disputes, but also for all small disputes, especially when they involve rather large distances between the parties, or even different countries of residence. It was then clearly recognized that ODR is not merely a by-product of e-commerce, or even a set of tools that belongs to the broader field of cyberspace law, but a change with potentially profound implications for the entire field of dispute resolution. Indeed, electronic communications means, and information technology in general, if used correctly, facilitate almost any form of resolution of almost any dispute. IT, if used correctly, improves the effectiveness of dispute resolution processes by simplifying information transmission and generally accelerating the proceedings. IT also improves efficiency, i.e. it reduces the costs of dispute resolution processes, in particular by limiting the need for travel.

[Rz 19] The fourth—and probably the most important—relationship between information technology and the law was also triggered by the ODR movement: this time, the focus was on the effects which IT can have on the work of mediators and negotiators. It all started during the final period of the war in Yugoslavia. As the difficult negotiations between Bosnian Serb, Croat, and Muslim ethnic factions seemed to have stalled, the United States brought in a clever and innovative IT solution to help the negotiators and the mediator reach an agreement[4]. They simply gathered the different factions around a digital map of the territories at stake in the negotiations. This very detailed map was interactive, thereby allowing the negotiators to work with realistic and graspable analyses of construction feasibility, minefield clearance operations, and boundary marking. Other typical examples are computer-assisted negotiation systems from afar, where the computer automatically carries out some of the tasks a human third party would usually have to do—such as sending reminders, proposing action plans, and suggesting standard settlement terms.[5] Drawing on this example, Ethan Katsh and Janet Rifkin cast the concept of the «fourth party», [6] which stands for

> «something that is an influence on the process of communication and negotiation, something that adds value to

> the third party [i.e. the mediator or the arbitrator], something that typically does not replace the third party but can displace her, in the sense that the third party operates with an ally or assistant alongside».[7]

[Rz 20] This fourth party further takes the form of «applications that enhance the expertise of the third party and thus do more than simply deliver the expertise of the human third party across the network».[8] In other words, the third party, be it the mediator or the arbitrator, is there to help the parties solve their dispute[9] and the fourth party does exactly the same: it is not only an ally to the *third party*, but also an assistant–next to the third party–to the two *disputing parties*.

[Rz 21] The technology that the fourth party represents is globally developing along two main lines.[10] First, very simple tools are being developed, such as red flags, emoticons, images or sounds whose goal may be compared to that of pens and flipcharts in traditional offline dispute resolution methods, i.e. to help clearly convey a message or to attract attention. Such tools also serve other, though similar functions by virtue of their automation: e.g., they may help automatically remind participants of deadlines.[11] On the other hand, very complex and sophisticated technological tools and platforms are being experimented with and sometimes implemented. This use of high technology aims at a much more intense exploitation of the tools that electronic communication technology offers. Virtual workspaces are one example–and in many respects an extreme one–of such complex and sophisticated tools.[12] In between these two extremes of simplicity and complexity, a whole range of technologies exist, the best known being extranets and virtual case-rooms, case management websites, and videoconferencing. At this stage, it must be remembered that the fourth party is not limited to ODR nor to processes that take places essentially online;[13] it can also be used in all types of dispute resolution processes.[14] Much of the experience gathered in ODR is actually being exploited in the context of offline arbitration.

[Rz 22] The fifth and last relationship between information technology and the law, which follows from all the above, is the effects IT can have on arbitration procedures. The most prestigious arbitration institutions are currently experimenting with IT tools: the International Chamber of Commerce (ICC) with its NetCase program,[15] the American Arbitration Association (AAA) with its WebFile scheme,[16] and the World Intellectual Property Organization (WIPO) with EFAC.[17] Private ventures are developing hardware and software and trying to sell them to the arbitration world,[18] not to mention the various online arbitration programs developed by the Chartered Institute of Arbitrators. Legal commentators have also started to embrace this topic.[19]

[Rz 23] In summary, the idea of using IT in arbitration is a burgeoning theme, which follows from experiments related to global electronic information management, the circulation of information in an increasingly globalized and borderless world, the online dispute resolution movement (which more precisely led to lessons regarding procedural setups and techniques of dispute resolution using IT), the idea that IT may displace or on some occasions even replace the neutral third party in dispute resolution, and the gradual introduction of IT tools into everyday business and legal practice. As the use of IT in arbitration is clearly in its early stages of development, the present book will first offer a comprehensive presentation of the IT tools that may be used in arbitration. Thereafter, these technologies will be submitted to legal analyses, both global and specific, and some possible future technologies will be mentioned.

II. Functions of IT for arbitration

[Rz 24] In its most comprehensive sense, information technology encompasses any use one can make of computers, because every time one uses a computer, one handles information through technology. Hence, speaking of «the use of IT in arbitration» may in fact cover a large variety of radically different actions, which collectively cover–and go beyond–the daily work of most lawyers. Such recourse to technology ranges from the use of handheld devices (such as personal digital assistants or smart phones), to simple word processing, online legal research, billing software, shared calendaring, automated interest calculation, automated conflict of interest checking, e-mailing, videoconferencing, and more exotic technologies like 3D virtual reality.

[Rz 25] Obviously, it is not the purpose of the present book to comment on all these IT uses; this is not a treaty on legal software. Instead, the focus will be on issues that involve data transmission, i.e. electronic communication means that can be used in the context of arbitral procedures. Individual data management, i.e. situations in which

data is handled but not transmitted over electronic networks, will in principle be left aside, except for occasional examples, illustrations, or explanations.

[Rz 26] Nevertheless, in this section´s context of a general introduction to IT in arbitration, it seems worthwhile to briefly list the main purposes of technology in this field. On some occasions, the tools which are further analyzed in this publication are indeed mere extensions of more traditional technologies (such as document management or digital presentations) to collaborative electronic environments or more generally to situations where data is transmitted (e.g. case management websites or digital presentations during videoconferences). Hence, a brief overview of the variety of uses of IT in arbitration may help understand the general technological environment in which the more advanced tools are being developed.

[Rz 27] The following list provides a general overview of some of the basic types of IT use in arbitration; most other IT functions (legal research aside) are derivatives or combinations of these uses:

- *Transmitting messages and files*: one of the most obvious uses of information technology—beyond text editing—is the transmission of messages and documents using electronic networks. Usual technologies for this purpose are e-mails and web-based means such as web interfaces and bulletin boards.

- *Meeting from afar*: a thin line separates the idea of transmitting messages and files, which can be considered to take place in asynchronous fashion, from something closer to an actual meeting online. Such meetings are based on technologies such as chat rooms and videoconferences, which imply synchronous communications.

- *Handling documents*: documents can be handled (in the sense that their content is interacted with) using IT with some notable benefits. For instance, the ability to rapidly search for occurrences of specific words largely increases access to the information contained in a document (and may consequently increase the probability that the point gets through to the recipient). The possibility of copying and pasting entire sections of documents is another obvious and often-used advantage. In addition, documents can be linked to each other through hyperlinks.

- *Creating documents*: IT facilitates the production of new documents. As suggested above, tools like «copy-paste» accelerate the process of production. Typically, in the context of arbitration, the drafting of an award involves many instances of «copy-pastes» from the parties´ briefs and from documentary evidence. Moreover, IT has generated a new way of producing documents, since it is no longer uncommon that people in different parts of the world collaborate in the drafting of documents.

- *Managing documents*: using documents in electronic form facilitates their management (in the sense that they are interacted with as files, i.e. as information containers), for instance because their storage is facilitated, and searching and finding a document can be significantly accelerated if the naming of the files follows a clear policy.

- *Managing cases*: information technology can also be used to improve the management of cases, for instance by using progress tracking software, which for instance shows at which stage a given case is, what the next expected actions are, and when the deadline is. It may also graphically show the relationships between the various actors of the case.

- *Visually presenting arguments and facts*: IT solutions such as digital slideshows, video depositions and video presentations are increasingly being used during arbitral hearings, because visual presentations, and especially graphic ones, are more memorable and clearer than purely oral presentations.

- *Tracking*: IT has, to put it simply, an amazing memory. IT has given us the possibility to track everything that occurs on our (virtual) desktop and, with the collaboration of others, on their desktops. IT may indeed be used to record and store not only documents, but also presentations, oral statements, and videoconferencing exchanges. The advantage (and sometimes the danger) of this is that such data can be reproduced by anyone gaining access to it with perfect accuracy and at any time.

III. Why, when, and how

[Rz 28] The previous section discussed the main functions that IT may fulfill and their purposes. We will now turn to a review of the general advantages of resorting to such technologies, i.e. how they can advance legal practice, in which actual situations such functions may be usefully fulfilled by IT, and the ways in which such tools should be used.

1. What can IT do for arbitration?

[Rz 29] The purposes of using IT in work environments are fundamentally always the same, regardless of the context in which it is used. Such technologies allow tasks to be accomplished more rapidly, cheaper, and more easily. In other words, they seek to render work processes more effective, more efficient, and more convenient. The question here is how IT can achieve these properties in the context of arbitration. The answer to this question forms the substance of the following paragraphs. It should be specified that the present section only provides a general introduction of the advantages IT can offer for arbitration; the respective advantages (and disadvantages) of specific tools or technologies will be addressed in Chapter IV.

A. Efficiency

[Rz 30] The most obvious and acclaimed reason why IT should be used in arbitration is that it provides opportunities to reduce costs and time. The main types of costs that can be reduced relate to travel and document handling.

[Rz 31] Travel costs can of course only be reduced in the context of online meetings replacing face-to-face meetings, which is currently not very frequent. IT can provide significant cost savings in such situations. In addition to out of pocket expenses, the costs savings also include lost working time (including productivity diminution due to jetlag). Moreover, the travel-related costs of all the participants in the arbitration can be avoided, including those of arbitrators, parties and their counsel, witnesses and experts.

[Rz 32] Document handling also generates costs that can be reduced by resorting to IT:

- Document reproduction: as opposed to photocopies, digital copies cost virtually nothing. This is especially beneficial for larger cases with numerous lengthy documents.
- Document storage: digital copies of documents reduce the need for storage space, as a standard CD or DVD can contain thousands of files.
- Document shipment: transmitting files in electronic format, whether by e-mail or stored on a CD or DVD, rather than sending by mail or special courier (if not small van loads) of printed material around the globe can save significant courier costs.

[Rz 33] In terms of time saving, IT-related benefits may concern the following areas:

- Time for realization of tasks: specific tasks, such as hearings and other forms of meetings, but also transferring documents, can be undertaken more rapidly when appropriate technologies are used. Such technologies are for instance simple electronic communication means like e-mails for a limited number of relatively small files; more sophisticated tools such as case management websites with powerful *en masse* uploading and downloading facilities for larger or more numerous files; videoconferencing for hearings and other meetings such as deliberations.

- Time between tasks: IT may also save time in between specific tasks, in the sense that if travel or shipping times can be reduced or suppressed entirely, more tasks can be carried out in a shorter time space and it also becomes easier for all participants to find common available periods. Consequently, the procedure will be accelerated. The same holds true for the waiting periods due to shipping, whose suppression allows more seamless workflows, thereby increasing productivity and potentially shortening procedures.

B. Effectiveness

[Rz 34] In addition to such effects of acceleration of the proceedings, costs reduction and productivity gains of the various people involved in an arbitration, IT may also make certain aspects of an arbitral procedure more effective, in the sense that tasks can be undertaken—or goals can be reached—in a way that may not have been practicable without IT. For instance, in the absence of IT availability, costs and time constraints may lead to renouncing certain actions, like hearing a witness or experts who may not be quickly available, especially in fast-track procedures. This is for instance the reason why witnesses and experts were heard using videoconferences during arbitrations at the Olympics, where time constraints would have prevented their testimony if they had had to be physically present. [20]

[Rz 35] In other less radical situations, IT may increase the quality of some actions: for instance, videoconferencing allows a richer information transfer as it conveys a more detailed message than teleconferencing, and research in the field of online dispute resolution has shown that, in general, richer communications have a higher potential to lead to satisfactory results.[21]

[Rz 36] In this sense, videoconferencing should not be compared with face-to-face meetings, but rather with teleconferencing. The sense of reality conveyed by videoconferencing is midway between teleconferencing and face-to-face meetings and it may thus replace teleconferencing with advantages related to the quality of the discussion and, on those occasions where the level of details of the discussion does not matter so much, it may replace face-to-face meetings (a question of effectiveness) with advantages related to speed and costs (a matter of efficiency).

C. Convenience

[Rz 37] Finally, IT may facilitate certain actions related to arbitral procedures in a way that does not concern speed, costs, or the quality of certain tasks, but that simply makes some processes more convenient. For instance, electronic documents can be searched easily using the «find» function available in all word processors. It should be noted, though, that this obviously requires the documents to be in a format where the text is recognized as such, which notably excludes documents that are scanned (for instance in pdf format) without recourse to a text recognition function and a subsequent check of the recognized text. (Although scanning briefs in image format for subsequent transmission to other participants in an arbitration obviously makes little sense, it is not unheard of.)

[Rz 38] Other advantages on the front of convenience that were already mentioned above, are for instance the possibility of archiving documents easily and the ability to carry an enormous amount of files to a hearing without any consideration of their physical weight.

2. Situations

[Rz 39] Having considered the various uses of IT for arbitration and their different advantages, it remains to be seen in which specific situations these benefits may be put to use. Obviously, a detailed answer to this question would depend on the specific IT tool one considers. This is not the purpose of the present section, which merely serves as an introduction on information technology in arbitration. Consequently, the following lists general considerations regarding the situations in which a rather heavy reliance on IT may be of particular interest. Indeed, the lists provided above on the various ways in which IT can be used and which general advantages it may have if used correctly shows that *some* recourse to *some form* of IT appears useful in almost any situation. However, in certain specific cases, the benefits of using IT are particularly clear. The following paragraph focus on those cases to illustrate the main factors that should trigger a particular interest in the use of IT.

[Rz 40] *Time-driven procedures* are the most obvious cases in which IT may be of particular interest. In such situations, time often becomes paramount and any solution that contributes to accelerating the procedure without creating a serious reduction of the quality of the procedure appears useful. More precisely, such situations could include:

- Hearings before provisional measures;

- Fast-track arbitrations, the epitome of which may be the Olympics arbitration scheme administered by the ad hoc Division of the Court of Arbitration for Sports, where awards are rendered within 24 hours from filing. In such situations, hearing witnesses or experts is often impossible without resorting to videoconferencing, which is precisely the solution adopted by the ad hoc Division.

[Rz 41] *Low cost procedures* constitute the second most obvious situation in which IT may provide particularly useful advantages. The cost reductions relate to shipping and travel costs, but also to a form of automation (e.g. case intake) or standardization (procedure streamlined by setup of communication platform) of certain stages of the process.

- Consumer dispute resolution is the most notorious example of such a situation. The cost-saving potential of resorting to IT was in fact one of the main factors of development of the ODR movement in the first place (although, as the ODR experience has shown, the development costs may be quite high; it is the marginal costs related to the use of the system that are low).

- All disputes where cost constraints are a major consideration may in fact benefit from such cost savings through IT.

[Rz 42] *Short meetings of secondary importance*. IT may be used to replace face-to-face meetings in situations where the sense of reality and the ability to feel each other´s state of mind is not of utmost importance. Such replacement of face-to-face meetings may be achieved, depending on the actual situation and the desired level of presence, by videoconferencing, chat rooms, or bulletin boards.

[Rz 43] *Mass claims*. If the number of claimants is high, technology may be particularly useful in helping to simplify the process. This may for instance be achieved by streamlining the submission phase using electronic forms, as was done in the context of the Iraq compensation program or UNCC.[22] SquareTrade´s online assisted negotiation and online mediation program, which is primarily used for eBay disputes, is another good example, as SquareTrade resolves some 800´000–1´000´000 disputes a year and its intake and first steps of resolution are entirely automated using interactive electronic forms. IT may also play an important role in class actions which in the US are now more and more brought to arbitration.

[Rz 44] *Multiparty disputes.* Similarly, the more numerous the participants in an arbitration, the more benefits may be reaped from the use of IT. Indeed, it makes almost no difference whether one or a very large number of copies are made of a file in electronic format, and its distribution takes roughly the same amount of time whether the file is addressed to one or many recipients[23]. The use of a case-management website for the multiparty arbitrations of the Americas Cup, i.e. ACJ ECAF under the auspices of WIPO, is a good illustration.[24]

3. Two golden rules

[Rz 45] For many people, information technologies and computers in general still have some sort of magical appeal, and are considered to be different in nature than mere pen and paper. They are sometimes viewed as something that, if mastered, may provide their bearer with some kind of special power. Hence, they are treated differently than traditional work tools, in the sense that some believe, often unconsciously, that the more IT, the better, and the more important the situation, the more «powerful» the technology should be. This attitude leads to two misuses that may totally defeat the purpose of IT: general over-use and recourse to technology as if it were a trump card to be played in particularly important situations only. These two misuses call for two fundamental recommendations: do not over do it, and master it before using it.

A. Do not overdo it

[Rz 46] The basic rule governing all uses of IT, in all situations, is that technology is not a goal in itself and should only be resorted to if it improves the process for which it is used, for instance because it makes the process more effective (the quality of the outcome is improved) or more efficient (a comparable outcome is reached but at a lower

cost or in less time).

[Rz 47] It follows that «e-everything» should be avoided; at least it should never be a goal in and of itself. Moreover, increased technological complexity on the end-user side requires exponentially increased time to familiarize oneself with the technology and its integration into one´s work habits. In other words, one should never underestimate the price one pays when decreasing user-friendliness in exchange for enhanced technological capabilities.

[Rz 48] The KISS principle («keep it simple and stupid») may be an exaggerated reaction to this issue, but it has the advantage of clearly expressing the intuitive rule that investments in terms of time, money, and effort in new software or hardware will only be made reluctantly by the vast majority of people. This is particularly true of professionals with well-developed working habits and time restrictions, which is in principle the case of arbitrators and counsel in arbitration.

B. First master it, then use it

[Rz 49] It often happens, not just in relation to the use of information technology but in life generally, than we have in mind some innovative solution or technique, thought to be extraordinary or at least particularly impressive, but have never had the time to try it out. Then, one day we are faced with a particularly important event and, keen to impress, decide the time has come for using our «secret weapon». Thus, people try new ways of making a presentation at a major conference, a new rhetoric during a crucial discussion, or new tricks thought to be particularly shrewd during a critical negotiation, and often fail quite spectacularly because they are in fact mere beginners at these new, previously untested solutions or techniques.

[Rz 50] Why we have a tendency to do this may only be guessed— probably some sort of mix between an intuition that we are not up to the task and a form of organization that makes us believe that only urgent matters are really important, thereby repeatedly postponing tasks that do not have an immediate result, and all this combined with the general tension generated by the importance of the occasion. The fact is that many people do indeed use techniques before having taken the time to master them.

[Rz 51] The use of IT is no exception. For instance, lawyers soon having a major case seek to use some relatively complex IT solution without having the time to try the system—to *play* with it, really—before this major occasion. The result would hardly be a frank and easy success.

[Rz 52] Hence, the second golden rule in relation to the use of IT may be said to be the following: do not try new tools when things are getting serious or, in other words, in an important situation, master an IT solution before using it!

IV. The most common concerns related to the use of IT

[Rz 53] Most lawyers, when advised to implement some IT solution in their practice, voice the same concerns: first, electronic communications create a particularly important risk of security breaches; second, technology is unreliable and usually breaks down at the most inconvenient time; third, faking identities is relatively easy on the Internet and consequently it may be difficult to trust the authenticity of a message; and fourth, professionals have their working habits and are afraid that changing them to adapt to IT may decrease their productivity.

1. Security

[Rz 54] Here is an example of the typical attitude of a lawyer towards technology. Many law schools are equipped with shared printers, which are located in rooms that are oftentimes not locked and thus easily accessible to students. Some professors, when preparing their exams with the help of their assistants, insist on the fact that the exams are not sent by e-mail among them, fearing that students might intercept the message; rather, the files are transmitted on floppy disks or USB-drives. But then, sometimes, the draft exams are printed out and left sitting on the shared printers for several hours, free to be picked up by students.

[Rz 55] Here is another such example. Some law firms forbid their practitioners to save any file on their desk computers or on the local server, suggesting instead that they use the firm´s virtual private network, i.e. an encrypted remote computer network, for fear of hackers intruding into one of the local computers or servers. Hacking into the firm´s files on this network would indeed be truly difficult. But most practitioners need to take files with them, to work on at home or while traveling. On such occasions, it is not infrequent for a lawyer to download all the files pertaining to a case onto a laptop, which is usually not access-protected, and is sometimes even left in a gym locker, beneath a chair in a bar, or in a car in a public parking lot, all places where thefts are common.

[Rz 56] Here is a third example, which does not relate specifically to lawyers: many reports on consumer behavior on the Net show that one of the greatest concern of online consumers is a misuse of their credit card number—this is even one of the current main obstacles to the development of e-commerce. But in the offline world, people give their credit card numbers away all the time in totally unprotected situations (in restaurants, for instance) without a second thought.

[Rz 57] In sum, most people are more concerned about security in «cyberspace» than in the «real world». Some reasons account for that. On the one hand, most people are confused by the apparent complexity of computers, which are thereby associated with the sense of lacking control. On the other hand, common knowledge about computer security is much lower than the general understanding of security in the «real world», because concerns relating to the latter have been around for much longer. In addition, this lack of knowledge and this sense of lacking control are fueled by two more factors. First, hacking is a feat—the hackers´ own word for successful security breaches is actually «exploit»—while breaking into a house or stealing a laptop in a parking lot is trivial. News items and movies featuring hacking exploits fuel the idea that electronic communications, but also electronic data storage, are fundamentally insecure. Second, the Internet security industry has become one of the most successful IT-related sectors, making it economically important for Internet users´ security concerns to remain.

[Rz 58] Concretely, such security concerns relate to two main aspects: the transmission of information (interception) and its storage (intrusion).

A. Interception of e-mails

[Rz 59] It is often considered that a standard, unencrypted e-mail is no more secure than a postcard. This is technically correct, as all those who have the e-mail in their «hands» are in principle be able to read its contents. It should not, however, be misunderstood to mean that anyone could intercept any e-mail communication. This would be exaggerated to the point of being wrong, although it is what many people believe. The reality is that an e-mail can basically only be intercepted at two points.

[Rz 60] The first such point is the nodes through which an e-mail transits. All e-mails that are not purely internal to a corporate network travel through a relatively high number of nodes, i.e. servers, systems, and network devices, which all constitute possible points of interception. Some of these nodes, but not all, are indicated in the header of each e-mail—more precisely in the full version of the header, as most e-mail programs hide this information by default for convenience. Roughly simplified, these nodes play a role equivalent to mailmen and all other persons handling mail in the postal system. An unencrypted e-mail passing through these nodes is similar to a postcard going through the postal system: for everyone having access to one of these nodes, an e-mail is as easily readable as a postcard, using a simple technique called packet sniffing.

[Rz 61] The question that arises then is whether these persons are interested in actually taking advantage of their ability to intercept your e-mail. To answer it, one should first think about what these nodes actually consist of. There are four main types of nodes:

- Internet Service Providers (ISP): the entity providing access to the Internet (and related services such as domain name registration and hosting) has particularly easy access to the information that travels through its system. There was indeed a case in 1999, largely reported in newspapers at the time, of a San Francisco ISP that intercepted e-mails of one of its customers, namely Amazon.com, and transmitted them to a competitor.

- E-mail providers: traditionally, most people´s e-mail address is provided by their ISP, but with the growing number of e-mail addresses each person uses and the development of attractive substitute e-mail providers, this tends to be less true. This offers a new point of interception, as e-mail providers have access to the data that transits through their systems as ISPs do.

- Corporate networks and backbones: e-mails sent from an office travel across the corporate network and backbones. Sometimes the corporate network itself plays the role of an ISP, but not necessarily. If it does not, the e-mail goes first through the office network and then through the servers of the ISP. In any event, a message may be intercepted within the corporate network by system administrators and security officers, for example, but also by other employees who manage to break into the system. Depending on the security measures implemented by the system administrators, it may even be very easy to «break» into the system and sometimes it is sufficient to run a simple program, called a packet sniffer, on one´s own computer to intercept e-mail traffic. It may be added that hotel or conference center networks, or the systems of an Internet café, are generally even less secure than a corporate network.

- Local loop: most Internet traffic travels through a shared physical set of wires, also used for telephone services and possibly cable television. Such wires may be tapped, though such an action becomes obviously much more complicated than e-mail snooping at one of the other nodes mentioned above.

[Rz 62] As to the likelihood that e-mail interception indeed occurs, in principle most of these nodes are commercial enterprises that have a strong interest in respecting the privacy of the e-mails that transit through their system. Corporate networks also have a strong incentive not to interfere in communications. Nevertheless, renegade employees may for instance act in retaliation against their employer—such actions have occurred in the past. In addition, most governments now have the capabilities to intervene at one of these nodes, and it has happened many times that the «cyberpolice» in repressive countries have arrested political dissidents on the basis of an intercepted e-mail. If these capabilities are considered in light of the fact that governments sometimes go as far as kidnapping arbitrators in order to influence the outcome of an arbitration procedure, it becomes sensible to consider security measures when e-mails are sent to and from problematic countries.

[Rz 63] The second possible point of interception of an e-mail is the sender and recipient´s computers. Interception can be either manual (by far the most frequent occurrence) or by way of software. Manual intrusion requires stealing a login and password in order to log into the computer´s usual resources (e-mail server, shared disk), either from afar or by physically breaking into the room containing the computer and finding, for instance, a post-it under the keyboard or in a drawer with the login and password. Intrusion by software consists in installing bugging software (called spyware) on the targeted computer, which typically records and transmits all or specific keystrokes. Such installation can be achieved by two ways: either by physically sitting in front of the computer in question and, using a disk or USB-drive, copying the bugging software onto the computer´s hard disk, or by electronically transmitting the bugging software (e.g. as an e-mail attachment), which then installs itself on the targeted computer. As a confirmation of the ease of breaking into the sender and recipient´s computer, a team of researchers from the University of California, Berkeley, recently showed how a ten-dollar piece of electronic equipment could be used to sniff out any form of data entry using a keyboard, simply by recording the sounds keystrokes make. [25]

[Rz 64] In sum, there certainly are security threats, but it seems rather clear that the likelihood of e-mail interception is rather low, comparable to the risk of interception of paper correspondence. In this context, one should recall that no correspondence is perfectly secure, not even in the real world and that it therefore seems unreasonable to worry excessively about the security of electronic communications. In other words, the foregoing paragraphs are not meant to increase the security paranoia that often exists in relation to electronic environments, but merely to explain where the main risks arise. These main risks, identified above, call for the following three types of security measures.

1) The most basic and obvious set of measures is the implementation of the same security solutions as those used for physical documents. Concretely, this means protecting the physical access to one´s personal computer, which should be considered to be an inherently confidential object.

2) Standard computer user safety recommendations provide a second set of measures to reduce security risks. Such recommendations for instance include:

- not to open any e-mail attachment if the sender is unknown, because this may launch an application installing spyware or a virus;
- to ensure that all computers one uses are equipped with high quality and up-to-date anti-virus and anti-spyware tools;
- if possible to avoid using software products that have a high number of known security loopholes or that are targeted by virus and spyware producers, such as Microsoft applications, as the vast majority of spyware and viruses are designed to take advantage of Microsoft security loopholes, due in part to anti-Microsoft behaviour, frequent among virus and spyware writers;
- dedicate professional computers exclusively to professional use, as deceptive applications are often downloaded in the context of peer-to-peer file swapping or while visiting not strictly professional websites;
- all these recommendations only truly make sense if they are followed by all the users of a specific computer, which leads to the additional recommendation to strictly monitor access to the computer in question. Do your children, for instance, sometimes use one of the computers you also use for work? This computer may be the floodgate to infecting your other computers as you transfer files from this computer to them.

3) If more security is desired, one may resort to the following technologies:

- protect documents with password-restricted access: many word processors provide a function allowing the encryption of a document and password-restricted access to it. A document can then be sent without concerns for security, regardless of the transmission channel. The password is then conveyed separately over another channel, which is considered more secure (telephone, fax, registered letter, etc.). In Microsoft Word, for instance, this function is turned on at «file / tools / general options». PDF documents can also by password-protected, for instance using Adobe Acrobat Professional, which features a command «document / protection», which offers many document protection functions. Other PDF editors, some of which are available for free (e.g. PDFCreator), achieve a very similar result;
- use encrypted e-mails, which may be acquired quite easily and installed for free.[26]

B. Interception of web-based transmissions: protection through SSL

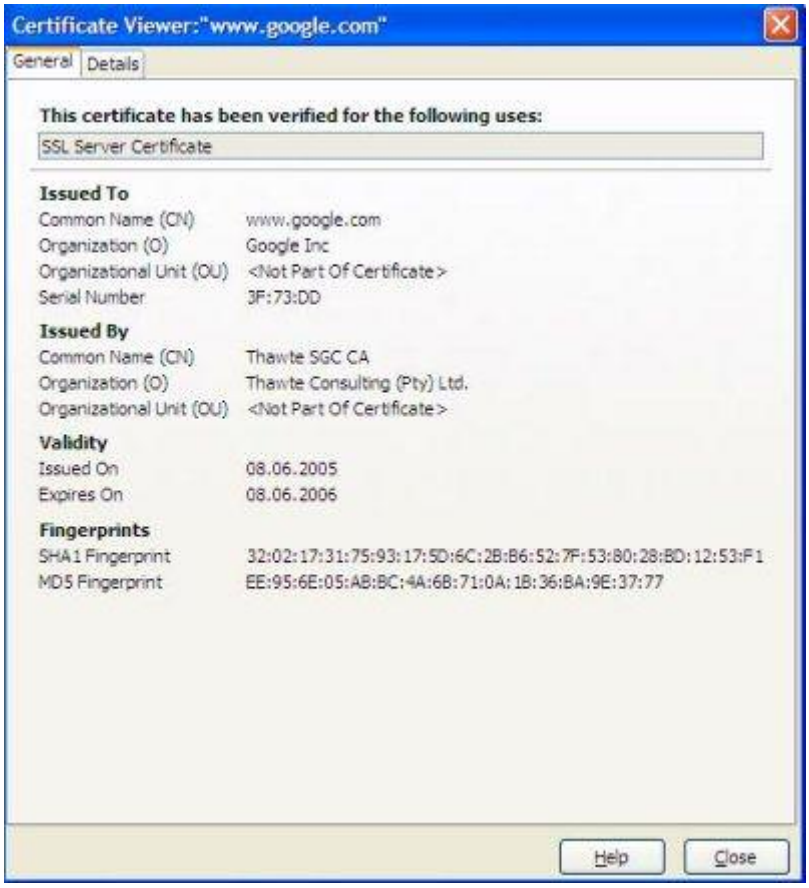
[Rz 65] Secure Sockets Layer (SSL), introduced in 1994, is the main protocol used to encrypt, and thus protect from interception, communications over the Internet between a server and a user. The most typical situation for which it is used is the submission of confidential information by the user in the context of Internet browsing. In this case, SSL is used with the standard web-browsing protocol called the HyperText Transmission Protocol (HTTP) to form HTTPS, the more complete protocol used to secure web pages for applications such as e-commerce when data such as credit card numbers is submitted. One may recognize a secure web page by the fact that its address begins with «https» instead of «http» and that a padlock icon is displayed at the bottom of the page.

[Rz 66] When a web page is SSL-secure, this means that the user´s browser will encrypt the data (resorting to encryption of up to 256-bit, which is currently considered to be unbreakable) using a code provided by the server

(called a public key). It is, in other words, incumbent upon website builders to provide for such security measures. The user cannot do much but verify that no sensitive information is transmitted to a website whose address does not begin with «https».

[Rz 67] Other instances of use are interactions between an e-mail program and the server it is using (the retrieval and sending of e-mails is secure between the user´s computer and the e-mail server), file uploading and downloading from distant servers, or creating a Virtual Private Network (VPN), which is a private and secure communications network built into the public network that is the Internet.

[Rz 68] In addition to securing communications with a server to prevent eavesdropping, SSL also authenticates the website to which one submits information, or more precisely the server of the website. This authentication allows preventing fake websites from easily harvesting confidential information that a trusting user would submit. This authentication takes the form of an SSL certificate, which can be viewed by double-clicking on the padlock displayed at the bottom of the browser´s window. Such a certificate looks like this:



[Rz 69] When a certificate authenticates a website, it proves that the site belongs to whom it says it belongs. For this purpose, the certificate contains information about the certificate holder (Google Inc in the example above), the certificate issuer (Thawte in the instance above), and the certificate itself, in relation to the periods of its validity for instance.

[Rz 70] Most certificates are issued by trusted third parties and must be paid for. However, it is also possible to create one´s own certificate and to «self-sign» it. Such a self-signed SSL certificate provides the same technical protection against interception, i.e. it encrypts the communications in the same way as a third-party certificate would do. Of course, it does not authenticate the website in a trustworthy manner. In most browsers, self-signed certificates trigger a warning message indicating that the certificate was not recognized, but most people are not stopped by such a message, just as they are not stopped by a window warning that a third-party certificate has expired. Self-signed certificates are sometimes used for websites that are essentially for Internet traffic within a corporation, for instance for the site of a company´s webmail.

C. Protection against intrusion into data storage systems and other applications

[Rz 71] The protection against intrusion into data storage systems and other applications is in principle a matter for professional system administrators. The diversity of hacking strategies and security mechanisms that have been developed in response to them is too great and changes too quickly for us to present here. Nevertheless, it may be useful to briefly point out the three basic technical properties that are used to secure access to systems and applications: authentication, authorization, and accounting.

- *Authentication* is in essence the process by which a user provides information that is in principle only available to him to identify himself to the system. The most common authentication mechanism on the Internet today is simply to log into a system using a username and password. Under some circumstances however, passwords may be stolen as they are transmitted across networks, and badly chosen passwords can be guessed. There are other stronger authentication systems that resort to certificates, which cannot be guessed, and encryption, which prevents interception. In addition, biometric authentication systems, relying on fingerprint or retina scans, are increasingly being used as their prices have decreased to a few hundred euros. [27]

- *Authorization* is the process that follows authentication, i.e. it relates to granting access to a user who has been authenticated. More precisely, the authentication phase leads to granting specific privileges to specific users–everyone does not have the same access rights. In principle, an IT system is organized so as to attribute predetermined roles to specific users in relation to particular resources.

- *Accounting* (also called «logging») is the process of monitoring and tracking the operations of a given system and the behavior of the users of such systems. Such processes are used, for instance, to verify if someone is trying to break into a system or to misuse it. Accounting can for instance reveal unusual usage patterns, which may indicate that a password was stolen, that attackers have found vulnerability in a system, or that a previously well-behaved user (for instance an employee who has just learnt that he/she was laid off) has had a change of heart. Hence, an essential component of a secure application is a thorough monitoring and tracking mechanism, one that automatically provides detailed information about the following elements: (1) attempts to compromise the security of the system (for example attempts to log in by guessing passwords); (2) successful intrusions by hackers, misuse and abuse of the system by legitimate users or cheaters; and, if possible, (3) an automated check of the log files and automated reporting of suspicious activities. For users who are not professionals but would like to take some security measures themselves, an accessible way is to acquire intrusion detection software such as Tripwire.[28] Such systems monitor changes in the software installed on a server and set off an alarm if it is being tampered with.

D. Getting infected

[Rz 72] One of the major preoccupations when using IT relates to security against system violations that can disrupt the system or provide information about the user or the user´s system. Such IT security threats can take several forms.

a. Viruses

[Rz 73] A virus is a program that infects a computer. It is well known that viruses are the source of major problems and can cause huge financial losses. A virus can affect a computer in different ways such as removing files, altering its content, reconfiguring the system, displaying a graphic content, or overwhelming a system.

[Rz 74] A virus has the ability to copy itself into a system without being asked to do so. There are different ways of doing so, since viruses can be contained in an executable file or be transmitted by e-mail. Nowadays the most common and dangerous types of virus are the mass mailing viruses that access a user´s address book and e-mail themselves to the contacts contained in it using the same e-mail system, thus causing recipients to believe that the e-mail is safe. Viruses can be activated in different ways, just by executing the application or automatically on a certain date or with a certain event.

[Rz 75] Based on the previous considerations, one should be reticent to execute any file the origin or name of which

is suspicious.

b. Macro Virus

[Rz 76] Macro viruses are a kind of virus that replicate through macros. A macro component is a program to automate repetitive action in certain software applications, in particular datasheets, word processors, databases, etc. Thus, files containing macros can contain a virus that replicates in templates and in other documents.

[Rz 77] A Microsoft Word user must know that Microsoft Word is very vulnerable to viruses, since its macro language is very easy and Microsoft Word is very widely used. Thus one should be very careful not to enable macros when opening a Word document coming from an untrusted source since the template attached to the document could be infected.[29] Effectively, if the e-mail is opened there is no risk as long as one does not open the file, since an e-mail with an infected document does not infect the computer unless the document is opened in Word.

[Rz 78] At this point one would consider not accepting any e-mail attachment and simply removing the attachment when receiving an e-mail containing one. Another possibility would be to open the attachment with a viewer so the user can look at the content of the document without activating macros. A third possibility is not to activate any macros when requested to do so. Finally it is necessary to install an anti-virus program and update it regularly.

[Rz 79] Further, as doc files can carry many viruses, an alternative consists in saving the file in the rtf format, since rtf files do not contain any macros. The rtf file can then be loaded into Word or converted back into a doc file. Thus, rtf is a good instrument for transferring a document while ensuring that no virus is transmitted. However, there are some disadvantages to using the rtf format: the document´s formatting can be altered during the conversion, so it is better to make some proofs before committing to use the rtf format. Notwithstanding, receiving an rtf file is not always secure because some macro viruses force the user to save a document as a doc file but with an rtf extension. Thus, when trying to open the infected document Word will automatically open, load the file and activate the virus. To avoid this, the user may use Notepad to open the file. If it is a real rtf file, it will load as ASCII text starting with «\rtf».

c. Adware and spyware

[Rz 80] Adware is a way of advertising. It is a program that sends advertising in different forms like a banner or a pop-up window. Adware can be installed in the computer with the consent of the user who agrees to receive advertising. A problem arises when adware is combined with spyware. Spyware is software whose purpose is to collect information about the user to direct to him more personalized advertising according to his Internet habits. In addition, adware may cause technical troubles since it consumes CPU power bandwidth and hard drive capacity. There exist applications that can stop adware.

d. Password sniffers

[Rz 81] A sniffer is hardware or software that intercepts passwords when they travel through a network. It can be installed in different ways, most commonly through a Trojan horse. The main problem with a password sniffer is the difficulty of detecting it since it does not change anything on the user´s system, it just logs. Therefore, if the number of logs rises significantly, the presence of a sniffer is very likely.

[Rz 82] No programs currently exist to protect a system against password sniffers. The only method to fight against this menace is to modify passwords frequently and to be sure that they always travel through an encrypted network.

e. Trojan horses

[Rz 83] A Trojan horse is a program that, behind a useful function, hides another, less benign for the user. There are many types of Trojan horses, and they can take the form of adware if their installation has not been openly announced to the user and agreed by the latter. Another sort of Trojan horse is even more dangerous since it gives the appearance of an antivirus when it actually introduces a virus into the system. The Trojan horse can also make copies of files for its creator or deliver a tool that may be used to outwit a system security mechanism.

[Rz 84] The best way to be protected against Trojan horses is to take preventive actions and not to run any program or open an unexpected document or one coming from an untrusted source. As mentioned above, a Trojan horse may hide its destructive nature and appear trustworthy.

f. Worms

[Rz 85] A worm is a program that replicates itself into a computer network, instead of in a computer like viruses do. Worms have usually a destructive effect on the system and they can delete files on a host system or send documents via e-mail, making a computer a spam sender. As worms are programs themselves, and are not attached to other programs or files, they can spread very quickly over a network from one computer to the next without needing another program.

2. Technical failures, breakdowns

[Rz 86] Another frequently expressed concern is that technology may cease to work precisely at the moment when it is needed the most. Here the concern often matches concrete complaints based on personal experience: who indeed has not experienced a computer, a network access, a printer, or more simply a photocopying machine that crashed or broke shortly before an important deadline? And it is true: technological systems break down, time and again, no matter how careful one is. A report even showed that five to ten per cent of the global time of work is lost due to problems with computers.[30] This unproductive time is of course not only due to technical failures (it can also be one user´s inability to make a specific application work, or the waiting time for a connection or a printer), but no doubt these amount to a significant part thereof. In addition, the heavier the reliance on technology, or in other words the more important the computer resources used, the higher the chances of a breakdown, as the technology is more in demand and the user makes more mistakes when accomplishing technically complex tasks.

[Rz 87] Nevertheless, this is a not an issue without a solution. The three following types of measures should help avoid most problems in this context.

- *Redundancy.* Cars have spare tires, because punctures are inevitable. Planes have all their technical equipment in duplicate or triplicate, because a technical deficiency must not affect the flying capabilities of the plane. IT systems should follow the same principle. Technical failures and breakdowns are actually an issue of availability, and the usual solution to availability issues is to have another system ready to fulfill the task that the defective system should have handled. The important parts of technical equipment should have backups. Specifically, this means that one should always have, if relying on technology for certain actions, another computer available, preferably a spare one which resembles the original one as much as possible. In addition, all important files should be accessible from two sources, for instance from a shared hard disk and from a personal disk. In professional data storage environments, the shared hard disk, usually accessed over a virtual private network, is backed up every day and is also accessible in another way, for instance over the web.

- *Dedication*. Using a computer for many different tasks may require installing different software. And programs sometimes conflict, especially if an error occurred during the installation progress, preventing the originally installed programs from operating as they did before. Using a computer for different purposes may also require particular configurations, which the user may not know how to cancel when reverting to the original purpose of the machine. One of the most intrusive forms of applications in this regard is sophisticated computer games and file-sharing programs, but they are not the only ones. Consequently, it is advisable to dedicate the computers to be used for arbitration to specific purposes. This implies, above all, that the computer should be used only for strictly professional matters. This includes monitoring who uses your computer, avoiding that one´s children use it for computer games and file sharing. This further implies carefully checking all data imported to this computer, e.g. if it comes from a source that cannot be trusted completely (for instance your computer at home, which is usually not professionally managed); preferably, the data should first be submitted to a virus check on your professional computer or network. Concretely, this may be done by limiting administrator access to the computer.

- *Anti-virus*. These last years, famous viruses have made the headlines for causing major problems to the business community. Recent surveys state that only 83 % of Internet users use an anti-virus application, and of those, only 73% update it regularly. [31] In other words, many severe technical breakdowns could be avoided by installing a high quality anti-virus application and updating it frequently. This is not an anodyne issue if we consider that viruses caused $55 billion in losses to companies in 2003. [32]

3. Issues of authentication and non-repudiation

[Rz 88] Again a university example: in early summer 2004, a few days before a final examination, one professor´s assistant received an e-mail saying «I´ve a last-minute doubt regarding one question of the exam. As I´m not at home, I don´t have the list of questions with me. Could you send it to me again? GKK». The address from which the e-mail was sent read gabrielle.kaufmann-kohler@bluewin.ch. The assistant prepared the reply, attached the file containing the examination questions, and prepared to click on «send», but, struck by a sudden doubt, called the alleged sender of the message on the phone, who denied having sent any e-mail regarding this matter and having a bluewin e-mail address (and having any doubt regarding the questions of the examination). No doubt the student who had to find out about the exam questions in advance was more of a clever technician than a good lawyer…

[Rz 89] The saying «On the Internet, nobody knows you´re a dog» captures this issue quite nicely. And indeed, identity theft is one of the main concerns of both online shoppers and Internet merchants. [33] By extension, many lawyers feel a general uneasiness about the issue of authenticating the real sender of a message. By and large, the issue is overrated. The following, first specifies the issue—it has two different dimensions, which on some occasions require different solutions—and then sets out possible solutions, which are presented in order of increasing complexity.

[Rz 90] The issue of authentication, in a broad sense, corresponds to two questions that may be asked by the recipient of a message. The first question is: «Can I be sure the sender of this message is the person he says he is?»

[Rz 91] This is of importance in the situation where information is requested, expressly or implicitly, by the sender of the message. This is authentication in its strict sense.

[Rz 92] The second question is: «Can I be sure the sender of this message will not deny having sent it, as it bears no manuscript signature?»

[Rz 93] This is of significance in the situation where the message carries consequences that may be negative for the sender (waiving a right, for instance). This question relates in fact to what is technically called non-repudiation. [34] On this matter, one should bear in mind that the general legal principle is that the burden of proving that a given sender has sent a specific message lies with the person who alleges to be entitled to a right or course of action on the basis of this message.

[Rz 94] Considered from the perspective of a message´s sender, and not its recipient as was done above, both questions also correspond to the situation where a message is misattributed to someone, i.e. a message is attributed to a given sender, who in fact did not send the message in question. Finally, non-repudiation also has its counterpart for the sender, who may wish to ascertain that the recipient of a message will not subsequently deny having received it.

[Rz 95] Hence, one may suggest the following concrete and simple solutions for avoiding, or at least lessening, issues of authentication and non-repudiation, both from the point of view of the recipient and the sender:

- Make a *quick phone call* if there is any suspicion whatsoever. This will avoid that fraud and a technical defects. Both authentication and non-repudiation are thus ensured, although this solution does not produce strong evidence that a message has indeed been sent or received (as it can be denied that the telephone call took place). If some evidence is needed, the same action should be undertaken, but by fax.

- Consistently use the *same e-mail address*. As the example above suggests, creating an e-mail account with a

fake name is easy. Using the same address, and not one from the office, another one from home (e.g. with two e-mail clients such as Outlook) and a third one when travelling (e.g. using a webmail system such as Hotmail), obliges a fraudster to make an intrusion into your e-mail account in order to pass himself or herself off as you, which is more difficult than creating a fake e-mail account. In addition, when a new e-mail address needs to be created, for instance because of spam volumes, the new address should be communicated to your contacts using the old e-mail account, not the new one.

- *Change the password* of your e-mail account regularly, and watch who knows your password. This reduces the risk of identity theft, i.e. that someone uses your e-mail account to access confidential information or to commit any other fraud. This recommendation is particularly important if the same password is used for different logins or situations.

- *Acknowledge receipt* of a message, if it is not otherwise replied to. Not only is this basic good manners (as e-mails still sometimes get lost as a result of technical reasons, e-mail overload and ensuing difficulties with their management), it also allows non-repudiation of receipt—particularly so if the above recommendations are respected, as they ensure the identity of the acknowledging person.In this sense, it is a service done to the sender. If all the persons involved in a process systematically follow this procedure, it can be expected to create an atmosphere of trust and it will be more difficult to allege non-receipt. It must be said that the currently most widely deployed e-mail protocols do not allow for the automatic non-repudiation of e-mails, i.e. non-repudiation without the recipient´s collaboration. Only if specific protocols and e-mail programs are used can one prove the notification of an e-mail.[35]

- For particularly important documents, *use a password*[36] that only the true sender and intended recipient know (this password should be transmitted through a different channel, for instance over the phone). Password protection authenticates the sender and provides for non-repudiation of sending (and it constitutes quite strong evidence thereof). In addition, such password protection obviously also achieves it primary goal, i.e. that only the intended recipient is able to read the document.

- The most complete solution, which is more complex to implement, is to use *digital signatures* with public-key encryption. Such digital signatures provide the best guarantees of authentication, which often go beyond the level of certainty that is actually required in practice. Digital signatures are addressed in further detail below. [37]

4. Working habits

[Rz 96] The most fundamental obstacle to the use of information technology in arbitration, as in most other business contexts, is working habits. One must admit that working with electronic documents might jar with several aspects of the working habits of the majority of senior lawyers, who constitute the main population in the field of arbitration. Younger generations (born in the seventies and later), who grew up with computers, often have an easier contact with computers. Nevertheless, even these younger people have usually been trained to work with books, articles, memos, and other paper documents spread out on a desk, notes scribbled on notepads, files organized in hanging folders and ring binders, papers piled in stacks, etc.

[Rz 97] The problem is that no matter how big one´s screen, it will always be smaller than most desks and it will always be in two dimensions. Consequently, the number of documents that can be displayed at one time is less than on a desk; the vast majority of people actually prefer to have only one document displayed at a time, which occupies the entire screen, as the two-dimensional layout of a screen makes it more difficult to concentrate on one window than it is to focus on one paper document even on relatively full desk. Hence, many people find that, as long as one works with a relatively limited number of documents and files at a time, they are closer at hand on a real desk than on a virtual desktop and that it is easier to keep an overview of paper documents than of electronic ones. Moreover, reading on a screen requires getting used to it, especially for longer texts; it requires a different kind of concentration from that needed to read a book, and it is not taught in school.

[Rz 98] In addition, many users make a very common mistake in the use of computers, i.e. they put their e-mail software on automatic e-mail check at very short intervals, sometimes even every minute, and have incoming e-mail

accompanied by a pop-up or sound alert. This reduces concentration and thus efficiency, thereby precisely achieving the opposite result than the one sought.. Any management manual will confirm that such behavior seriously distracts the user, as any task requires a given period of time (which is longer if the task is more complex) to obtain full attention and efficiency. Each switch between tasks makes one lose such a period.As a result of this bad working habit, work on a computer is less efficient than with the computer completely turned off.

[Rz 99] These differences between working with computers and working on a real desk have created a reluctance to spend the time needed to acquire the necessary skills and to change working habits. Many lawyers print out e-mails in order to read them like a letter—ironically, even some of long-standing experts in the field of IT and the law. The most extreme ones actually even admit to being almost totally unable to use a computer and having a secretary as a human interface between them and the machine. At the other end of the scale, arbitrators coming to a hearing with nothing but their laptops are still considered «impressive», which means that they still are an exception. So the question: why change? Why learn to use the best of IT in legal practice? The answer is based on a basic management principle: the most important tasks are those that have the highest «multiplying effect», as management theorists call it. This is the capacity of a project to allow or trigger other projects, i.e. to be a catalyst for improving the work process of an organization as a whole. Some obvious examples include selecting and recruiting a skilled workforce, learning a language, and drafting an action plan. Acquiring IT skills falls into the same category.

[Rz 100] Hence, as one such «impressive» arbitrator using only a laptop during arbitration hearings suggested, it would be useful for all lawyers to acquire at least the following basic skills [38]:

- Typing: many applications teaching how to type quickly are currently on the market. Basically they teach by repetition of exercises. At the beginning of the course they explain how to place one´s fingers properly. Thereafter, they go through exercises requiring the user to strike given keys, in increasingly complex and quick sequences. Typing skills may be improved tremendously by the use of such applications. It should be remembered that a major part of most lawyers´ work consists of typing and that a very large part of interactions with a computer consist of text input. In other words, the time lost learning to type quickly is in principle paid off a great many times by the time gained later on.

- Learning in depth some basic applications, such as Microsoft Word, PowerPoint, and Adobe Acrobat.

- Moreover, and it cannot be stressed often enough: do not keep your e-mail on automatic-checking mode with short intervals between e-mail checks. As a rule of thumb, one may say that it takes about 20 minutes to reach full concentration when accomplishing a relatively complex task, such as writing. An incoming may easily put an end to one´s concentration, which must then be rebuilt. Retrieving e-mails once or twice a day should be enough.[39] One should not allow other people to get used to and thus expect extremely prompt e-mail answers. Similarly, one should not expect it from other people. Urgent requests should be accompanied by a phone call.

- Finally, it is useful to spend some time forcing oneself not to print everything out but to read lengthy texts on a screen, as well as to work on a file involving numerous documents while resisting the temptation to use paper copies of the documents.

5. Organizing a procedure during which recourse to IT is made: some recommendations

[Rz 101] Some basic recommendations should be kept in mind when planning an arbitral procedure that is likely to include a recourse to IT, be it in writing the arbitration agreement, drafting procedural rules for an arbitration institution, or in the organization of the proceedings of a specific arbitration case. These recommendations are listed below. They are not, exhaustive; they merely serve as general guidelines on some of the important aspects of conceiving an arbitration procedure.

[Rz 102] The *arbitration agreement* should include no detailed provisions on the technologies to be used. If included at all, technical provisions should be termed as broadly as possible (i.e. using terms such as «electronic document management», «electronic document transmission», «videoconferencing»), because the available technologies change rapidly and the dispute may only emerge a long time after the agreement has been signed.

[Rz 103] The same holds true, but to a lesser extent, with regard to *institutional rules* of procedure drafted for an unlimited number of future case. Procedural rules should not contain detailed provisions on technology because of the difficulty of foreseeing all possible purposes of technology. Consequently, only general statements should be contained in such provisions. For instance, one may think of «formats that are standard in the international legal community», with examples like «doc, rtf, jpg, bmp», or «format that can easily be read and produced by all parties». The final decision on specific IT solutions in this matter should always remain within the discretion of the arbitral tribunal exercised in consultations with the parties.

[Rz 104] The *procedural order* by the arbitral tribunal on the IT solutions that will be used should be rendered, as much as possible, after having sought the parties´ agreement, during a preparatory meeting or during the Terms of Reference phase in an ICC arbitration. Such a decision should in particular cover:

- The exchange of electronic documents: whether documents will be exchanged as e-mail attachments, through a case management website, or using a physical carrier (DVD/CD).

- Admissible file formats. Standard format transmission should always be used (doc, rtf, pdf, jpg, bmp, etc.), to avoid forcing a party to install expensive proprietary software on the computer on which the file is to be read. In addition, one should use formats that do not carry metadata (information about the author of the document, on which computer it was modified, tracked changes, etc.[40]), and that do not execute scripts (very small applications executed by the computer, generally Microsoft Word macros but possibly viruses). Concretely, this means that the rtf format should preferably be used, rather than doc. Conversion of a doc document to rtf is simply achieved by selecting rtf when doing a «save as», in any word processor.

- Available fonts. Unavailable fonts on a computer may significantly change the layout and pagination of a Word document.

- File naming and classification system. This is particularly important if a case management system is used to which all participants upload documents.

- Scanning documents not available in electronic format. The rules should specify whether it is possible or not, whether it should be done using a text recognition software (which always has some inaccuracies) or not (by saving the scanned document in an image format, thereby preventing the use of the search function and making editing much more difficult).

- Fall-back strategies. In case a given technology does not work properly, the rules should provide which other IT solution will be replace it, or whether offline solutions should be used instead, etc. For instance, when scheduling a videoconference, one should keep in mind that technical breakdowns occasionally occur. Some such breakdowns cannot be minimized by having backup equipment available, because it can be difficult to provide backups for certain equipment, e.g. the central servers of the Internet service provider. In such situations, it should for instance be decided in advance if a videoconferencing session that cannot be completed may be replaced by a telephone conference or if it should be rescheduled, etc.

- Videoconferences should be scheduled to last a half day at most; like teleconferences, such sessions require much more concentration than face-to-face meetings and are consequently tiresome.

- Costs allocation for the acquisition and use of IT tools.

- An express provision that the arbitral tribunal may amend such rules.

[Rz 105] On all occasions, one should remember the most basic principle: do not overdo it. In principle, one should use relatively simple and robust technologies. Using IT solutions should never have as a goal the demonstration of one´s IT capabilities. The use of IT is a means, not an end. The end (increasing efficiency, reducing costs) justifies the means, not the reverse.

V. Basic communication technologies

[Rz 106] Some standard communication technologies will be presented briefly in the next section, either because they are used in the context of arbitration, or because they constitute parts or even the basis of other means of communication that are relevant to arbitration. In addition, understanding, in rough terms how these technologies work from a technical point of view facilitates the understanding of the pros and cons they imply, and of the opportunities and issues they raise. The following will thus provide a brief overview of e-mails and discussion lists; chats; bulletin boards (often called Internet forums); designated community websites; and wikis.

1. E-mails and discussion lists

[Rz 107] Professionals will already be familiar with e-mail and discussion lists. Discussion lists have been used in several sectors to promote both professional and popular discussions. By the end of the 1990s there were thousands of public lists and many more closed ones. Many of these lists are moderated, although not all. Moderation ensures control of membership and that content is maintained. It has the downside that it can be used to stifle discussion. In general, though, moderated lists are the more effective communication spaces.

2. Chats

[Rz 108] Text chat, more commonly known as «instant messaging», provides synchronicity. The most popular non-commercial system is *Internet Relay Chat* (IRC). To use instant messaging, it is first necessary to install a client program which connects to one of a number of interconnected servers. Chat systems support virtual environments that can be configured to establish chat rooms (also called channels) around particular topics, interests, or real and virtual groups. Chat systems can be compared to analogue CB radio. In 2003-4 the most popular IRC clients were *mIRC*267 for Windows and *Ircle* for MacOS. While chat clients may be different, the networks to which they connect are the same. Chat systems are often integrated into more sophisticated means of communication that may be used in arbitration, such as case management websites and videoconferencing. In these contexts, their purpose is primarily to constitute a fall-back solution should other, more fragile, channels of communication (video and audio transmission, for instance) cease to work.

3. Bulletin boards or Internet forums

[Rz 109] In their traditional sense, electronic bulletin boards (BBs), were most commonly used in the 1980s. BBs allowed users to check the notices on the board and to post their own messages. To do this, users had to dial in and log on to a remote computer. In many instances it was possible to exchange messages in real time with other users who were logged on simultaneously. BBs offered users a sense of control and interactivity – unlike discussion lists where they received every message, BBs supported choice, selectivity and topical threads. Participants had access to all the available information, but they could choose what they wished to access. The features of BBs supported communication mechanisms that formed the basis of chat systems.

[Rz 110] Since that time, technology has evolved and BBs in the traditional sense are barely used nowadays. Since the mid-nineties, the term «bulletin board» is increasingly used in the sense of «Internet forums» (they are also termed «web forums», «message boards», «discussion boards», «discussion groups», or simply, «forums»). In this sense, they refer to applications providing for threaded discussions on a specified web page, organized according to topics and date of posting. In contrast to chat systems, bulletin boards are more asynchronous in nature, in the sense that chats are used for immediate reactions, often within a few seconds (hence their name of «instant messaging»), and are usually not recorded somewhere, whereas bulletin boards generate slower reactions and the various posts are in principle recorded by the server and stay online for quite some time. In the context of arbitration, bulletin boards are for instance used in virtual case-rooms to record briefs and other documents filed or to organize procedural matters.

4. Designated community websites

[Rz 111] The development of Web technologies has transplanted many BBs or IRC-type activities onto standard community websites, which allow people to make new connections and expand their personal networks. Ryze, for instance, was built with the special purpose of helping to create and extend business networks. The site includes private messaging facilities, an events calendar, a message board, home pages and profiles, and a contact management system. Ryze supports over 150 networks with very different sizes and communication intensities. Virtual case-rooms are built on this concept; the various participants in an arbitration proceeding constitute, after all, a designated community. In this sense, the communication technologies used in arbitration are means to enhance collaboration within a community.

5. Wikis

[Rz 112] A wiki is defined as «the simplest online database that could possibly work», and takes the form of a collaboratively edited website which can be altered either by any user or only by specific users. In other words, a wiki is a website on which individuals can add content as on an Internet forum, but this content can then be edited by other users: it is a collaborative writing tool accessed directly through a web browser. «WikiZens», as they are known, contribute to the development of the content wikis by adding to or editing the work of their fellow authors. While it is surprisingly rare to hear of WikiZens destroying the work of others, most wikis have a rollback system which allows the recovery of maliciously deleted material, and facilities for blocking the IP addresses of repeat offenders. In the legal context, one of the most famous recent uses of a wiki is the collaborative writing of the second edition of Lawrence Lessig´s book *Code and other Laws of Cyberspace*,[41] whose actual text is open to editing by any Internet user until a specific date, after which it will be revised by the main author and published in paper form. This technology provides particularly useful advantages when a team is working at the same time on the same text, as it avoids working with numerous versions of the same document annotated and corrected by different people.

VI. Some considerations about e-mailing

[Rz 113] Although the use of e-mails has become as natural to many people as placing a phone call, and despite the fact that about a billion people today possess an e-mail address, the use of this technology is still very much marked by unfortunate practices. The reasons for this may be that the technology provides for much more diversified uses than the telephone and that the social norms (which fundamentally constitute best practices) do not yet exist for e-mail quite to the same extent as they do for other forms of correspondence. Hence, this section seeks to suggest some guidelines generally accepted by entities that have taken a position on this subject.

1. Guidelines for an appropriate use of e-mails

[Rz 114] Electronic mail has become one of the principal means of private and professional communication. The extended and frequent use of e-mail has made it a routine task, with the consequence that people are less prudent when using this means of communication. Some such routine uses of e-mail may imply common errors, which can be solved by companies and individuals setting up their own policies for e-mail use.

[Rz 115] E-mail can be very useful. At the same time, it may also be dangerous since it can constitute an open door for viruses, hackers and other unwanted visitors. Moreover, the negligent use of e-mail may cause the disclosure of confidential and private information that was not intended to be sent.

A. Sending e-mail

[Rz 116] When sending e-mail the main concerns are the information sent and the addressee. When considering writing an e-mail, it is very useful to consider five of the classical journalist´s questions: What? Who? How? When? Why?

a. What information is to be sent?

[Rz 117] One should consider the kind and size of information to be sent, which includes when forwarding an e-mail, if it is really useful or indeed advisable to forward the history or not. The e-mail should never be used to send a password or bank account information, and unnecessary attachments should be deleted. It is important to be cautious when writing e-mails, especially if the content can prejudice the sender (incriminating e-mails), since in some cases, like in antitrust proceedings, can be legally compelled to disclose e-mails. Thus, it is always best to assume that nothing will remain private, and to remember that removing an e-mail from a computer or e-mail account does not remove it from the server (it also remains hidden on the hard disk for an undetermined time). In other words, an e-mail can almost always be recovered.

b. To whom are you addressing the mail?

[Rz 118] It is important to use the carbon copy («cc») and blind carbon copy («bcc») options correctly and to check to whom the e-mail is sent, in particular when using the option «reply to all», as one may not wish to reply to all the addressees on . Furthermore, when using the carbon copy option, privacy issues may arise if copying to one´s own client (since it discloses his address) or to the client of the opponent without an express consent.[42]

[Rz 119] Also, an e-mail should be sent only to people who really need it, in order to avoid the proliferation of e-mails, which can encumber one´s mailbox.

c. How is the information sent?

[Rz 120] At this stage, a prudent user should consider if, regarding the type of information at hand, it is appropriate to use e-mail rather than other means of communication. Once the possibility of using e-mail has been accepted, you should write it clearly using ASCII-Format (rather than HTML). When attaching documents, it is advisable not to use the Word format or any other proprietary format, but rather rtf, pdf, or even HTML formats.[43] In the subject line, the sender should also write a descriptive title to allow easy identification (a common system of nomenclature is very helpful). Naturally, if an encryption system is available, it should be used.

d. When is the e-mail sent?

[Rz 121] Here the user must consider if the moment he/she intends to send the information is appropriate or whether it may be preferable to send it later for any strategic reasons. Once the e-mail has been sent, it cannot be retrieved.

e. Why is the e-mail sent?

[Rz 122] The purpose of the e-mail has to be considered, since it can determine the language used (if no answer is expected the e-mail should specify that it is for information purposes only). The intended purpose of the e-mail obviously also determines whether it is really necessary to send it.

f. Other precautions

- Only important those e-mails should be marks as such.
- Use always the same e-mail address for the same addressee.
- Add a disclaimer, if only for the psychological effect it has.

B. Receiving e-mail

[Rz 123] As suggested above, e-mail is one of the main conductors of viruses. Thus, one should be very cautious when opening e-mails. Some advice:

- Be suspicious when an unexpected e-mail suggests the recipient to do something, such as opening a URL link. The most common and dangerous way of transmitting a virus by e-mail is by requesting its recipient to click on

a URL address or to open a file with the extension .exe or .doc (for the latter, because of the macros a Word document may contain).

- Moreover, with the advent of HTML mail, a system can be infected just by opening an e-mail message. And if the mail client has a preview pane that shows the contents of a message before the mail has actually been opened, then one does not even have to open the message to be infected! This risk is due to the fact that modern e-mail programs, those running on most current computers, can display much more than just plain text documents. The current crop of e-mail programs can display colored backgrounds, graphics and special text fonts. To achieve these feats an e-mail program must accept and run little programs, called «scripts», embedded within the e-mail. Scripts may request a computer to download data from a website, and such data may be a virus. Most of these types of e-mail viruses are rather benign, but a few of them are designed to erase everything on the hard drive, and others, called worms, are designed to not only harm an infected system, but to actively try to spread themselves to more systems, usually through e-mail programs. It may be noted that most of the viruses in this category (so far) have been specifically created to take advantages of flaws in Microsoft Outlook and Outlook Express. As a protection, it is suggested to turn off all references to ActiveX, Java Script or any other special effects.

- Never reply to an e-mail requiring passwords or bank account information. Sometimes these e-mails use the pretext that the recipients bank has changed its system and needs this data. Naturally, such a request does not come from the bank. The practice of sending such fake messages is called «phishing»; it is one of the main sources of identity theft on the Net.

C. E-mail management

[Rz 124] Nowadays the main problem with the management of e-mail is the amount of e-mails received, including unwanted e-mails. Thus, it is time- and trouble-saving to learn to manage them:

- Use an e-mail provider with spam filter, a firewall and a virus scanner.
- Some e-mail clients have an assistant, which allows classifying e-mails received into different folders according to different criteria defined by the user.[44]
- Use an efficient method of classification to find e-mails quickly.

D. Sender authentication

[Rz 125] When using IT, one of the main concerns is the identification of the user to ensure that the person using a system, sending an e-mail or any other IT action is who he says he is, and to prevent other people from having access to the systems. This can be achieved by incorporating a system requiring the user to be identified.

a. Password

[Rz 126] An access password is a security code consisting of a string of characters. The protection offered by this system is due to the fact that only the user knows the password, which is usually matched to an ID. The advantage of this means of security is its simplicity and the ease of allowing third parties to access the system since it will be enough to communicate the password and the ID. However, the more people are provided access, the higher the likelihood of a password violation, since it is not possible to prevent third parties from communicating the password. In such cases the solution is very simple: change the password.

[Rz 127] It is also possible to obtain a password without getting it from the user by obtaining or decrypting the legitimate user´s password key into the system. Many instruments allow this, including dictionaries, cracking programs, and password sniffers, and they are increasingly effective. It may not even be necessary to use these sophisticated systems to obtain someone else´s password. Indeed, many people use very obvious passwords or write them down and leave them in a very accessible place in their desk.

[Rz 128] The best line of defense against all these types of intrusive attacks is a strong password policy that includes a minimum length, unrecognizable words, special characters and frequent changes. Such policies include as basic

precautions:

- Not to use a password generator because they use routines, making them predictable.
- Not to use any word that could appear in a dictionary (either forwards, backwards, forwards and backwards, or with mixed upper and lower cases).
- To use at least 8 characters combining letters, numbers and special characters.
- To change the password frequently.
- Never to write a password down.

b. Access token

[Rz 129] An access token is a security device that normally attaches to a COM port on a system which, when used in conjunction with appropriate software or hardware, allows authorized access to that system. Examples include smart cards and smart card readers. A smart card is a plastic card normally the same size and shape as a traditional credit card, but including a microprocessor and a user interface, that requires a smart card reader. Information contained on the card or generated by the microprocessor can be used for smart cards, which are relatively secure. Information stored on the chip is difficult to duplicate or disrupt, unlike the outside storage used on magnetic stripe cards. However, it should be noted that they are not secure against laboratory attacks. The cost of a card depends on the chip´s capacity and its capabilities.

[Rz 130] An access token can also be a small device screening a combination of changing characters which is synchronized with the system. To access the system it will be necessary to insert the ID, and in the password case, the password followed by the code appearing in the device at the moment. The level of protection of such a device is quite high since the password changes every minute. An intruder will need the ID, your password and the access token. Another variation is a device like a calculator that displays a password when the number given on the website is entered into the calculator. The security is increased since it is necessary to have a smart card to run this function.

c. Biometrics

[Rz 131] Biometrics is an increasingly important method of authentication sometimes known as the «third level of authentication»: [45]

[Rz 132] The primary areas of biometric technology are:

- Face recognition
- Fingerprints
- Hand geometry
- Iris recognition
- Palm prints
- Retina pattern
- Signature
- Voice

[Rz 133] Other areas for authentication are currently being researched and include body odors (the chemical pattern created by human body smell), ear shape (the shape and structure of the ear), and keystroke dynamics (individual human typing rhythms and characteristics).

[Rz 134] A key characteristic of a biometric access system is that it must operate in real time and the access can be given immediately. An example could be a fingerprint or eye scanner, which scans the fingerprint or the eye and instantly compares the results to a stored database of acceptable fingerprints. This should be contrasted to DNA testing. DNA is a unique biometric, however real time analysis of DNA is not yet possible.

E. E-mail encryption, digital signatures, and digital certificates

[Rz 135] E-mail encryption and digital signatures are very closely linked: both rely on asymmetric key cryptography.

E-mail encryption, which consists of making messages unreadable by third parties, involves this form of cryptography insofar as only one person is able to decrypt, and thus read, a message that anyone can encrypt. Digital signatures, which consist of creating a sort of code that only the signatory could have created, involve cryptography in the sense that only one person, the one who is authenticated by the signature, is able to encrypt a specific part of a message, which may then be decrypted by anyone. It may be noted that the encrypted part in this situation is not a part of the body of the message, which remains in plain text readable without decryption.

[Rz 136] The system of asymmetric key cryptography (also called public key cryptography) involves a pair of keys or ciphers: one public, one private. These two keys, which take the form of algorithms, correspond to each other, and to no other key. Together, they constitute what is sometimes called a key ring. The private key is a type of secret code. The public key is an open code, a counterpart of the secret one. The private key is used to decrypt data encrypted using the public key (in the context of e-mail encryption) and to encrypt data that can then be decrypted by the public key (in the context of digital signatures). The public key is used to encrypt data that can only be decrypted by the secret code (e-mail encryption) and to decrypt data that could only have been encrypted using the secret key (verification of a digital signature). These functions are further detailed below.

a. Private and confidential e-mails: encryption

[Rz 137] In the context of e-mail encryption, the public key is used as a padlock, and the private key is the only key that opens the padlock. Here is how it works: the public key transforms the text of the message into a cipher text. This cipher text can then only be decrypted using the corresponding private key, which only one recipient holds.

[Rz 138] An encrypted message looks like this:

```
From: Gabrielle Kaufmann-Kohler
Subject: My revisions of the manuscript
To: Thomas Schultz
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.1 (MingW32)
Comment: GnuPT 2.7.2

hQIOA2zmrj9w1bMoEAf/aWsz7AD5oKDJfPr2vWq9HcWlY4xFkBf9Zz+xNIEKoXeN
4GVXsNzhj7ls4yD1pIHtHFIZ3KEAIQGOjDAWMCDZGgbpAR6EbK3v1mkWN6cHEcNU
JAi+8xGcADQypfYVLHCywEQ7sq2yvHTtZ7xbxDh1NKSyttrlrxLOGYZNOpv9W+mu
2CYiSykHJMDPHvDylOXL/siY9tgvFOJAXJnmOBtM7L/HxEXUAJ5Uy60rOmQkhe8/
Qj4hA1Y6KHgXsfMf1+ko2M9NUxPOevZq5DJRfZXqA03xg72cm77IAsJu7j/nCT+k
lV4DR+4OH2ZRnU0jPgwiLrG8niQ++ucCjgV2YLFwxAf9GIm3dxBGcKBOPoBsgfmG
x5Thi58hsHYW2+LR/yR4yiJEigo3nacKReFeN+9ERXN9FTkVecmcrKzTSINMWbSb
O+slo8k05UOuqa2P7OLf0ymBjazzcI9xp7K398rbCGrN2LqjK2c7/HQTj3ZQifHA
2uH5vamPFJOO1vDz1/kZYvhOfFelxwztdFLFwQnfVDZYqsnjJVE3dnXOk/4jln8T
kf8mPrhRGEH9HuK2kdyJMY4KnE3enVhE/EzbXlpQOIdW6kLFJeYjB+w1j2RD5/ao
amNez37qa9KyfqCf++hpRFIqUaf1bCqJdj6uLsIEOovoxOla7Xo+s6bV26s6wYIS
MEwvCyNXoallpAqNuESbx+KVk7ny9nmY8C1uV8S6QTmWs37JZkHIAhY=
=cWfm
-----END PGP MESSAGE-----
```

[Rz 139] Once the message is decrypted using the appropriate private key, the cipher text simply becomes plain text, readable as any other text. If the text cannot be decrypted, this means that either the wrong public key was used for encryption or the wrong private key is being used for decryption, the latter implying in principle that the message has arrived in the wrong hands.

[Rz 140] User would apply for a pair of keys or «key ring», keep the private one secret and distribute the public one through websites called «keyservers» or by e-mail. This is what made asymmetric key encryption such a

breakthrough: there is no need to transmit the private key to decrypt messages, only the public key is used for encrypting messages.

[Rz 141] To send an encrypted e-mail to someone, one may either ask this person to send his or her public key, or try to download it from a keyserver—in any event, this person must own a key ring. This public key is then used to encrypt the message in such a way that only the holder of the private key can read it.

b. Identifying the sender and verifying the authenticity of the text: digital signatures

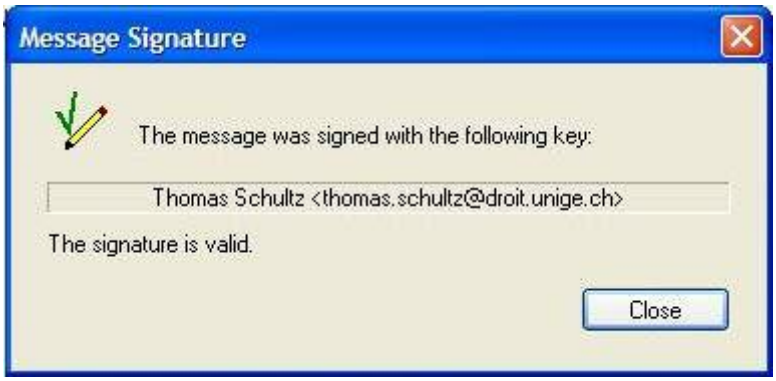
[Rz 142] In the context of digital signatures, the private key is used for signing, the public one for verification. Here is how it works: when applying a private key to a message in order to sign it, the signing program generates a hash value, which is a unique mathematical summary of the content of the message. One hash value can only relate to one specific message. If the message is altered, it will not produce the same hash value. This hash value is then encrypted using the private key and the message is sent. Its recipient then decrypts the hash value using the sender´s public key. If the recipient is unable to decrypt the hash value, this means that the public key being used does not match the private key, which indicates that it was not the expected private key that was used to encrypt the hash value and thus to sign the message. Once the hash value is decrypted, the recipient creates a new hash value on the basis of the message received, using the same hash algorithm as the sender. Thereafter, both hash values are compared: if they match, it means that the content of the message was not altered since its signature (i.e. since its «hashing») and, again, that the signatory of the message did indeed use the corresponding private key.

[Rz 143] On this basis, one may say that a digital signature has three functions: sender authentication, as only this specific sender´s private key could have signed the message; non-repudiation of sending, in the sense that the sender cannot deny having sent the message, as only his or her private key could have signed the message; and data integrity, which means that the content of the message has not been altered since its signature.

[Rz 144] Here is what a digitally signed message looks like:

```
Date: Mon, 07 Nov 2005 14:18:20 +0100
From: Thomas Schultz
Subject: Confidential documents
To: Gabrielle Kaufmann
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Dear Gabrielle

Please find attached the latest revisions on the manuscript of this book.

All best,
Thomas

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (MingW32)
Comment: GnuPT 2.7.2

iD8DBQFDb1NeQQXNCQCKu3sRAnvNAKC4KjsnnKJjEJBHMeXHgrz/5SnC/gCfd98p
9cY5x3QihK6aVcamiJ7i5WQ=
=UcRV
-----END PGP SIGNATURE-----
```

[Rz 145] The confirmation that the message has not been altered and that the sender did indeed use the purported digital signature looks like the following:



[Rz 146] To digitally sign an e-mail—for which one must own a key ring—one simply applies the private key to the message. The recipient may then check who signed the message and that it has not been altered since it was signed, by checking the message with the public key, that may be found on a keyserver or distributed by e-mail. The question on how and where to obtain the public key to verify a digital signature leads us to the next part, which relates to the question of which key ring one may trust.

c. Trusting digital signatures and key rings in general: linking ciphers to people

[Rz 147] A digital signature only means that a given private key has been used. It provides no guarantee, in and of itself, as to the holder of this key. It only authenticates the key, not the person who uses it. Hence, even if one assumes that the key has not been stolen, how can one know that the holder of a given key is indeed the person he or she claims to be? A private key can be the equivalent of a fake ID.

[Rz 148] E-mail encryption relies on the use of a public key. But who´s public key is used? In principle, if someone wants others to be able to send him or her encrypted messages, this person only needs to publish a public key. Anyone acquiring this public key through a public keyserver—in other words, anyone who knows how digital signatures work—can then send this person secure, encrypted information. Unfortunately, someone else can also create a key ring under a fake name, publish the public key (and thus know the related private key), claim that he or she is the individual bearing the name indicated by the key, and thereby receive at least some of the encrypted messages meant for the individual who does indeed bear the name indicated by the key. This begs the questions: how can one trust the public key? How can one know that a given public key does indeed belong to a given person?

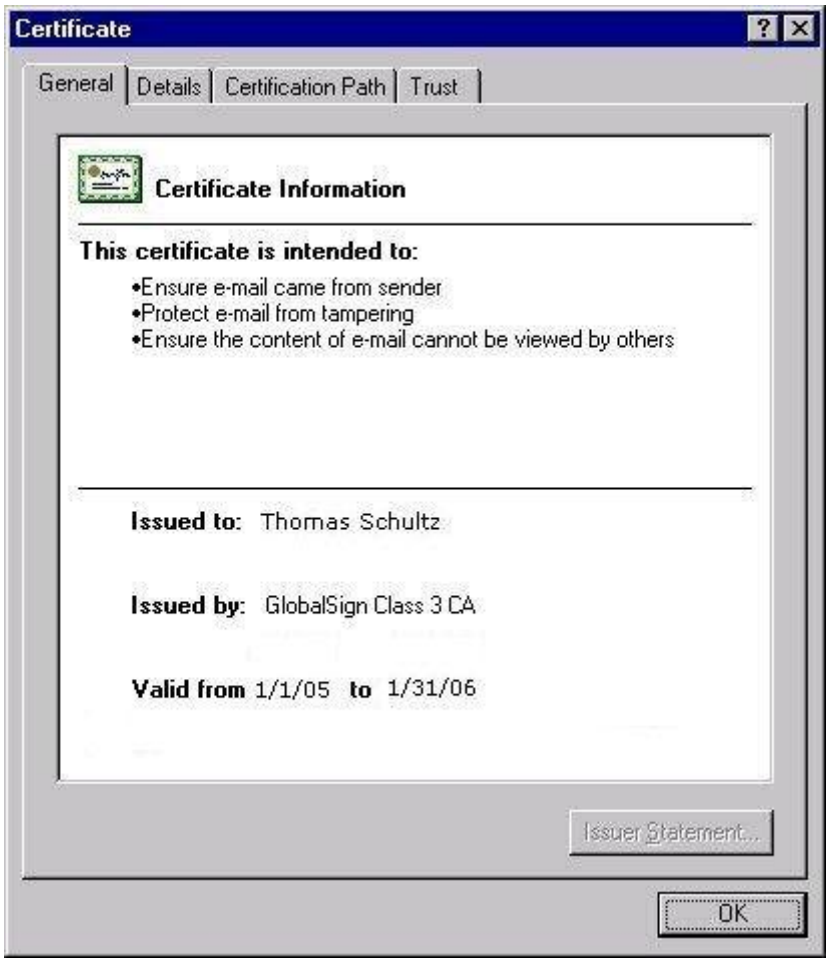
[Rz 149] The answer to these two questions is certification, i.e. a confirmation that the key ring and the identity do indeed belong together. This certification can take two forms: either it relies on so-called «self-certification» or «endorsements», or a third party provides a «real» certification.

[Rz 150] In the first case, called the «web of trust scheme», the certification, in other words the assurance of the identity of the holder of the key, may be based on one of two instances. First, this assurance may follow from a direct contact with a trusted party: if A knows B, and B tells A in a trusted way that he or she will now send the public key, which then identifies the private key that will be used in the future, this key ring may in principle be trusted. This is what is sometimes called «self-certification». Second, if A knows and trusts B and B knows and trusts C, then C may send B the public key, which is then forwarded to A. This scheme is called «endorsements». However, these two types of «certification» only work for small networks of persons who know each other. For the Internet globally, something else was needed: third-party certification.

[Rz 151] Third-party certification relies on the idea that a public key (and thus the whole key ring, as the private key necessarily corresponds to the public key) is built into a certificate, which contains information such as the name of the bearer of the key, its address, and so forth, thereby attesting that the public key belongs to the entity noted in the certificate. This public key certificate is then digitally signed by a trusted third party, in principle a certification authority (CA). Such CAs may either be commercial services, run be private companies or governments,[46] or non-profit ventures.[47] The task of such CAs is to check the applicants´ true identity and credentials, in other words to establish the correctness of a match between key rings and real individuals or companies. This match is established on methods that vary from one CA to another, but generally rely a combination of ID cards such as passports or

driver´s licenses, credit card information, and third party databases and services.

[Rz 152] The certification of a public key, which may be viewed using a command that varies depending on the e-mail program used, has the following appearance:



[Rz 153] A detailed guide on how to acquire, install and use a pair of keys in order to encrypt e-mails or to digitally sign them is provided in Chapter 5.

2. Privacy risks through metadata

[Rz 154] Metadata is information describing information. A very common example of metadata is the information provided by Microsoft Word when the «track changes» option is activated, since it allows the user to know who wrote or removed what information, when he did it, etc. Metadata is very useful when multiple authors work on the same document since it allows them to know what information has been changed since the last version. However, managing metadata is a critical since it can disclose information that was not intended to be shared.

[Rz 155] Companies entering into a contract often share the same document and make amendments to it to reach the final version. Within the same company different people can also be working on the same document and they may write comments for internal use. In this case, if metadata is not well managed it could disclose highly confidential information or information that could be offensive to the other side, with the results that the negotiations could be broken off or that a company could be put at a disadvantage because of the disclosure of confidential information.

[Rz 156] This example shows that metadata can have important business consequences. If we add that a company manages hundreds of contracts, this problem increases if users do not know how to use and remove this kind of information that can also be internally confidential . Of course, metadata can provide very useful evidence in cases of

document manipulation.

[Rz 157] Metadata can be transferred by sending documents via e-mail, sharing files or creating new documents from existing templates. This contrasts with the difficulty of removing metadata, since it requires that every person working on the same document turn the «track changes» function off and remove information included in the «properties» section. Even Internet filters are inadequate as they are unable to block out all metadata. Some applications exist that can hide and reveal metadata in Word documents and e-mail, protecting sensitive information while allowing compliance with audit requirements.

[Rz 158] The solution to the potential problems metadata may cause is not to stop using certain applications, but to pay attention to what is added, removed and/or amended and to have an adequate policy in place including tools to protect against unintended information disclosures. A very good solution when a document is not expected to be modified is to convert it into pdf or HTML format.

[Rz 159] To create documents, the Word format is the most used and Word stores metadata in «properties - custom properties» in the document.

[Rz 160] In general, metadata can be created with the user´s collaboration when a new document is created: the application requests certain data from the user. Normally the user does not know that it constitutes traceable metadata. However, most users do not fill in the requested fields since it is not necessary to create a new document.

[Rz 161] More common and effective is the creation of metadata without the interaction of the user. Metadata can be created:

- When the user creates a new document from a template, as the template copies all metadata to the new document.
- When the user displays the data entry dialog, adds or selects information and accepts it this information is stored as metadata in the document.
- When the user saves a document, the directory in which the document is saved may have a metadata file than can be inserted into the document.
- User details, time and date stamps are also stored as metadata.
- When the user edits a document, he can select some text and save it as metadata.

[Rz 162] Metadata can contain different types of information such as a user´s name and initials, the company name, the name of the computer, the name of the server or the hard disk where the document was saved, the name of other persons participating in the edition of the document, the name of previous document authors, documents revisions and versions, template information, hidden text, or comments.[48]

[Rz 163] On the basis of the foregoing paragraphs, the following recommendations may be suggested:

- *Create clean documents*. As previously said, creating a new document can attach metadata if a document is merely a modified version of an existing document saved under a new name. Thus it is advisable to disconnect a document from its past life by copying the old document into a new shell created with new template.

- *Edit cleanly*. Using the option to «save version» may not remove all deleted text. Thus it is advisable when editing documents to use the «comment» function instead of hidden text, footnotes or endnotes.

- *Don´t send, publish.* The expression «publish a document» means cleaning it up as if it had to be published, thus removing comments and making sure that no unwanted information or any undesired change remains in the document. «Publish» is the electronic equivalent of the instructions to verify that there are no marks, notes or comments on the document before copying it for distribution. This function is provided by software such as iScrub.

- *When creating a new document consider its recipient*. A good policy should distinguish among documents that are internal, documents to be shared with cooperators and documents to be shared with adversaries. To gain

efficiency some companies may use some information about a client for a document template. However it can be undesirable for this information or the relationship between the company and the client to be disclosed, and it is therefore necessary to «publish» the document as described above.

- Concluding thoughts:

  - Do not use «fast saves»
  - Do not use versions. An alternative is to create a folder with numbered files created each time from a new template instead of saving the old but modified document under a different name.
  - Create templates for different documents and for different purposes and/or addressees.
  - Before sending an e-mail, clean it up or have software do it for you. It is useful to have a checklist describing all actions that should be carried out to clean up the document.

CHAPTER 2

LEGAL FRAMEWORK

[Rz 164] In the context of arbitral proceedings, resorting to IT tools raises surprisingly few true legal issues as long as the proper sensible actions are taken. Think, for instance, of the validity of a digitally signed and electronically notified award in an enforcement procedure: while it is true that the validity of such awards may in some contexts be doubtful, there is no reason not to print out the award (which is, of course, almost always written in an electronic format in the first place), to sign it manually and to notify it to the parties by the usual channels. [49]

[Rz 165] This example is a reminder of the basic principle suggested above that one should not overdo it. Using electronic means of communication is not a goal in itself; IT should only be used if it provides a real advantage. Sending an award in paper form avoids uncertainty without creating a significant disadvantage. If this general approach is adopted, only two main threads of issues remain: those related to due process and those related to confidentiality. The following examines these two threads in turn.

I. Due process issues

[Rz 166] Due process issues raised by the use of IT in arbitration essentially relate to the right to be heard; the right to adversary proceedings; and the right to be treated equally. After addressing these three questions, this section reviews the possibilities of judicial review of awards rendered after proceedings during which difficulties involving due process have arisen. Finally, this section addresses the questions posed by the recognition and enforcement of such awards.

1. The right to be heard

[Rz 167] The legal rules on arbitration were not drafted with technologies like case management websites, videoconferencing, and virtual workspaces in mind. Consequently, the legal framework must be tested against this new technology to see how virtual workspaces should be used, if and how the technology should be adapted, and if this framework, in its present form, is flexible enough to accommodate this technology.

[Rz 168] The following sections, examine the legal requirements posed by due process, with its various forms.

A. The right to be heard: sufficient opportunities to present one´s case

[Rz 169] In arbitral proceedings, the parties have the right to be heard, which means that they must be granted a reasonable opportunity to present their case, i.e. to allege facts, present legal arguments, and to produce evidence on relevant facts.[50] Can the use of technology breach due process standards? The question may arise in connection with

sophisticated communication technologies that cannot be easily accessed and mastered by the parties, for instance, if very complex web interfaces are necessary for the parties to present their case. This question calls for several indirect answers.

[Rz 170] First, the arbitral tribunal should always seek to obtain the parties´ consent to the use of such technology. [51] This will in principle resolve the issue: although the parties cannot validly waive all opportunities to present their case, they can jointly choose the method to allege the facts, present legal arguments, and produce evidence. [52] If the consent of the parties cannot be obtained, the question of whether the possibility of presenting the case using complex technology constitutes a real opportunity or merely an illusory right will depend on the technical skills of the parties and the user-friendliness of the technology. The more complex a given technology, the higher the parties´ technical skills and the user-friendliness must be in order to be able to validly obligate them to use it.

[Rz 171] Second, the issue may be avoided altogether if there are supplementary, more traditional, opportunities to allege facts, present legal arguments, and produce evidence. For instance, if the parties can present their submissions and evidence in writing (paper form or electronic format), this will in most cases meet the requirements of the right to be heard, documents-only arbitrations being generally acceptable. [53] The only exception may arise in connection with the right to an oral hearing, which constitutes the next point of analysis.

B. The right to be heard orally

[Rz 172] If there is no face-to-face hearing during the procedure, but only, for instance, a videoconference during which the parties present their case and make their allegations of facts, can this amount to a violation of the right to be heard because no oral hearing was granted?

[Rz 173] The right to a reasonable opportunity to be heard does not guarantee a right to an oral hearing in all circumstances. [54] The European Convention on Human Rights, which might be referred to at least *per analogiam* [55], requires an oral hearing only if it is indispensable to the protection of the «interest of the person concerned» and if the person concerned has not waived that right. [56] As to the law governing the arbitration procedure, [57] which may provide for a possible right to an oral hearing, it varies from one arbitration law to another, but one can make out two main situations. Either there exists no right to an oral hearing (as is the case under English [58] and Swiss law, [59] for instance), or there is a right to oral hearings but it can be waived (this is the case under German, [60] French, [61] Italian, [62] Dutch, [63] Belgian, [64] and Swedish law, [65] as well as under the UNCITRAL Model Law [66]). Consequently, the need for an oral hearing is not a legal obstacle, either because the applicable law does not provide such a right, or because this right can be waived. [67]

2. Adversary proceedings

[Rz 174] In application of the right to be heard in adversary proceedings—in French terminology the *principe de la contradiction*—the parties must be provided with an opportunity to respond to the allegations, argument and evidence submitted by their opponent, by making allegations and submitting arguments and evidence in rebuttal. [68]

[Rz 175] Most arbitral proceedings take the form of a request for arbitration, a response, a reply, and a rejoinder. These rounds of briefs are usually followed by one or several hearings and end with post-hearing briefs. During these communications, the arbitral tribunal or members thereof must have no contact with a party that excludes any other party, because each must be able to take a position on the other party´s arguments and evidence [69]. Moreover, the right to be heard in adversary proceedings requires that both parties have equal access to the record, again to allow them to take a position on the submissions filed by the opponent.

[Rz 176] In the context of arbitral proceedings making use of electronic communication technologies, issues may primarily arise in connection with a technical failure in the transmission of documents using a case management website, or of images and sound or other information in a videoconferencing session (online hearing) or using a shared virtual workspace. In such events, one of the parties may indeed be prevented from receiving the submissions of its opponent and thus responding to them. This amounts to a restriction of the right to be heard in adversary proceedings. If this restriction is significant enough, i.e. if the information that has been exchanged while only one of

the parties and the arbitrators had access to it was sufficiently substantial, and if the arbitral tribunal does not order a replay of the submissions or provide the opposing party with the submitted information in another way and allow a specific opportunity to react to it, then this restriction may constitute a violation of the right to be heard in an adversary proceeding. An award may then be challenged on this ground[70]. This problem can be avoided by using software that automatically interrupts the hearing of one party if the computer of the other party is disconnected, or a reliable means of instant communication to alert the arbitral tribunal of the disruption—a direct telephone connection for instance.

[Rz 177] Some IT tools may even carry a lower risk of ex parte communications between one party and the arbitrators than exist in the offline context, but for technical breakdowns. Indeed, some means of communication such as chat rooms and bulletin boards (or Internet forums) do in principle not allow ex parte communications. E-mails, obviously, are a different matter. Unilateral communications, especially those that arise from simple mistakes, are very likely to be avoided while using chats or bulletin boards[71]. On a more theoretical ground, academic experiments have even suggested resorting to messaging software with an embedded electronic agent that monitors all communications between the parties and the arbitral tribunal. The agent then either permits or blocks these transmissions.[72]

3. Equal treatment

[Rz 178] In arbitral proceedings, the parties have a right to be treated equally by the arbitral tribunal. [73] This does not mean that they must be treated identically, but rather that none of the parties may be put at a disadvantage as a result of the conduct of the proceedings.[74]

[Rz 179] In connection with IT tools, issues may arise because of possible discrepancies between the technological capabilities of different parties, both with regard to the availability of technological tools and the skills to use them. Such discrepancies may be caused by factors like geographical location, firm size, resources, and personal experience with IT. Also, some technologies are widely accessible (due to their low acquisition costs) and familiar even to average users, while others do not have these qualities, causing important disparities among technologies and raising issues with regard to compatibility, costs of acquisition, and familiarity.

[Rz 180] If the procedure and the technological means of communication are organized in such a way that some IT-related actions of one party depend on prior IT-related action of the other party, i.e. if the use of technological tools by one party can only be undertaken after the opponent has acted, the lack of IT competence may disrupt or slow down arbitral proceedings. On the other hand, it is likely that the arbitral tribunal will seek to organize the procedure and the use of IT tools in such a manner as to ensure that the proceedings are not disrupted by the voluntary or involuntary inept use of the technology. In other words, it is likely that the parties will simply have to cope with their own lack of IT capabilities in order to, for instance, meet the time limits set by that the tribunal. With regard to complex technologies, the right to be treated equally may be violated if the technology used cannot be equally accessed and mastered by both parties, one party being at a substantial disadvantage. If the use of such technology has been imposed by the arbitral tribunal and if the technology in question requires more than a reasonable education in IT matters, then such a disadvantage is likely to constitute a violation of equal treatment. Some authors consider that even videoconferencing, when imposed by the arbitral tribunal, might constitute unequal treatment of the parties.[75]

[Rz 181] Nevertheless, one may say that, in general, the larger the case, the less important certain discrepancies between the parties become. For instance, the larger the case, the lesser the role which acquisition and training costs will play.[76]

[Rz 182] Finally, true for the right to be heard, the arbitral tribunal would be well advised to obtain prior consent of the parties regarding the technology to be used and to use software as user-friendly as possible whenever possible, it is further advisable to use only well known formats[77].

4. Judicial review of arbitral awards rendered after proceedings making use of IT

[Rz 183] An arbitral award may be challenged in the country in which it was made (i.e. in the country of the seat of the arbitral tribunal). An action to set aside may only be based on a limited number of grounds, which depend on the applicable law. The applicable law is that of the seat of the arbitral tribunal or, less often, the procedural law chosen by the parties to govern the procedure.[78]

[Rz 184] The grounds for setting aside an award vary somehow from one country to another. All legal systems provide for an action to set aside based on a violation of the right to be heard, but the precise scope of these actions varies, as «each national court approaches the question from its own particular national standpoint». [79]. As a general rule, if the arbitrators:

- have not given the parties a sufficient opportunity to present their case; [80]
- have not granted the parties an opportunity to be heard orally in a country where such a right exists and this right has not been waived;[81]
- have not granted the parties sufficient opportunity to respond on the other party´s submissions; [82] or
- have not treated the parties equally;[83]

[Rz 185] then the award may be set aside by the courts.

[Rz 186] One may recall, however, that an objection based on the violation of procedural rights must be raised immediately before the arbitral tribunal or else the procedural right being violated is considered waived.[84]

5. Enforcement of awards

[Rz 187] An arbitral award may also be refused enforcement or recognition based on a violation of the right to be heard. As the enforcement and recognition of arbitral awards is essentially governed by the New York Convention of 1958, the following considerations will review the three provisions of the Convention that may allow a refusal of enforcement on grounds of due process.

[Rz 188] According to Article V(1)(b) New York Convention, enforcement may be refused if the party against whom the award is invoked was «unable to present his case». This most important ground for refusal under the Convention sanctions, at the stage of enforcement, a violation of due process by the arbitral tribunal. One may remember that the concept of due process covers the parties´ right to be heard in its different forms referred to above. [85] The provision only sanctions very serious irregularities.[86] In the context of case management websites, videoconferencing and possibly virtual workspaces, one may assume that examples of very serious irregularities could derive from one of the following situations.

- A true inability for one or both parties to allege facts, submit arguments, or produce evidence due to the technology chosen by the arbitral tribunal, for instance because such technology was particularly difficult to use and prevented a party from filing its submissions in time.

- In the absence of a videoconferencing session and an in-person meeting, the parties may invoke the violation of the right to be heard orally—if such a right is provided for by the law governing the arbitration the parties have not waived it. If the right to an oral hearing exists and a videoconferencing session but no in-person meeting was held, this should not amount to a violation of this right, as the goal of an in-person meeting is to be able to react instantaneously to the allegations of one´s opponent, which goal is met in a videoconferencing session. Videoconferencing should be regarded as a valid form of oral hearing.

- Lengthy technical failures, e.g. disruption of sound and image transmission, in a videoconference allowing one party to make its case without the other being online; and

- Gross inequalities in the use of the technology selected by the arbitral tribunal.

[Rz 189] Article V(1)(d) provides that recognition or enforcement may be refused if the arbitral procedure was not in accordance with the agreement of the parties, or, failing such agreement, was not in accordance with the law of the

country where the arbitration took place. The considerations involved in connection with the conformity of the procedure *with the law of the place of arbitration* is not essentially different from the ones just discussed in the context of Article V(1)(b). The issue of the conformity of the procedure *with the agreement of the parties* (for instance an agreement that there should be no virtual workspace, or that a specific technology should be used) calls for three comments. First, although the majority of commentators state that the agreement of the parties prevails in any case over the law of the place of arbitration recent views hold that Article V(1)(d) applies only to agreements that meet the mandatory requirements of the law of the place of arbitration. [87] Second, although the Convention provides «no criteria enabling the determination of which procedural rules are sufficiently important to justify the refusal […] in the event that the arbitrators fail to comply with them», [88] U.S. and English courts have held that only those violations of agreed rules that work «substantial prejudice to the complaining party» are covered by Article V(1)(d).[89] Third, it is only very rarely that courts refuse to enforce or to recognize an award based on this provision. [90] In other words, successfully contesting enforcement on Article V(1)(d) is rather unlikely, and in some countries it requires proof of substantial prejudice and that the rules agreed upon and which were violated complied with the mandatory provisions of the place of arbitration.

[Rz 190] According to Article V(2)(b), enforcement and recognition may also be refused if the award is contrary to the public policy of the enforcement state. The public policy addressed here is international public policy, the source of which is, however, the national (i.e. the provision does not refer to «transnational public policy»). It is to be construed narrowly[91]. Although this provision is often relied upon, courts very rarely accept this ground to deny enforcement or recognition.[92] Nevertheless, in one case the *Oberlandsgericht* of Hamburg refused enforcement because the arbitrator relied on documents submitted by one party but not communicated to the other party. [93] In other words, serious violations of the right to be heard, may amount to a violation of public policy under Article V(2)(b). The absence of oral hearings is however very unlikely to constitute such a violation, as such hearings are not even mandatory in the vast majority of countries, and the concept of public policy embedded in Article V(2)(b) is much stricter than the concept of mandatory provisions.[94]

II. Confidentiality issues

[Rz 191] Confidentiality raises increased practical issues in an IT context, because of the extreme ease with which documents can be copied and transmitted and because in videoconferencing entire sessions can be easily recorded without anyone noticing. This acute presence of confidentiality concerns does raise traditional legal issues, not novel ones. The following, briefly reviews the general aspects of confidentiality in arbitration.

1. Basis for a duty of confidentiality

[Rz 192] Confidentiality has traditionally been considered an essential element of arbitration, said to lead parties to prefer arbitration over national court proceedings.

[Rz 193] A duty of confidentiality can be based on national law, on institutional arbitration rules, or on agreement between the parties, be it express or implied in an arbitration agreement.

[Rz 194] Currently, very few national legislations provide expressly for a general duty of confidentiality in arbitration, although some aspects of confidentiality are covered by national provisions. Exceptions are found in New Zealand, where the Arbitration Act[95] provides for a duty of confidentiality in domestic and international arbitration, and in Spain, where the new Arbitration Act compels the parties, the arbitrators and the arbitral institutions to maintain the confidentiality of any information provided in the course of arbitral proceedings [96].

[Rz 195] Many commentators agree that some general duty of confidentiality is implied in an arbitration agreement, although the precise scope of this duty is usually left unclear.[97] By contrast, others consider that no such duty exists even if the parties´ arbitration agreement contains a clause requiring the proceedings to be conducted in private. [98] Still others hold an intermediary position, arguing that since the parties have the option of agreeing that their arbitration process be confidential, a legal requirement of confidentiality not only exists if they have so chosen. [99] A review of national court decisions shows remarkably varying results.[100] On the one hand, in France and the United

Kingdom for instance, courts have found that there is an implied duty of confidentiality in arbitration giving rise to damages in case of violation. For the Paris Court of Appeal, such a duty is, «in the very nature of arbitral proceedings».[101] The same Court has been less categorical in recent cases.[102] For the English Court of Appeal, in *Dolling-Baker v. Merrett*, the «nature of arbitration» creates an implied duty of confidentiality, subject to some exceptions.[103] *Ali Shipping* reaffirmed the *Dolling-Baker* finding, holding that «confidentiality attaches to arbitration agreements as a matter of law»,[104] yet admitting that some exceptions could arise. On the other hand, a U.S. District Court found in *United States v. Panhandle Eastern Corp.* that the private nature of commercial arbitration did not create a general obligation of confidentiality.[105] The High Court of Australia followed a similar reasoning in *Esso/BHP v. Plowman,*[106] where it concluded that confidentiality is not an essential attribute of the arbitral procedure, and an arbitration clause does not imply a confidentiality duty. The court then went on to hold that some technical and commercial information should be maintained confidential, but that public interest must sometimes prevail over the interest of the parties in maintaining confidentiality.[107]

[Rz 196] At any rate, even when it is recognized, there are generally accepted exceptions to the presumption of confidentiality[108], for instance, courts, arbitrators and even the parties themselves may impose disclosure and publicity[109] or national courts may have to intervene to enforce provisional measures or compliance with an arbitral award.[110] In addition, arbitral awards are commonly published without the names of the parties by arbitration journals, institutions and commercial publishers.[111]

[Rz 197] Most institutional arbitration rules regulate the issue of confidentiality only partially[112], by providing for the private nature of arbitration hearings[113] and/or imposing a duty of confidentiality on the institution and on the arbitral tribunal.[114] The degree of confidentiality required varies depending on the institution.[115] Many institutions (including the AAA[116], the ICC[117], the Stockholm Chamber of Commerce[118], the Arbitration Court at the Russian Federation Chamber of Commerce[119], and the CEPANI[120]), as well as the UNCITRAL Arbitration Rules,[121] provide for the privacy of hearings meaning that persons not involved in the proceedings may not attend. A minority of arbitral institutions have more detailed rules on confidentiality, such as the AAA[122], the LCIA[123], and the WIPO Arbitration and Mediation Center[124], the China International Economic and Trade Arbitration Commission[125], the Japan Commercial Arbitration Association[126] and the Swiss Rules of International Arbitration.[127]

[Rz 198] As a result, one may suggest that parties concerned with preserving the confidentiality of their arbitration proceedings should weigh the confidentiality benefits of the different arbitration rules and/or national legislations when drafting their arbitration clause. Because of the variety of solutions described above, parties wishing to ensure confidentiality would be well advised to provide for it expressly in their arbitration agreement.

2. Who is bound by the duty of confidentiality?

[Rz 199] Four types of participants in arbitral proceedings may be bound by a duty of confidentiality: the arbitrators, the parties, and witnesses or experts, the arbitral institution.

[Rz 200] As regards *arbitrators*, only a few national legislations provide for an express duty of confidentiality, such as the the Spanish Arbitration Act[128]. In Switzerland, arbitrators are bound by a duty of confidentiality which derives from their contractual relationship with the parties.[129] In other countries, such as England[130] and Germany[131], specific provisions allow dissenting opinions by arbitrators, which might otherwise be regarded as a breach of the confidentiality obligation imposed on the arbitration tribunal.[132]

[Rz 201] Several arbitration institutions impose a duty of confidentiality upon arbitrators: the American Arbitration Association (AAA),[133] the China International Economic and Trade Arbitration Commission (CIETAC),[134] the Japan Commercial Arbitration Association (JCAA),[135] the Stockholm Chamber of Commerce (SCC),[136] the London Court of International arbitration (LCIA)[137], the Swiss International Arbitration Rules[138] and the WIPO Arbitration and Mediation Center.[139]

[Rz 202] With regard to the *parties* in arbitration proceedings, very few national legislations prohibit them expressly from making public information regarding an arbitral proceeding or an award rendered in the context of an arbitration proceeding.[140] However, the rules of several arbitration institutions require the parties to keep the[141] [142] [143] [144]

proceedings confidential, including the rules of the LCIA, WIPO, the CIETAC, and JCAA.

[Rz 203] Concerning *witnesses*, courts in England have interpreted *Dolling-Baker* to find an implied duty of confidentiality in arbitration proceedings which extends to witness statements. [145] Arbitration institutions are less forthcoming; only a few impose a duty of confidentiality on witnesses, such as the Swiss International Arbitration Rules,[146] the China International Economic and Trade Arbitration Commission (CIETAC)[147], the Spanish Court of Arbitration[148] and WIPO.[149]

[Rz 204] National legislations make in principle no provision with respect to the confidentiality duty of arbitration institutions. Some arbitration institutions, including the ICC, the Stockholm Chamber of Commerce (SCC)[150], and WIPO,[151] explicitly self-impose a duty of confidentiality.

3. What information is confidential?

[Rz 205] The duty of confidentiality can relate to the publication of the existence of arbitral proceedings and of details thereof; to information produced during such proceedings; to the hearings; and to the award.

[Rz 206] There is no consensus among national laws and courts on the extent of details that may or may not be disclosed, and even as to whether the mere existence of arbitration proceedings must be in principle kept confidential [152]. Not many institutional rules require parties to keep the details of the existence of arbitral proceedings confidential.[153] In any case, an exception to any such duty of confidentiality is recognized where parties have an obligation to disclose the existence of the proceedings, for example, insurers, or the stock exchange [154].

[Rz 207] There is no general consensus either on whether documents and information provided produced in the course of arbitration proceedings are confidential. Some national courts have held that there is no general obligation of confidentiality that would apply to documents and information generated in arbitral proceedings, [155] while others have found a «duty of confidentiality [that] attaches to arbitration agreements as a matter of law», and that includes «pleadings, written submissions, and the proofs of witnesses as well as transcripts and notes of the evidence given in the arbitration».[156] Under an exception to the confidentiality duty recognized by the *Ali Shipping*, *Bulbank* and *Esso* cases, a court in a subsequent proceeding may order a party to produce documents from an earlier arbitration. [157] Another exception allows a party to disclose evidence introduced in a pending arbitration when doing so to protect a legal right.[158] Despite the exceptions mentioned, it is the general view that the documents produced in arbitration proceedings are confidential[159] and this view in reflected in the rules of several arbitration institutions. [160] The question regarding documents not produced for the arbitration but used as evidence is more controversial[161].

[Rz 208] Many arbitral institutions provide for the privacy of *hearings* in their rules, i.e. they exclude persons not involved in the proceedings.[162]

[Rz 209] As a general rule, the publication of an arbitral award is not a breach of a duty of confidentiality, [163] at least if information that could identify the parties is deleted. Publication serves important public interests such as encouraging arbitrators to take greater care in drafting awards that will be open to public scrutiny; contributing to the development of the law, including the *lex mercatoria*; and enabling practitioners to cite prior decisions, thus ensuring a consistent application and development of the law. [164] Unlike national laws, most institutional rules make publication subject to the parties´ consent.[165]

4. Sanctions for a breach of confidentiality

[Rz 210] The *sanctions* for breaching the duty of confidentiality are those that normally result from the breach of any contractual obligation: an injunction,[166] damages,[167] or both. Sanctions can be included in an arbitral award that can later be enforced by court order if necessary.[168]

5. Some recommendations

[Rz 211] In sum, there is no consensus and there are uncertainties regarding the existence, extent and addressees of a duty of confidentiality in arbitration. Hence, in a context where confidentiality matters and where electronic communication means are used to and thus confidentiality breaches may be more likely, it is advisable for an arbitral tribunal to address the issue at the outset of the proceedings. This will allow to record the existence and scope of confidentiality and to choose methods of electronic transmission that preserve confidentiality.

CHAPTER 3

CURRENT PRACTICE AND GUIDELINES REGARDING THE USE OF INFORMATION TECHNOLOGY IN ARBITRATION PROCEEDINGS

[Rz 212] Chapter 1 provided a general introduction on information technology; it has portrayed in general terms its potential benefits and presented ways to take advantage of them, suggesting what could be done. Chapter 2 then shown the obstacles, or rather the constraints that law imposes on the use of such new communication technologies, advising what should not be done.

[Rz 213] Chapter 3 now discusses what is actually being done: how the world of arbitration has taken advantage of IT tools to date, in terms of technical services and recommendations offered by arbitration institutions.

I. State of practice

[Rz 214] Three of the world´s most significant arbitration institutions have embraced the necessity of providing parties and arbitrators wishing to use IT with systems that have proven reliable. All three institutions have thus developed—or are in the last stages of the development of—institutionalized IT services specifically adapted to the procedures they administer. The following describes the project of the ICC (NetCase), and the systems of AAA (WebFile) and WIPO (ECAF).

1. ICC – NetCase

[Rz 215] NetCase is a case management website for participants in ICC arbitration proceedings, [169] launched a few weeks ago. It is accessible by the parties, their counsel, the arbitrators and the Secretariat. Its goal is to allow participants, if they consent to its use, to communicate and share information rapidly and securely using the Internet, [170] yet it does not exclude the use of traditional, offline means of communication. This platform is restricted to proceedings conducted under the auspices of the ICC. NetCase constitutes neither an arbitral procedure in itself nor a stand-alone service for dispute resolution, but merely a way to facilitate communication and organization between the parties and the arbitrators by offering instantaneous information 24 hours a day.[171]

[Rz 216] The NetCase environment provides security and confidentiality, speed, organization, accessibility, private forums and cost savings.

- Security and confidentiality: all communications and documents traveling between the user´s browser and NetCase are encrypted. Before accepting documents for posting, NetCase first automatically checks them for viruses and refuses any infected document. In addition, access to NetCase is password-protected.

- Speed: documents are available to all participants as soon as they are posted on NetCase. In addition, documents are transferred as quickly as by e-mail, with the advantage of a secured environment.

- Organization: all information and documents are organized in a uniform manner (as correspondence, memoranda, procedural orders, Terms of Reference or award(s)[172]) in order to lessen the risks of confusion and conflict that can arise from multiple filing systems. The origin of the documents is indicated so as to make

them easily identifiable,[173] and all submissions and exchanges are tracked to help participants follow the chronology of a case.[174] The system accepts pdf and tiff formats.

- Uniformity: NetCase allows all participants to view the same content at the same time in the same display form and environment.

- Accessibility: NetCase is accessible anywhere, anytime, using the Internet, regardless of the browser and operating system used. Users are thus be able to consult the documents posted on NetCase or information on the status of proceedings 24 hours a day using any computer simply by logging in with their ID and password. In addition, message alerts inform participants when a new message or document has been posted on NetCase.

- Private forums: these allow participants to communicate in an access-restricted environment that is more secure than the exchange of unprotected e-mails. Furthermore, within the forum, more restricted rooms may be created that can be accessed only by specified participants in the proceedings, e.g. the arbitrators, or one party and its counsel, or the arbitrators and the arbitral institution.

- Cost savings: by allowing the electronic exchange of documents, NetCase reduces the costs of preparing, handling and sending hard copies, although it does not completely eliminate the need for them, as national legal requirements may require some communications, such as the notification of an award, to be sent by traditional mail.[175]

[Rz 217] The NetCase platform offers a number of functions, including:

- An address book containing the details of all participants, including those of the Secretariat team in charge of the case.

- General information giving an overall picture of the case, with party, counsel and arbitrator names, the chronology of the proceedings (including dates of different stages of the case)[176] and a financial overview. Specific sections relating to the various aspects of the case (arbitral tribunal,[177] finance,[178] expert witnesses,[179] and forums) contain more detailed information.

- A calendar of the proceedings with the deadlines fixed by the Secretariat or the arbitral tribunal.[180]

- Assistance in the form of an e-mail address at which participants can contact the Secretariat for help, and guidelines explaining the different sections and the system as a whole.[181]

[Rz 218] In its first version, the NetCase platform still has some limitations, which are intended to be removed in future versions:

- Language: the use of an extensible markup language format (XML)[182] has been set aside for the time being due to compatibility issues. The first version uses HTML format in English and French, and future versions could be proposed in German and Spanish and even in other languages.

- Search function: the initial version does not incorporate a search function since it requires a complex work of compilation, updating and listing of keywords. This function may be included in a future version when the optical recognition of characters improves.

- Digital signatures: there is no uniformity regarding this issue because of varying national legislations. However it is recommended that parties discuss this issue if they want to use digital signatures.

- Digital certificates: similarly, there is no uniformity concerning the entities authorized to provide digital certificates and the kind of information they must contain.[183]

2. AAA – WebFile

[Rz 219] The American Arbitration Association (AAA) provides an online service, AAA WebFile, that allows users to file claims online and to «make payments, perform online case management, access rules and procedures, electronically transfer documents, select neutrals, use a case-customized message board,» and check a case´s status. [184]

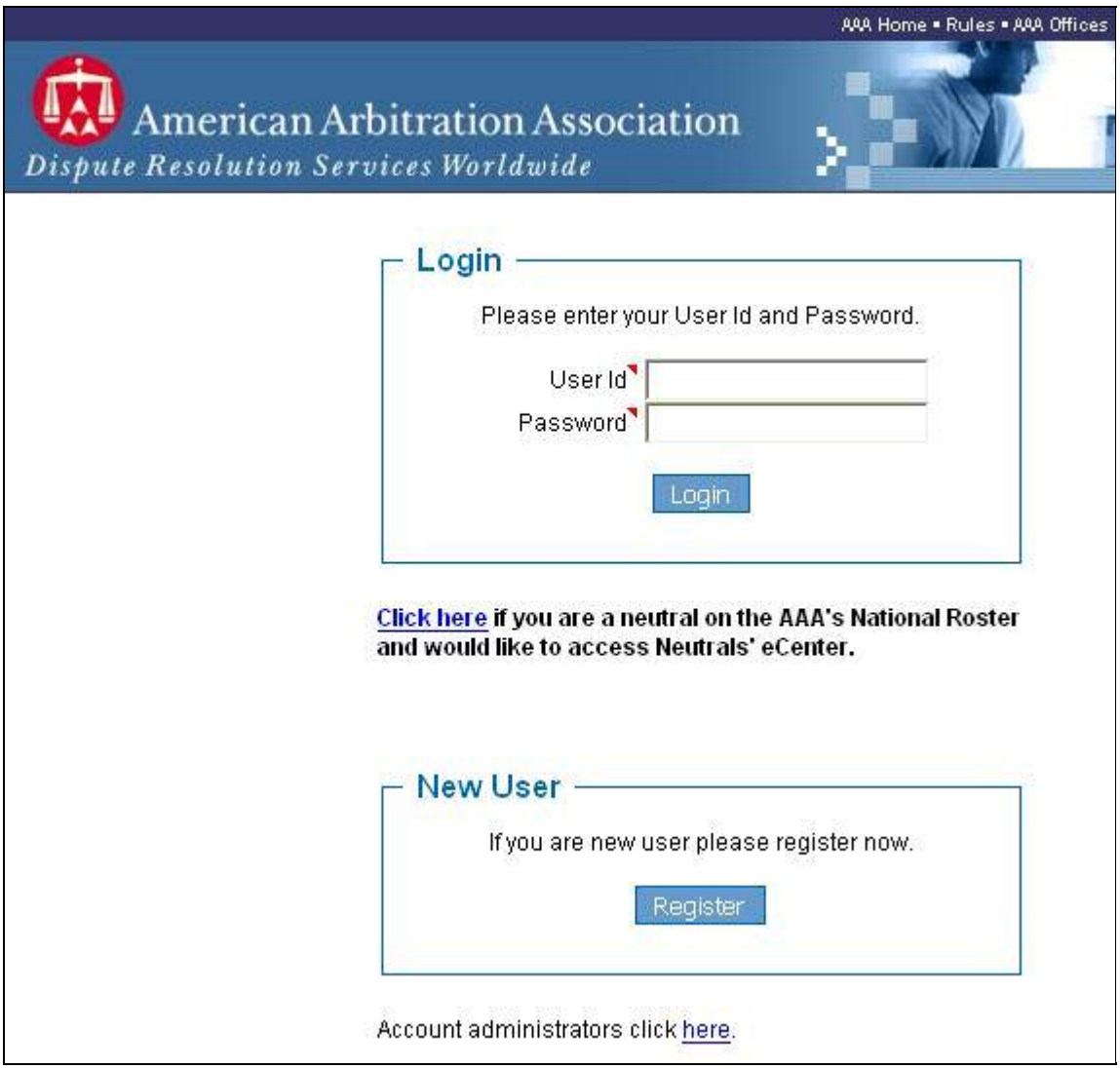


Fig. 1: Log-in screen

[Rz 220] To use the service, parties must complete a registration form and select a password in the «Online Filing» section of AAA´s web site. [185] The username and password enable the parties to file an online claim and later return to view and manage the cases he/she has already filed with AAA. [186]

[Rz 221] Filing a claim online involves the following steps:

1. Selecting who is filing the claim: the claimant or his representative.[187]
2. Selecting the set of rules to apply and the type of dispute resolution procedure (arbitration or mediation). [188]
3. Reviewing the agreement upon which the dispute is based, and confirming that AAA is named in the arbitration or mediation clause.[189]

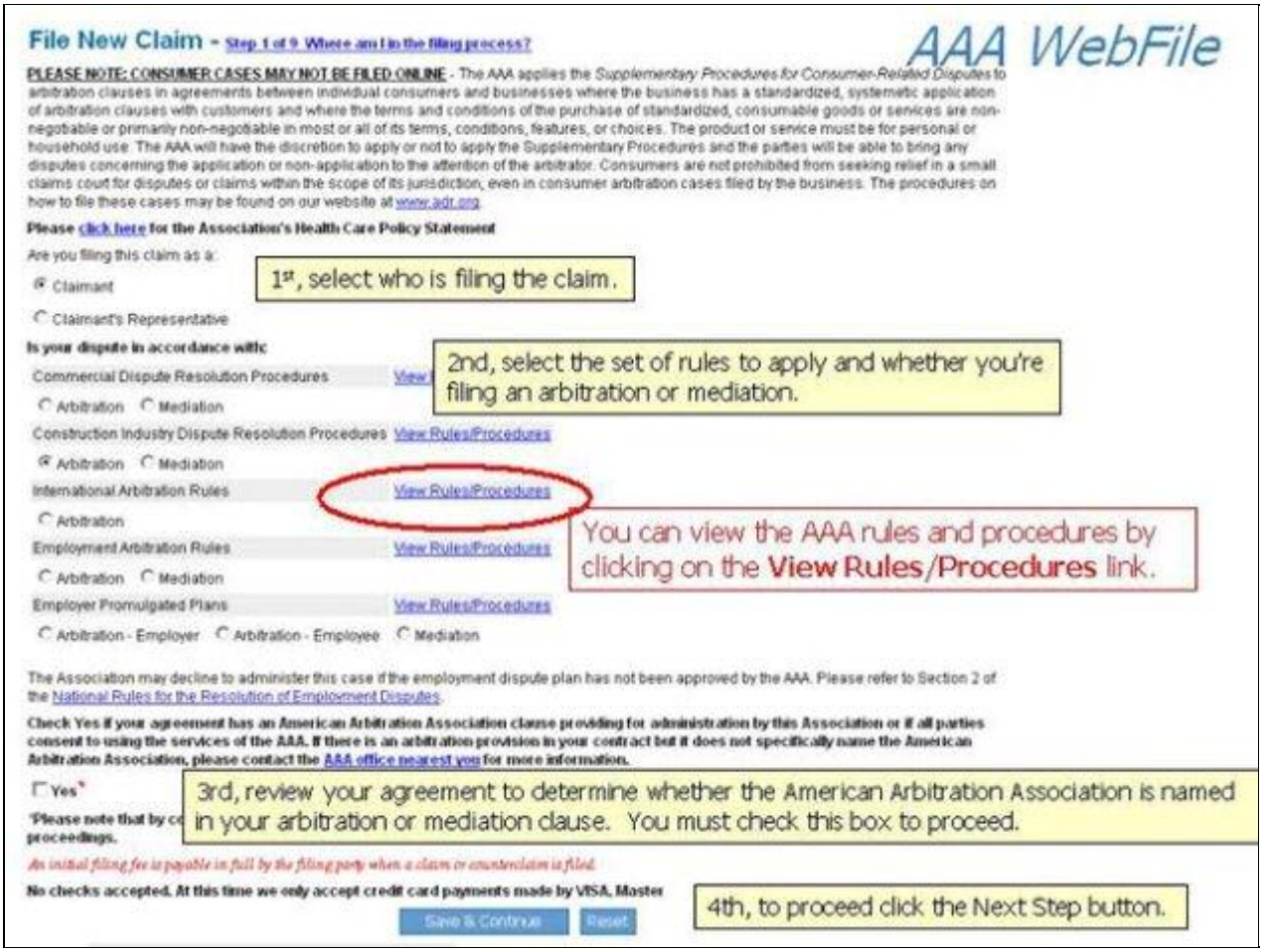


Fig.2: Filing a claim

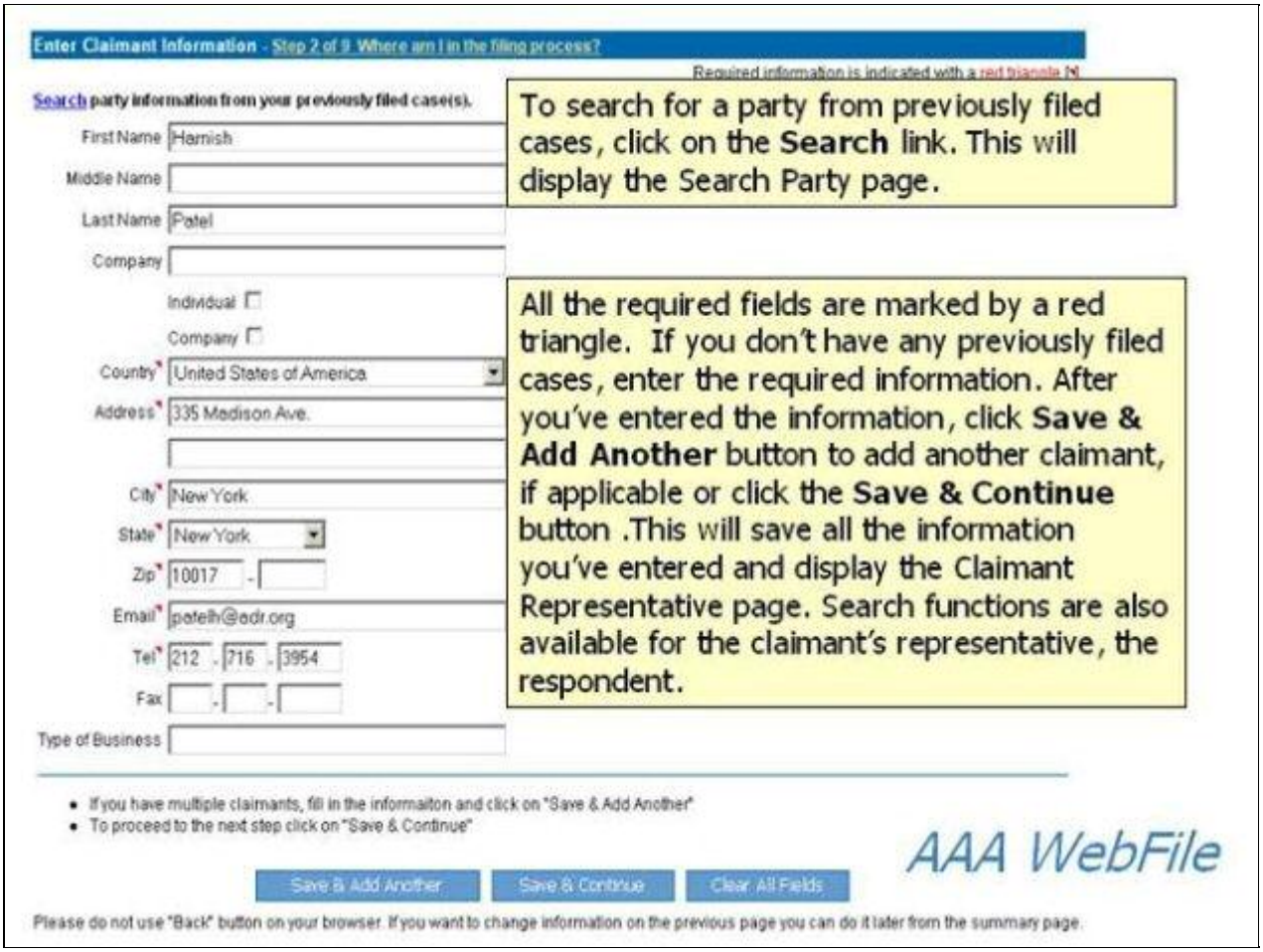


Fig.3: Entering claimant information.

1. Providing information about the claimant. The user can search for a party from a previously filed case, and has the option of adding more claimants if necessary.[190]
2. Providing information about the claimant´s representative. This page may be left blank if there is no representative. The user can add representatives for all the claimants involved if there is more than one.[191]
3. Giving information about the claim, including the claim amount and claim details. This step also allows the user to select the number of arbitrators and the place of the hearing, and to enter the arbitration clause.[192]

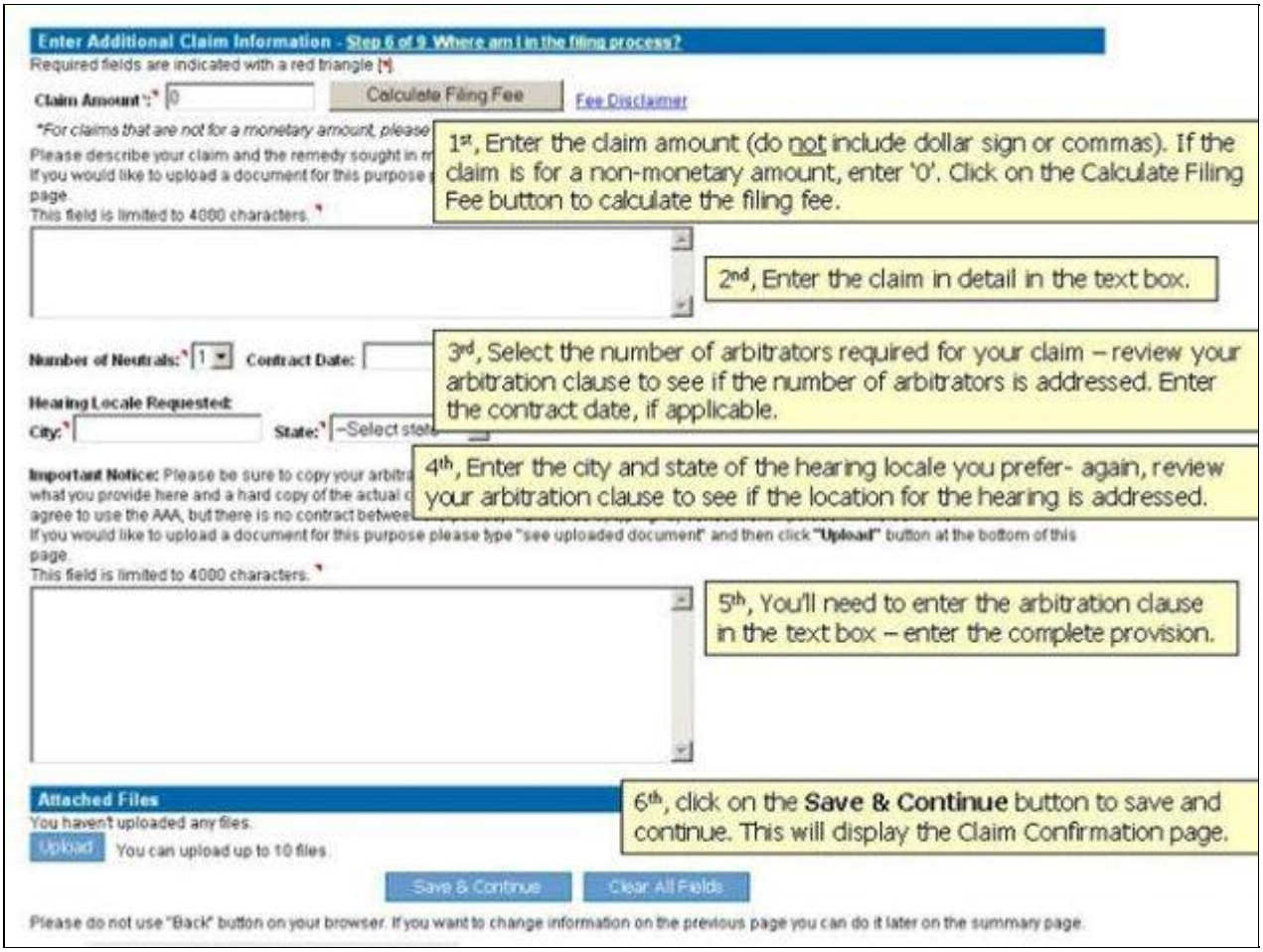


Fig.4: Additional claim information page

1. Calculating the initial administrative fee. This can be done even before the claim is completed.[193] A claimant must pay an initial administrative fee when he files a new claim. The amount of the fee varies depending upon the type of dispute and the amount of the claim. Additional fees may also be charged. Users are notified by the case manager of any additional fees.[194]

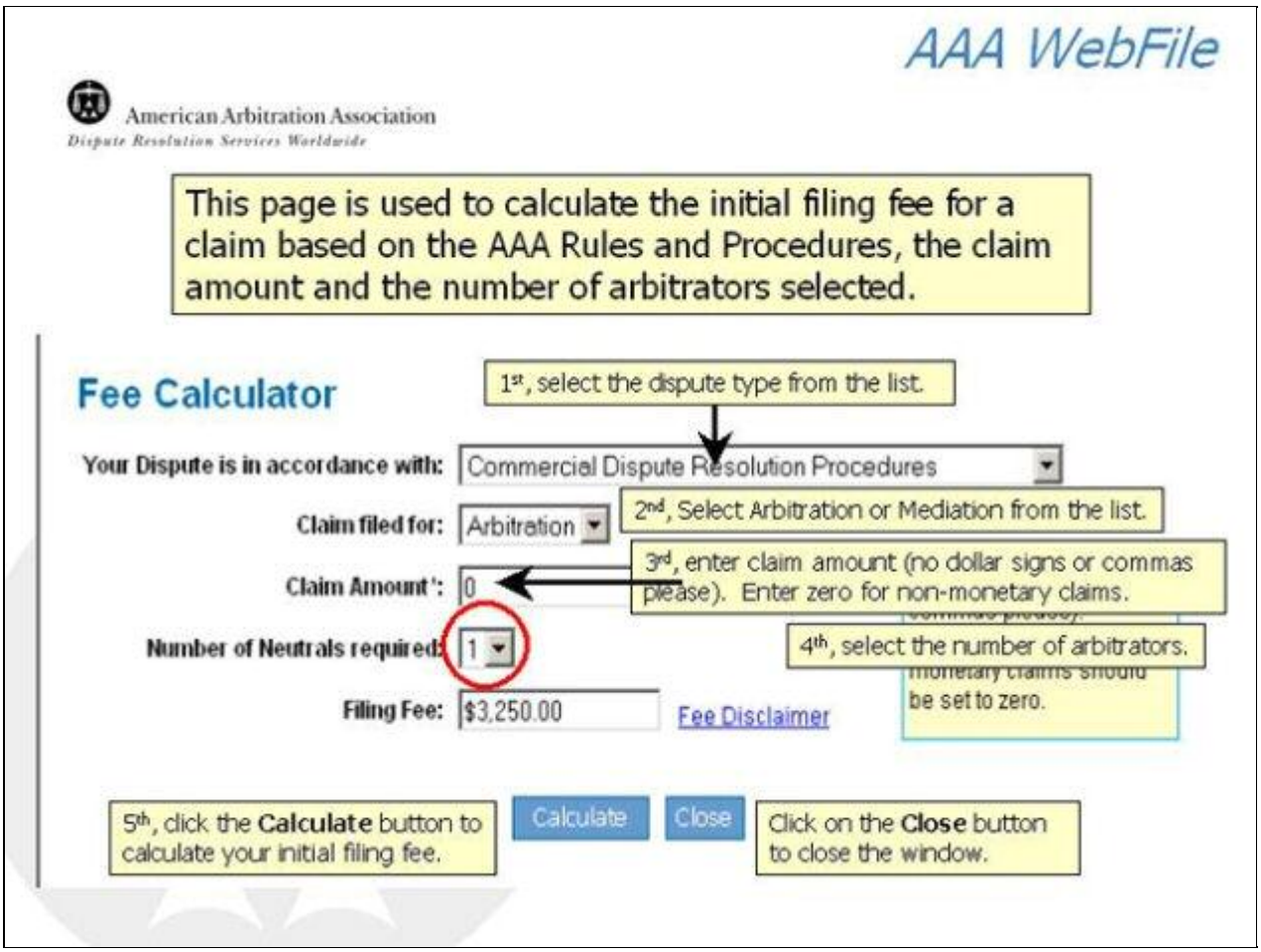


Fig. 5: Fee calculator

2. Printing the claim summary page containing the claim confirmation number.[195]

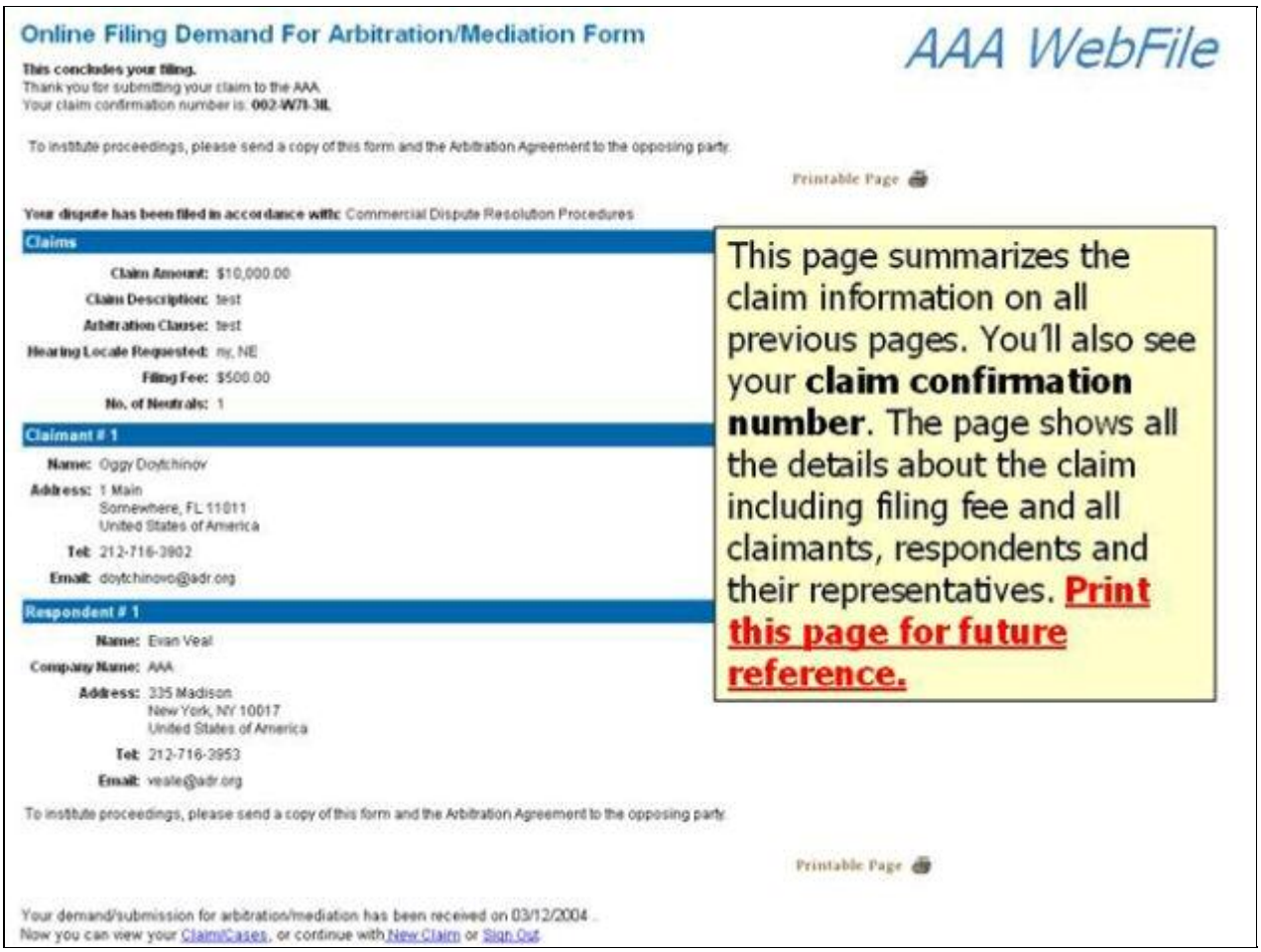


Fig. 6: Claim summary page

3. Completing the payment form.[196] The website accepts credit card payments only. Payments may be made by check if the user prints the «Summary» page and mails it with the check to the nearest AAA office.[197]

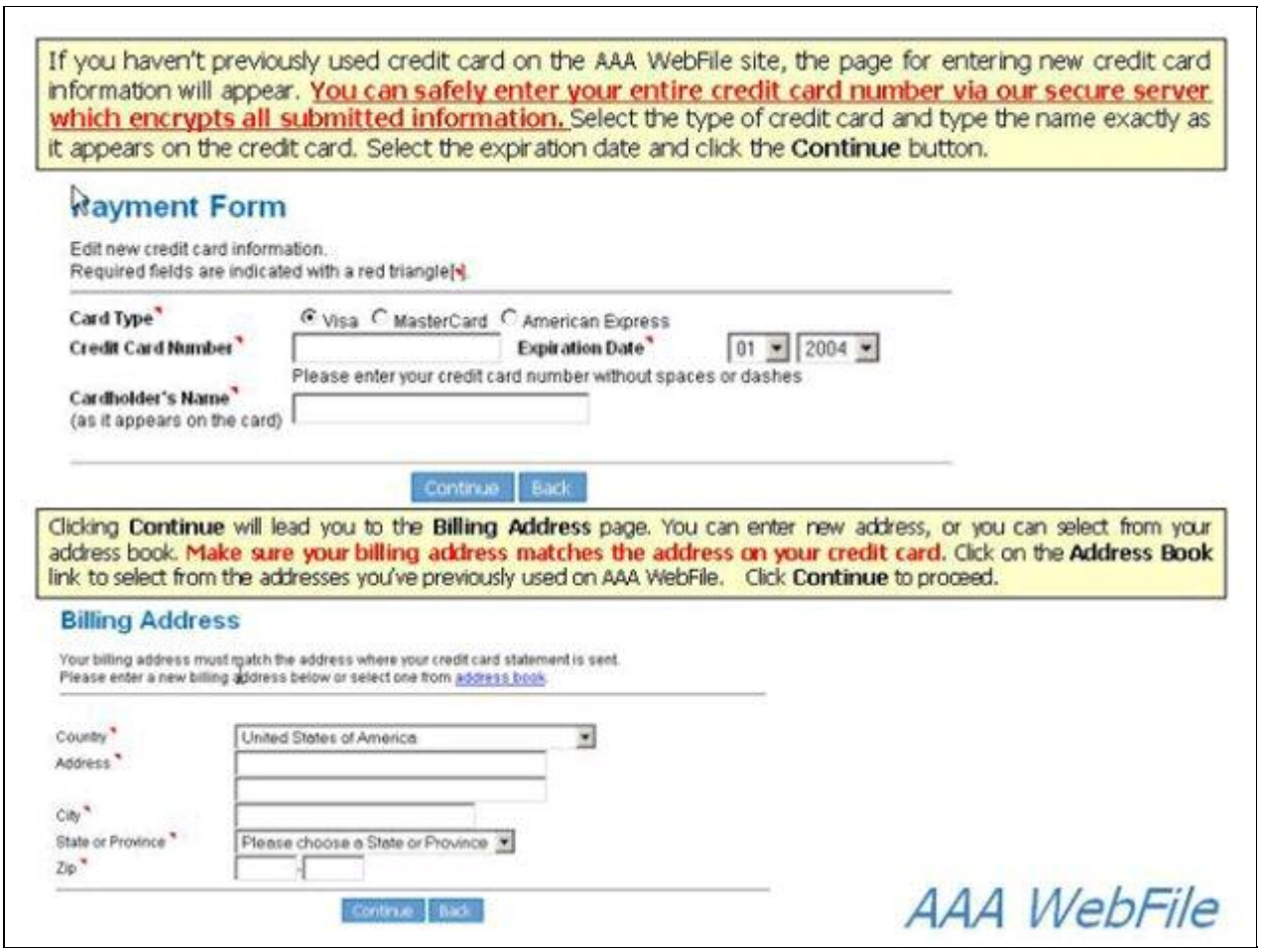


Fig 7: Payment form

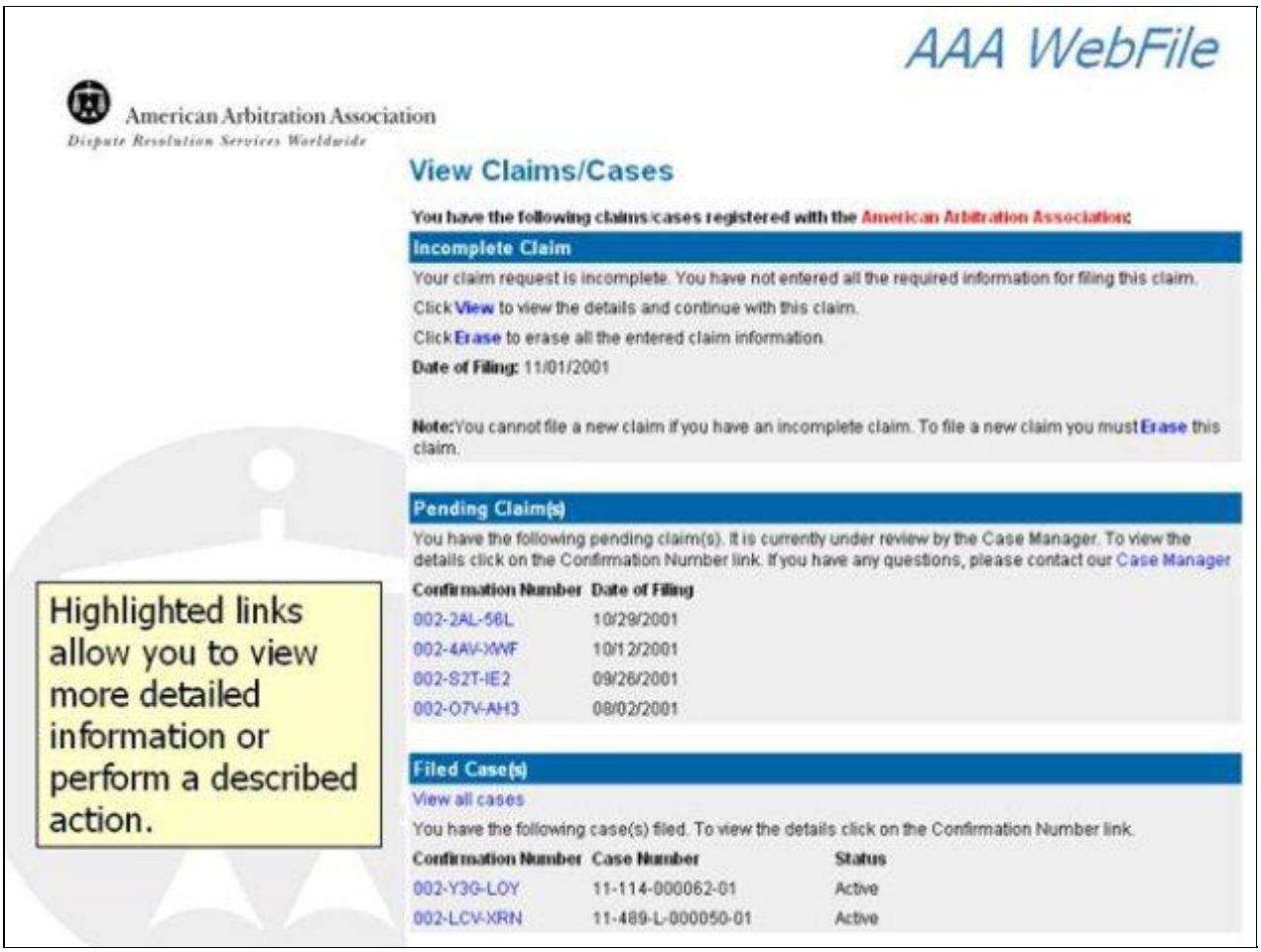


Fig. 8: Screen summarizing incomplete and pending claims and filed cases

[Rz 222] After a claim has been filed online, the user receives a confirmation number from AAA WebFile via e-mail, and the claim is listed under «Pending Claims» in the «View Claims/Cases» page of the WebFile site. A case manager then reviews the claim and notifies the user by e-mail if it is approved, usually within 2-3 days.[198]

[Rz 223] Users can review the claims they have filed in the «View Claims/Cases» page of the website. This page lists incomplete claims (when the user has not provided all the information required for filing), pending claims, and filed cases (claims filed by the user that have been approved by a case manager). Only incomplete claims can be modified.[199]

[Rz 224] Once a claim has been filed and approved by a case manager, a list of neutrals will be prepared and can be accessed by a link from the «Filed Case Information» page.[200] The user can view the curriculum vitae of the neutrals, rank them, and submit his selection to AAA. [201]

[Rz 225] Participants can also consult hearing information from the «Filed Case Information» page. If necessary, a user can submit an online request to postpone a hearing. [202]

[Rz 226] Other tabs on the «Filed Case Information» page allow participants to consult information about claims filed and the parties, as well as upload and review documents submitted in the course of the proceedings. [203]

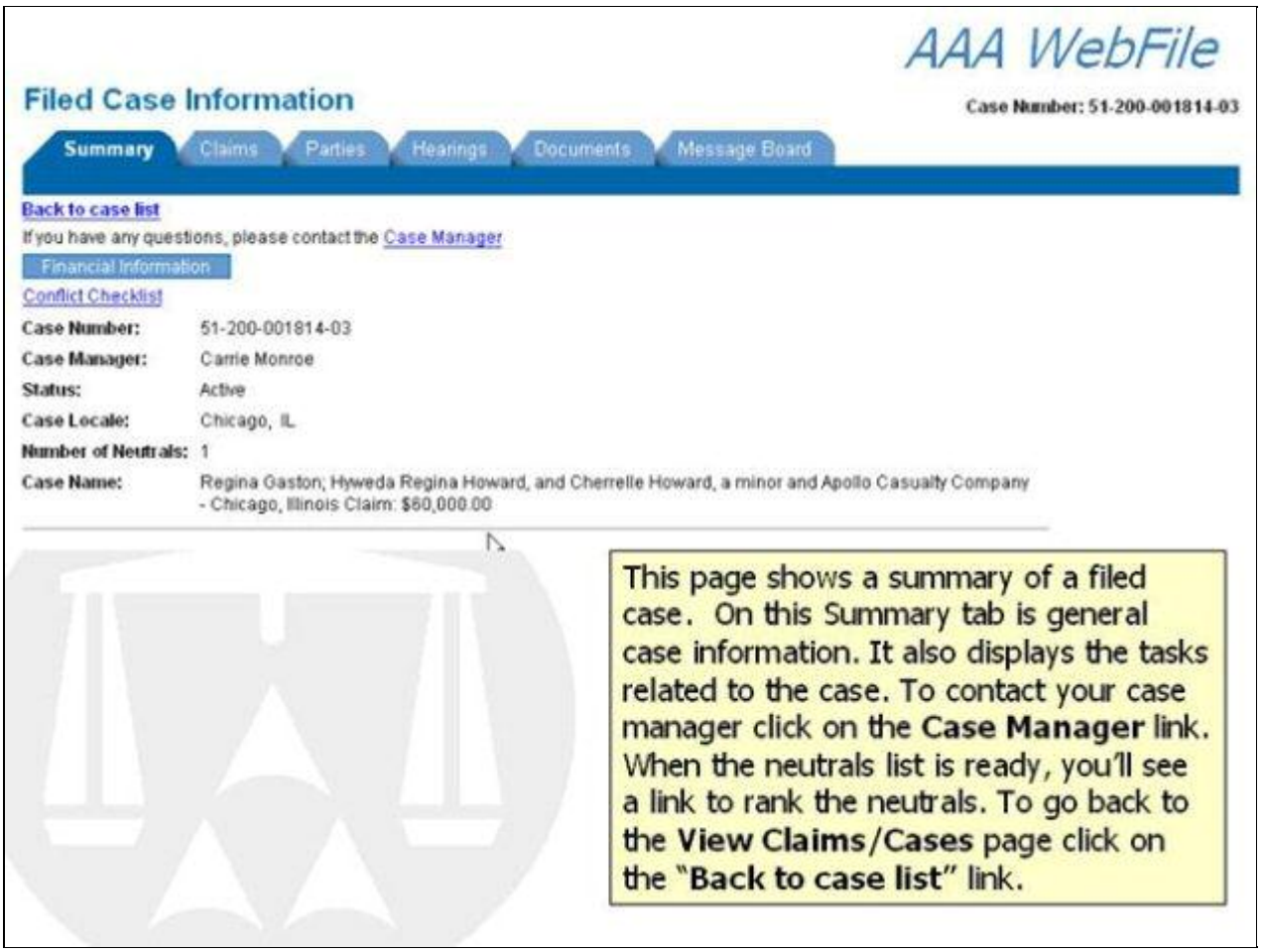


Fig. 9: Filed case information

[Rz 227] Finally, the AAA WebFile site provides a message board where the case manager posts non-urgent messages about a case. Only the case manager, the parties and the neutral(s) involved in a case can access the message board for that case.[204]

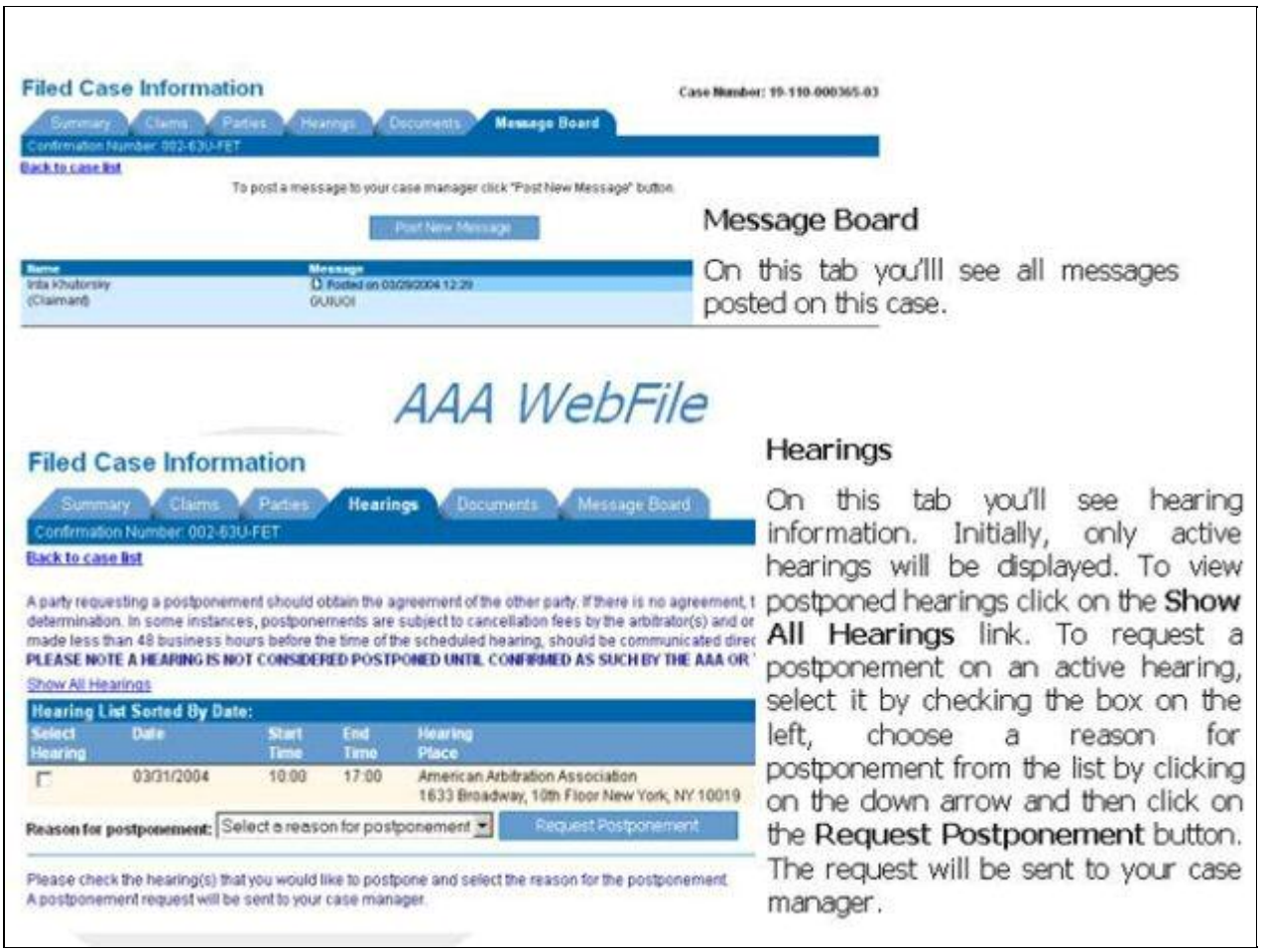


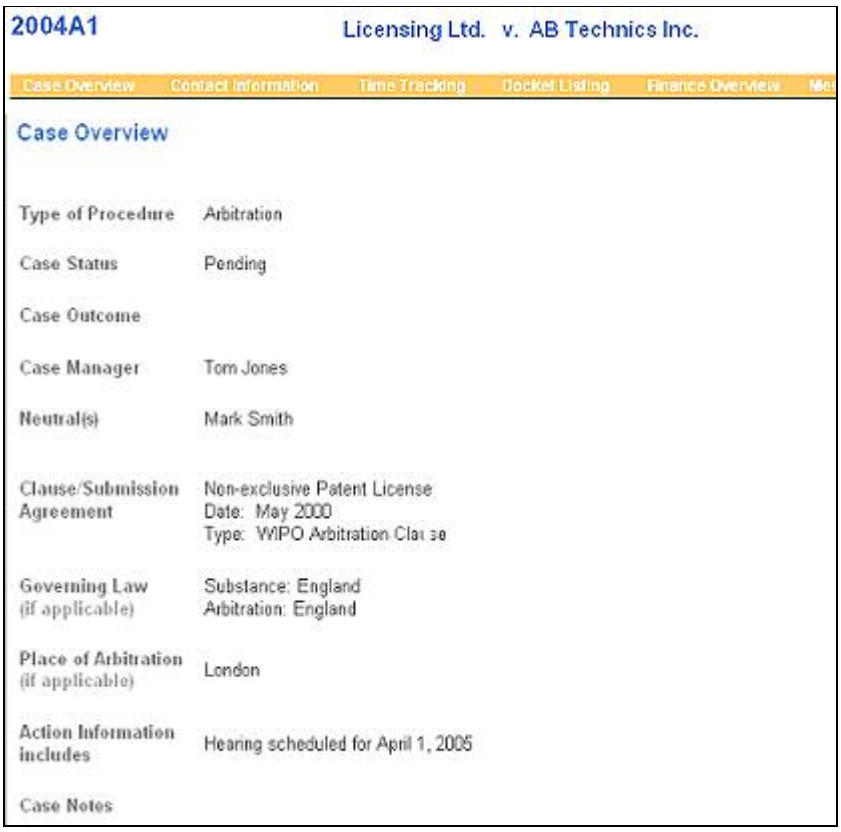
Fig. 10: Message Board

3. WIPO – ECAF

[Rz 228] The Arbitration and Mediation Center («the Center») of the World Intellectual Property Organization (WIPO) was created in 1994.[205] Its role is to assist in resolving private international commercial disputes by providing Alternative Dispute Resolution (ADR) services including mediation, arbitration, expedited arbitration, and mediation followed by arbitration («med-arb»). Many of the cases administered by the Center deal generally with disputes related to intellectual property, in the areas of technology and entertainment in particular.[206]

[Rz 229] The Center recently created a secure web facility for use in its proceedings, which seeks to facilitate the conduct of cases under the WIPO Mediation, Arbitration and Expedited Rules. This facility, the WIPO Electronic Case Facility (ECAF), enables parties, the arbitral tribunal and the Center to file, store, and retrieve case-related submissions electronically. It is secure and allows for access from anywhere in the world using the Center´s website. It takes the form of a case management system, a central database accessible via the Internet that allows participants in a case to submit documents online and to access a case overview, contact information, time tracking, docket listing, a finance overview, and a message board.[207]

[Rz 230] The ECAF´s Case Overview page provides basic information about a case, such as its status, the type of dispute clause or submission agreement, the governing law and the place of arbitration, and upcoming action in the case.[208] (Fig 1)



2004A1 Licensing Ltd. v. AB Technics Inc.

Case Overview | Contact Information | Time Tracking | Docket Listing | Finance Overview | Me

Case Overview

Type of Procedure	Arbitration
Case Status	Pending
Case Outcome	
Case Manager	Tom Jones
Neutral(s)	Mark Smith
Clause/Submission Agreement	Non-exclusive Patent License Date: May 2000 Type: WIPO Arbitration Clause
Governing Law (if applicable)	Substance: England Arbitration: England
Place of Arbitration (if applicable)	London
Action Information includes	Hearing scheduled for April 1, 2005
Case Notes	

Fig. 1: Case overview page

[Rz 231] Contact information for all participants is available on the Contact Information page.[209] (Fig. 2)

2004A1 Licensing Ltd. v. AB T

Case Overview | Contact Information | Time Tracking | Docket Li

Contact Information

Case Manager: Tom Jones

Arbitration and Mediation Center
World Intellectual Property Organization
34, chemin des Colombettes
P.O. Box 18
1211 Geneva 20
Switzerland

Telephone: +41 22 338 8247
Fax: +41 22 740 3700
Email: arbiter.mail@wipo.int

Claimant/Requesting Party: Licensing Ltd.

Contact person: None

High Street
New York
United States of America

Telephone: +1 (020) 1111 1111
Fax: +1 (020) 1111 2222
Email: email@xyz.com

Claimant/Requesting Party Authorized Representative(s)

John Doe
John Doe Law Firm

Broad Street
New York
United States of America

Telephone: +1 (020) 123 4567
Fax: +1 (020) 123 7890
Email: doe@doe.com

Respondent/Other Party: AB Technics Inc.

Contact person: Jane Smith

Main Street
Utrecht
The Netherlands

Telephone: +31 (0)12 123 1234
Fax: +31 (0)12 123 1111
Email: smith@abtechnics.com

Respondent/Other Party Authorized Representative(s)

Mary Jane Arnold; Sophie Cloakville
Mary Jane Arnold Law Firm

Central Square
Utrecht
The Netherlands

Telephone: +31 (0)12 333 3333
Fax: +31 (0)12 333 4444
Email: cloakville@arnoldlaw.com

Neutral(s)

Role : Sole Arbitrator

Mark Smith (Profile)

Partner
Smith & Associates

Main House
London
United Kingdom

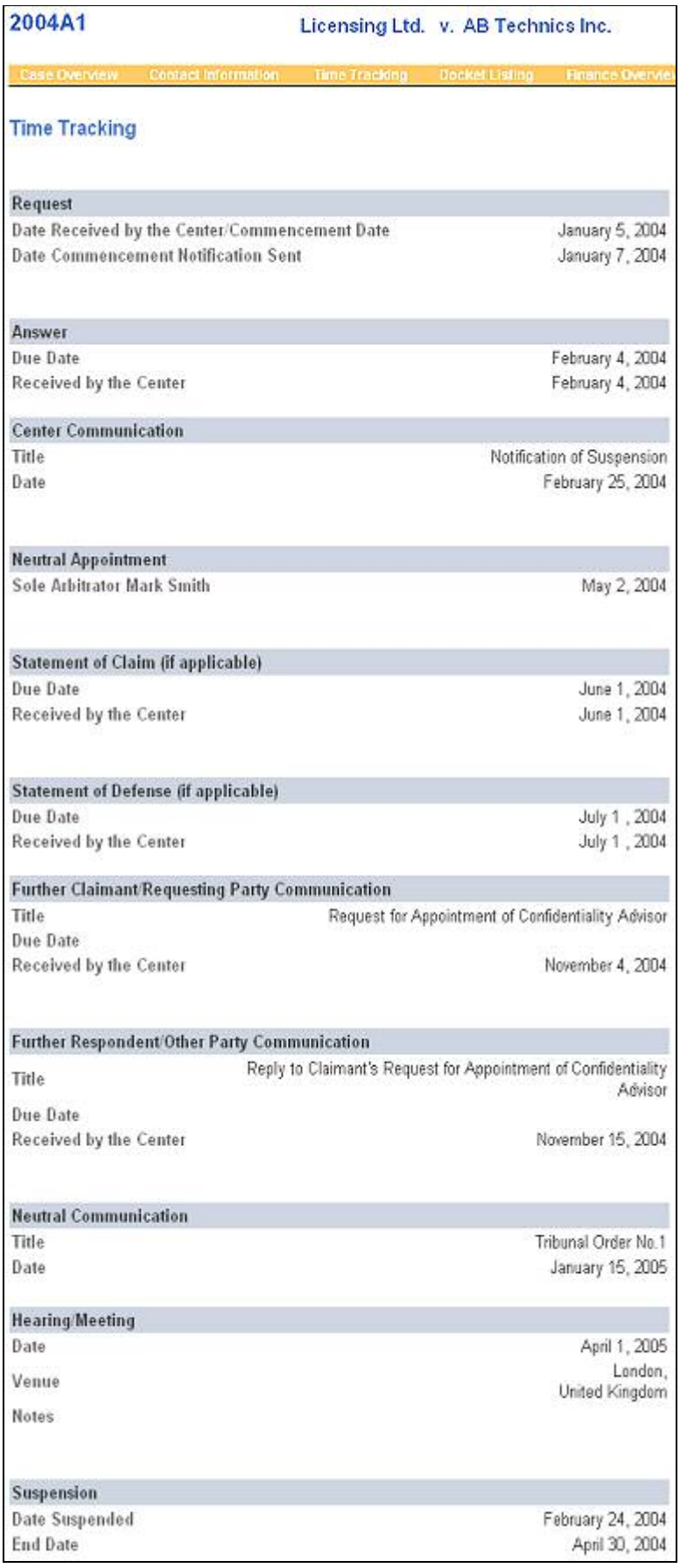
Telephone: +44 (0)20 444 4444
Fax: +44 (0)20 444 5555
Email: smith@smithassociates.com

Contact Information Notes

Please note that the Arbitrator's phone number will change to + 44 (0)20 55

Fig. 2: Contact information page. It includes information about the case manager, the claimant, the respondent, and other persons involved.

[Rz 232] The Time Tracking page serves as an informal agenda of the important dates in the case. [210] (Fig. 3)



2004A1 Licensing Ltd. v. AB Technics Inc.

Case Overview | Contact Information | Time Tracking | Docket Listing | Finance Overvie

Time Tracking

Request	
Date Received by the Center/Commencement Date	January 5, 2004
Date Commencement Notification Sent	January 7, 2004
Answer	
Due Date	February 4, 2004
Received by the Center	February 4, 2004
Center Communication	
Title	Notification of Suspension
Date	February 25, 2004
Neutral Appointment	
Sole Arbitrator Mark Smith	May 2, 2004
Statement of Claim (if applicable)	
Due Date	June 1, 2004
Received by the Center	June 1, 2004
Statement of Defense (if applicable)	
Due Date	July 1 , 2004
Received by the Center	July 1 , 2004
Further Claimant/Requesting Party Communication	
Title	Request for Appointment of Confidentiality Advisor
Due Date	
Received by the Center	November 4, 2004
Further Respondent/Other Party Communication	
Title	Reply to Claimant's Request for Appointment of Confidentiality Advisor
Due Date	
Received by the Center	November 15, 2004
Neutral Communication	
Title	Tribunal Order No.1
Date	January 15, 2005
Hearing/Meeting	
Date	April 1, 2005
Venue	London, United Kingdom
Notes	
Suspension	
Date Suspended	February 24, 2004
End Date	April 30, 2004

Fig 3: Time tracking page

[Rz 233] Participants can submit communications electronically into an online docket (the «Docket Listing» page). The other participants are then automatically notified of these submissions via e-mail and may also view and search the docket at any time. The online docket can also be used to record submissions made in hardcopy outside ECAF. Information received is organized in a searchable format. [211] (Figs. 4 and 5)

2004A1 Licensing Ltd. v. AB Technics Inc.

Case Overview | Contact Information | Time Tracking | Docket Listing | Finance Overview

Docket Listing

Only documents to be recorded as part of the casefile should be submitted in the Docket.

Search Docket

To sort, you may click on the column headers

Item No	Submitted By	Date	Subject
7	John Doe Claimant Representative	23/02/05 14:52:51	Claimant's Reply to Response
6	Sophie Cloakville Respondent Representative	23/11/04 17:10:02	Comments re: Confidentiality Advisor
5	John Doe Claimant Representative	22/11/04 14:52:24	Proposals re: Confidentiality Advisor
4	John Doe Claimant Representative	14/05/04 17:16:46	Mark Smith
3	Sophie Cloakville Respondent Representative	14/05/04 17:13:50	Answer to Request for Arbitration
2	Tom Jones Case Manager	14/05/04 17:09:56	Acknowledgment of Receipt of Request
1	John Doe Claimant Representative	14/05/04 16:59:10	Request for Arbitration

Fig. 4: Docket listing pages.

[Rz 234] ECAF´s Finance Overview page provides participants with an informal tool to review the case fees due and received.[212] (Fig. 5)

2004A1 Licensing Ltd. v. AB Technics Inc.

Case Overview | Contact Information | Time Tracking | Docket Listing | Finance Overview | Me

Finance Overview

Registration Fee

Claimant/Requesting Party

Amount: 2,000 USD	Adjusted Total Amount:
Due Date: February 3, 2004	Due Date:
Amount Received: 2,000 USD	Amount Received:
Date Received: February 1, 2004	Date Received:
Payor: Licensing Ltd.	Payor:
Notes:	Notes:

Respondent/Other Party

Amount: 2,000 USD	Adjusted Total Amount:
Due Date: March 3, 2004	Due Date:
Amount Received: 2,000 USD	Amount Received:
Date Received: March 3, 2004	Date Received:
Payor: Mary Jane Arnold Law Firm	Payor:
Notes:	Notes:

Administration Fee

Claimant/Requesting Party

Amount: 2,000 USD	Adjusted Total Amount: 10,000 USD
Due Date: July 3, 2004	Due Date: December 3, 2004
Amount Received: 2,000 USD	Amount Received: 8,000 USD
Date Received: July 1, 2004	Date Received: November 25, 2004
Payor: Licensing Ltd.	Payor: Licensing Ltd.
Notes:	Notes:

Respondent/Other Party

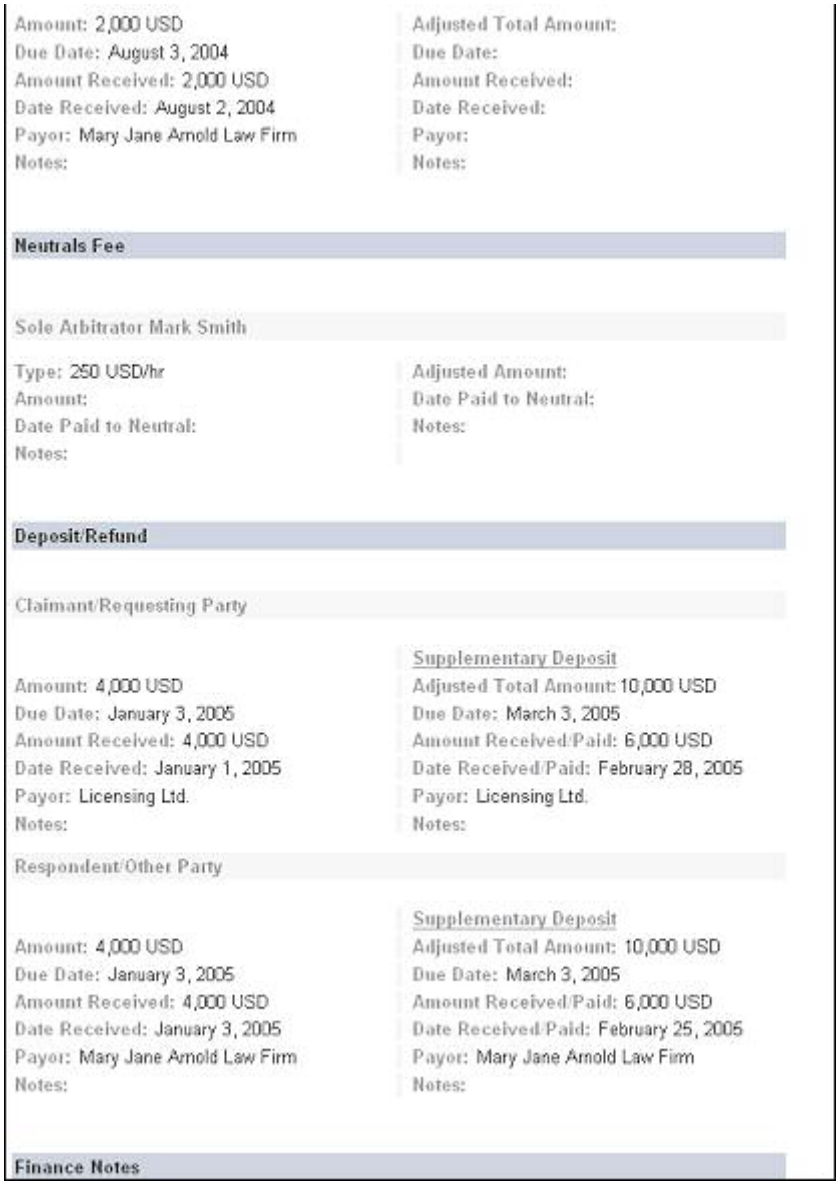


Fig 5: Finance overview page

[Rz 235] Participants can also communicate through ECAF´s message board, which is intended for communications that are not part of the case record. These messages are accessible to all participants using the system. [213] (Figs. 6 and 7)

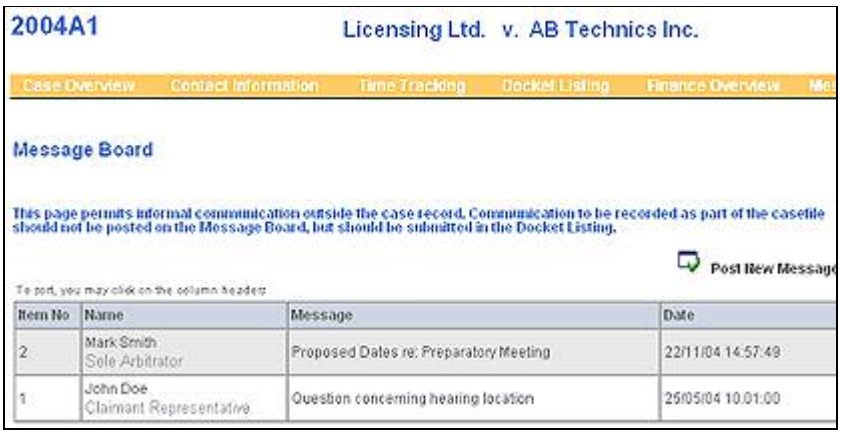


Fig 6: Message Board page

Fig 7: Posting a message on the Message Board

[Rz 236] With the exception of the docket listing and message board, all the pages in the ECAF are maintained and updated by WIPO´s Arbitration and Mediation Center. [214]

[Rz 237] Data security is ensured through a username, password and a changing passcode delivered by RSA SecurID card, a hand-held device that provides a different passcode every time a participant accesses the system. All information stored in ECAF is systematically firewall protected and encrypted by using Secure Socket Layer (SSL) technology.[215]

[Rz 238] The Center is currently developing a project for 2006–2007, which will adapt ECAF for use in the 32nd America´s Cup. Most of the disputes related to this sailing event are within the jurisdiction of the America´s Cup Jury (ACJ), a five-member ad hoc arbitral tribunal. IT provides obvious benefits for the ACJ, whose work is constrained by the fact that the five members of the ACJ reside on four different continents from the sometimes harsh time constraints of the issues to be solved, as in many sports contexts, moreover, as a rule ACJ proceedings involve all the twelve teams and the official bodies of the Cup, with the consequence that numerous submissions are addressed to numerous participants. The multiplicity of actors make san electronic filing facility particularly useful. [216] In addition to planning for ECAF, the ACJ is also contemplating the use of specific videoconferencing technologies.

[Rz 239] The WIPO Arbitration and Mediation Center also administers the domain name dispute resolution service, established in December 1999.[217] This service resolves mainly domain name disputes under either the Uniform Domain Name Dispute Resolution Policy (UDRP), for the .com, .net, .org, .biz, .info and .name domains, and other procedure, adapted from the UDRP for over 45 national domains (for instance, .fr, .ie, .nl, .ch). This domain name dispute administration service has IT features in its public online facilities, including model forms in Word format and online forms, online resources and acceptance of online communications. The service also provides IT case management support.

[Rz 240] WIPO online facilities seek to facilitate communication and organization in the resolution of international private commercial disputes. They are flexible and provide a choice of IT options. Ease of use and interoperability are key aspects. The facilities are based upon widespread existing tools, and are scalable so that new functions can be added over time.

II. The guidelines of the International Chamber of Commerce

[Rz 241] The ICC is one of the most important global players in the field of arbitration. In addition to the administering one of if not the largest number of international arbitration procedures in the world, the ICC is also a think tank for new developments in the field of dispute resolution. Further to developing the NetCase system, the ICC has issued a series of green papers followed by practice guidelines on the use of IT. Its work in this regard deserves to be mentioned here. This section starts with a short summary of the ICC´s main report on IT, and then reviews in more detail its practical recommendations.

1. Report by the ICC Section on IT on Special IT Requirements in International Arbitration

[Rz 242] The overall objective of the ICC Section on Information Technology is «to address the relevant possibilities and risks resulting for international commercial arbitration from (a) the deepening penetration of access and use of IT by arbitration users and (b) the increase of information transmission and processing capabilities of IT.» [218]

[Rz 243] In March 2002, the ICC Section on IT issued a preparatory paper considering the role of the ICC in encouraging the use of IT in international arbitration.[219] This paper addressed a series of underlying considerations which led to the actual guidelines issued by the ICC. Such considerations are presented in the next section.

[Rz 244] The paper reviews the uses of IT in international arbitration, the most obvious of which is the «formal exchange and manipulation of data within any single arbitration process» [220] through physical storage media, e-mail and shared access to a website (e.g., a virtual case room). [221] It emphasizes that the use of IT has the potential to greatly increase the efficiency of international arbitral proceedings in terms of speed, cost and ease of use of the information exchanged,[222] especially in the case of large submissions. [223]

[Rz 245] The report alsonotes that information technology can be used effectively during hearings: to present technical evidence[224] or to allow real-time collaboration through telephone conferencing, video-conferencing and through the production of electronic transcripts of the hearings. [225] It further mentions that IT also facilitates access to legal resources such as all types of legal texts as well as information on comparative law and practice. [226]

[Rz 246] The report goes on observing that information technology is not used widely yet in international arbitration. It suggests the following possible general reasons:

- the adversarial nature of arbitration;
- the difficulty of adopting a uniform approach when parties already have their own IT «habits»;
- the expense involved in maintaining and using the necessary IT infrastructure;
- lack of skills or willingness to use IT solutions;
- inadequacy of the legal environment related to the use of IT in international arbitration; and
- conservatism.[227]

[Rz 247] The report further identifies four types of more specific issues related to the actual use of IT in international arbitration:[228]

- *Technical issues*: they include technical compatibility (capability related to hardware, software, word-processed documents, spreadsheets, images, databases, specialist programmes, compression, encryption, electronic signatures, and information and document integrity),[229] the «lowest common technical denominator»,[230] and system failure.[231]

- *Inherent practical issues*: they include unique «project» characteristics,[232] confidentiality and security,[233] and other specific issues relating to the use of computerized data storage. [234]

- *Legal issues*: the principal legal issues relate to ensuring that the use of IT does not comprise the integrity of the arbitral proceedings.[235]

- *Financial issues*: they may arise in particular in relation to the allocation of additional expenses incurred by the

use of IT.

[Rz 248] On the basis of these factors and issues, the ICC developed guidelines on the use of IT to resolve business disputes; these guidelines are the topic of the next section.

2. Guidelines on «Using Technology to Resolve Business Disputes»

[Rz 249] In a special supplement to the Bulletin of the ICC Court of International Arbitration, the ICC Task Force on IT in Arbitration issued guidelines on «Using Technology to Resolve Business Disputes». This supplement provides a series of Operational Standards,[236] whose purpose is to provide standard, optional[237] solutions to facilitate the use of IT in international arbitration. The Standards are not procedural rules, and are intended to be adapted to each arbitration proceedings and modified as necessary.[238] They are only mandatory if they are expressly incorporated as procedural rules.[239] All, some or none of the Standards can be used.[240] It is suggested that they be referred to in the arbitration agreement, or adopted at the outset of the arbitration.[241] The following paragraphs summarize these standards.

A. General procedures

[Rz 250] The use of the Standards can be initiated by any party or the arbitral tribunal; this is done by transmitting the completed Initiation Form (a model of which is included in the annex to the supplement) to the other parties and to the members of the tribunal.[242] Each recipient should then complete the Form and send a copy to the other parties and to the members of the tribunal.[243] The Standards suggest that they be not be applied unless and until every party has acquired the necessary IT capacity, or if the parties agree on measures to overcome any such obstacle. The arbitral tribunal may also give instructions for the harmonization of the parties´ IT capacity.[244] In any case, the Standards state, that the parties´ final agreement as to the use of IT during the arbitration proceeding should be consolidated in writing.[245]

[Rz 251] The Standards further provide that any problem or incident with the application of the IT agreement, whether permanent or temporary, should be notified to the other parties and to the arbitral tribunal as soon as possible, using the so-called incident report form.[246] Once a problem is reported, the Standards suggest that each party take all reasonable measures to remedey the problem or prevent it from occurring again, and inform the other participants of the measures taken.[247] It is reminded that, in general, the parties should cooperate in good faith and use all reasonable efforts to remedy or overcome any obstacle or incident.[248]

[Rz 252] Finally, the Standards recommend consigning any modifications to the Standards in writing.[249] If the parties cannot agree on certain modifications, the arbitrators can make the modifications.[250]

B. Paperless files

[Rz 253] A second section of the Standards covers documents that are submitted to the arbitral tribunal or institution and copies of these documents provided to the other participants (i.e., the documents in an arbitrator´s file of the case).[251]

[Rz 254] This section applies if each participant agrees to convert all the documents it would normally submit in paper form into the agreed electronic format.[252] In this regard, wherever possible, each physical document should be converted into a single electronic document as identical to the original as possible, including pagination.[253]

[Rz 255] On the organization of files, it is recommended that the participants use a logical naming system for the files to identify the participant who submitted the file, the category of the file, and the file´s place in that category. The name and date of the original document should appear on the first page of the electronic document.[254] The parties can either agree on their own naming system,[255] or use the one proposed by the ICC.[256] The parties can also agree on a system for sharing structured information about the documents (e.g., a searchable document database).[257]

[Rz 256] All parties who submit electronic documents should retain the paper original at least until the end of the

arbitration proceeding, and longer if required by other rules or applicable law.[258] They should also use reasonable efforts to protect their own files from corruption, damage or destruction, and archive backup copies in a safe place.[259]

[Rz 257] On one point the Standards are overly cautious: they recommend that «paper» documents should not be exchanged in electronic format only, be it on CD or DVD, but rather in their original paper format, with a copy of all documents in electronic copy. The Standards further provide that if the first option is chosen nonetheless, the participants should verify that this is admissible under the applicable law, and then clearly state their choice in writing.[260] This may well be over-cautious. Of course, some documents, such as awards, should definitely be notified in paper form, but the vast majority of national arbitration laws do not set formal requirements on the exchange of briefs. The parties must be heard, in adversary proceedings, and be treated equally, but this does not in itself imply that the communications be made in paper form[261].

[Rz 258] Lastly, the Standards recommend that, upon receiving any submission in electronic format, each participant should always verify that they can open and read the file. If not, they should immediately issue an incident report form. The participant who provided the file should investigate the problem promptly and provide a replacement file within 7 working days.[262]

C. Electronic communications

[Rz 259] Electronic communications may take place either by e-mail or, now that itis operational, through the use of the NetCase system accessible via Internet. Other ad hoc virtual case rooms may also be used.[263] If the parties decide to communicate via e-mail, each participant is required to save, both electronically and in paper form, the e-mails he sends and receives in the context of the arbitration proceedings. These must be saved for a reasonable time period after the end of proceedings.[264]

[Rz 260] Most likely in order to minimize the risk of virus transmission and to maximize compatibility, the Standards suggest that e-mails should be sent in ASCII format rather than HTML. The e-mails should include a clear reference to the case as well as the date, the name and the postal address of the sender. Any attachments should be listed in the body of the e-mail.[265]

[Rz 261] The Standards address one interesting point, which is often left out of negotiations on the use of IT: the frequency with which e-mails are retrieved. Under the Standards, the participants must check their e-mail inbox at least once every two working days.[266] In order to ensure non-repudiation, the Standards further judiciously require the participants to generate manually an acknowledgement of receipt of the e-mails which includes the entire text received.[267] Moreover, if an acknowledgement of receipt has not been received within two days, the participant expecting the receipt is advised to issue an incident report form.[268] The sender will then retransmit the message via e-mail or by another reliable method.[269]

[Rz 262] The parties may wish to use encryption or electronic signatures to protect the confidentiality and authenticity of their e-mail communications.[270] After discussion, they should draw up an agreement that can be implemented after approval by their counsel.[271]

[Rz 263] Participants in the arbitration proceedings may also wish to communicate using a virtual case room accessible via the Internet.[272] This case room should be hosted by a neutral entity controlled by all the parties, or, preferably, by the arbitral tribunal or institution: preferably the NetCase system. The selected case room should be set up so as to track the participants´ access, and records of access should be available to all participants during the arbitration proceeding and for a period thereafter.[273] Furthermore, each participant should be able to post messages in the case room, with or without attachments.[274] Here again, all participants should visit the case room at least once every two working days.[275]

a. Videoconferences

[Rz 264] If the participants agree to use videoconferences, the Standards suggest that the arbitral tribunal, after consultation with the parties, issue instructions on the logistics of the videoconference, including the timing of the video-conference, the sites used, the participants, and any special needs. It is essential that these instructions be

issued sufficiently in advance of the videoconference.[276]

[Rz 265] The participants´ designated technicians should then confer to determine whether the participants have the necessary equipment or whether external resources are needed, what the anticipated costs would be and how these costs should be allocated.[277] All this information should be memorialized in a protocol which must be approved before implementation.[278]

[Rz 266] Any technical problems should be notified to the sole arbitrator or president of the arbitral tribunal as quickly as possible.[279]

b. Audioconferences

[Rz 267] If the parties have agreed to use audioconferencing, the Standards suggest that, after consultation with the parties, the arbitral tribunal issue instructions, just as for videoconferencing, on the organization of the conference, including timing, identity and connection of participants and any special needs. Here too, it is important that these instructions are issued sufficiently in advance of the audioconference.[280]

[Rz 268] The audioconference should be led by the single arbitrator or the president of the arbitral tribunal, who verifies that all participants are properly connected. Each participant will then introduce himself before speaking and should not disconnect before the audioconference is declared finished.[281]

[Rz 269] Any technical problems should be notified to the single neutral or president as soon as possible.[282]

CHAPTER 4

AVAILABLE IT TOOLS FOR ARBITRATION PROCEEDINGS

[Rz 270] This chapter reviews the two main IT tools that may be used in arbitration proceedings, namely case management websites and videoconferencing. The emphasis is placed on videoconferencing, which raises a many more questions than case management websites. The latter is relatively complex to set up from a technological point of view, a topic beyond the scope of the present study, but earlier to use. This chapter also presents an innovative technology: shared virtual environments, which are not currently used, but may constitute a future direction for the use of IT in arbitration. For each of these technologies, we first describe the technology and, if applicable and not described elsewhere in this study, specific uses or experiments made of the technology. Thereafter, the use of these technologies is assessed, compared to technologies and other ways to communicate and interact in the context of arbitral proceedings. Finally, certain recurring issues and concerns are discussed and solutions put forward.

[Rz 271] This chapter does not address the exchange of files on data carriers, i.e. CDs and DVDs. These show some of the typical advantages of IT tools, such as arranging files or linking them using hyperlinks between documents or specific locations in such documents (in this respect, physical data carriers even have an advantage over the electronic transmission of documents through e-mails for example, as in the latter hyperlinks pointing to files easily become unusable when transmitted from one computer to another), costs of transmitting data, portability, etc. This matter, however, does not deserve special consideration here, as it does not raise any particular legal issue. For a general introduction to the advantages of using data carriers, the reader may revert to the general considerations addressed in Chapter 1.

I. Extranets, case management websites, and virtual case rooms

[Rz 272] Quantitatively speaking, the most important communication technology for arbitration proceedings, apart from mere e-mails, is one that helps manage long and numerous documents conveniently and efficiently. For this purpose, different forms of applications have been developed, or rather imported and adapted from other business contexts. In substance, they all consist of a sophisticated website allowing users to upload, store, organize, and

retrieve documents and other files, and to post messages, share electronic agendas, and generally facilitate access to all information related to a specific case. These technologies, alternatively called extranets, case management websites, and virtual case rooms, may be either institutionally implemented (as in the cases of NetCase, WebFile, and ECAF) or provided for ad hoc. They share the same pros and cons, and raise the same issues.

[Rz 273] Hence, the following paragraphs first set out this general technology in more detail, explaining its operations and uses. This section then reviews the reasons for its use, i.e. the properties it offers and functions it fulfills. Finally, this section discusses the main issues and concerns it raises, aspects requiring special attention when utilizing it, and limitations imposed to respect the procedural rights.

1. Description

[Rz 274] This study does not differentiate between extranets, case management websites, and virtual case rooms. Although, the three notions may refer to three different concepts, in the present context they can be treated as one and the same. The distinction as well as the identity for arbitration purposes are discussed below.

[Rz 275] Extranets are basically private segments of the Internet or private spheres of cyberspace. Technologically, they are «web spaces» with secure aspects, which means they include firewall server management, means of user authentication (they may even issue and use digital certificates), and encryption of messages. They may also rely on virtual private networks (VPN), i.e. specific and exclusive connections that tunnel through the public network. For the rest, they use the networks that constitute the Internet (i.e. the public telecommunications system) and the same protocol for exchanging information (i.e. the Transmission Control Protocol/Internet Protocol, or TCP/IP). The purpose of an extranet is to share, in a private fashion, part of an entity´s information and operations with its members, as well as — this is what differentiates it from an intranet—with its suppliers, customers, and partners. An extranet is used as a common repository of shared data to which all authorized members have access over the Internet. The access to such shared data has in principle two goals: document management and scheduling. Document management includes retrieving and reviewing the latest version of documents from remote locations and, conversely, publishing documents firm-, project-, or client-wide. Scheduling consists of online calendaring and includes setting deadlines and posting reminders, scheduling meetings with lists of attendees, and monitoring the status of projects.

[Rz 276] Case management websites are basically extranets that are specifically designed for the management of a legal case. They serve two main purposes: (1) providing a universally accessible, but password protected, platform for document repository, and (2) constituting a web-based interface that allows users to communicate rapidly and securely. Typically, such websites are available to the parties, counsel, arbitrators, arbitral institution , and possibly with limited access, witnesses and experts. Access may be protected by passwords and possibly by any of the additional technologies just mentioned above for extranets. Case management websites have been used, for instance, in mass claims and multiparty proceedings. They provide to the numerous plaintiffs functionalities such as information sharing, claims screening, matter tracking, discovery management, patent/trademark management, and contract tracking.

[Rz 277] Virtual case rooms are case management websites that are more specifically dedicated to the actual resolution of a case. Other case management websites are generally designed to assist with the global management of the case, but not its actual resolution Consequently, virtual case rooms may include more sophisticated means of communication including for instance more developed bulletin boards, telephone conferencing facilities, or videoconferencing software.

[Rz 278] Extranets that are not used for case management are of no interest here and the discussion will thus be limited to extranet for case management, which are no different from case management websites.The distinction between case management websites and virtual case rooms is essentially a question of the degree of sophistication of the available means of communication. In practice, the distinction between these two last categories is not useful enough to be pursued in this study. Hence, the study will use the term case management website, without making a distinction between this notion and virtual case rooms.

[Rz 279] Several arbitral institutions provide case management websites. These include the ICC (NetCase) , the AAA (WebFile)[284], and WIPO (ECAF).[285]

2. Assessment of case management websites

[Rz 280] Case management websites offer myriad advantages to users, including the following:

[Rz 281] *Voluminous document transmission*: E-mails allow users to send only a limited amount of information, because of volume restrictions set by Internet service providers. In addition, transmitting numerous documents, e.g. hundreds of files, as is regularly the case in larger arbitration cases, is troublesome using e-mails. Case management websites often allow the uploading and/or downloading of entire folders at a time, with no limitation regarding the volume or number of documents.

[Rz 282] *Security and confidentiality*: typically, all communications and documents travelling between the user´s browser and the case management website are encrypted; documents are automatically checked for viruses before being posted, and any infected document is refused; and access to the website is protected by user names, passwords, and a security certificate.

[Rz 283] *Speed*: documents are available to all participants as soon as they are posted.

[Rz 284] *Organization and convenience*: on case management websites, all information and documents are in principle organized in a uniform manner and are «searchable». Moreover, most such websites label each document with the person who has uploaded it and the time at which it was done; hence, the origin of the documents is easily identifiable. Also, all submissions and exchanges are in principle tracked to show the chronology of a case, which makes document retrieval much easier than if e-mails or (considering the organization of a lawyer) hanging folders and ring binders are used. Furthermore, financial information on arbitration costs can also be tracked. Other features may include an «address book» with the contact details of all participants a general overview of the case; a calendar of the proceedings; guidelines for the use of the website.

[Rz 285] *Accessibility*: case management websites are accessible anywhere and at anytime. If they are well designed, they should operate regardless of the browser and operating system used. The accessibility of the information posted on such a website is also enhanced, and in this regard made comparable to e-mails, by the fact that participants receive message alerts when a new message or document has been posted.

[Rz 286] *Private forums*: as shown above in the presentation of extranets, case management, and virtual case-rooms, such platforms have the advantage of increased privacy. Indeed, the participants communicate in an environment that is more secure than the exchange of unprotected e-mails. Access to submissions can also be restricted to certain participants as appropriate, allowing to open the platform to be opened to, for instance, witnesses and experts who may, for example, have access only to the shared calendar. If a document is placed in a given section of the website by mistake, making it available to a participant who is not intended recipient, The error can be easily undone, if it is noticed before that participant has accessed the document. The situation would be different with e-mail communication, as the sending of an e-mail cannot be concerned.

[Rz 287] *Cost savings*: compared to working with hard copies of documents, case management websites allow insignificant costs savings, as the costs of preparing, handling and sending hard copies are greatly reduced.

3. Issues and concerns

[Rz 288] The principal legal and policy issues that arise from the use of case management websites are similar to those that occur when using any other information technology tool in arbitration. [286] They may be briefly called. Any case management website must ensure that the following requirements are met:

[Rz 289] *The right to be heard in an adversary proceeding*: a party has the right to be heard in an adversary

proceeding, which includes at least one opportunity for a party to present its allegations of facts and legal arguments, and the right to tender pertinent evidence on relevant facts, as well as the right to rebut the opponent´s case, which implies equal access to the record and that the arbitral tribunal does not have *ex parte* communications with any party.

[Rz 290] *Equal treatment:* the parties must be treated equally from a procedural point of view. In the present context, this requirement implies that the website is easily accessible to users with different levels of computer literacy. The filing processes should be simple and assistance should be available, whenever possible.

[Rz 291] *Transparency of the process*: a clear description of the process should be available, including costs, if any, and any substantive and/or procedural rules. The publication of any outcomes or statistics must be clearly disclosed. Any information given must not only be complete, but also easy to access and understand.

II. Videoconferencing

[Rz 292] Videoconferencing (sometimes known as a «video teleconference») is an IT-based solution that enables meetings among persons using both telephony and closed circuit television technologies simultaneously. It allows two or more participants located in different places to communicate with almost no consideration for geographic distance, sharing images, sound, and possibly software applications. Videoconferencing used to necessitate relatively sophisticated and expensive technical equipment. This has largely become untrue during the last years thanks to the advent of data transmission protocols allowing video over IP, which has significantly reduced the costs associated with its use. Videoconferencing software now only requires fairly basic terminal equipment, i.e. the equipment each end user must have on its side of the connection, which largely facilitates the organization and use of such software.

[Rz 293] Traditionally—if such a word can be used with such sophisticated IT solutions—the use of videoconferencing in arbitration (and in legal processes generally) relied on particularly high-end solutions, including for instance very high quality conferencing microphones, extra-large screens or very powerful projectors, cameras that could pan, tilt and zoom from afar, and, above all, dedicated lines or even satellite-based networks. Typical videoconferencing hardware equipment of this type costs approximately USD 10´000 – 15´000 [287].

[Rz 294] In addition to requiring a significant financial investment, such high-end IT solutions may be quite complex to use, for instance because they require non-standard equipment, which may use different transmission protocols and may be complicated to install. As a result, for such high-end solutions, it is recommended to resort to professional videoconferencing service providers, i.e. private companies that provide videoconferencing equipment, rooms, and technical assistance[288].

[Rz 295] Moreover, most uses of videoconferencing in such contexts have been point-to-point connections, i.e. including only two terminal stations, usually one for the arbitral tribunal and the parties who convene in a conference room, and one on the other side for the witness or expert who for some reason could not join the hearing in person [289]. Videoconferencing can actually be used in more sophisticated configurations, e.g. connecting each individual, or at least each team, separately from different locations.

[Rz 296] Much simpler solutions exist, which utilize familiar, standard and inexpensive equipment. Although they have generally been dismissed as not sufficiently sophisticated for arbitration [290], an experiment carried out at the University of Geneva seems to indicate that this will change not before long. At any rate, one should remember, in this situation just as in any other situation where recourse to IT is made, that the simplest solution, which is often also the most robust, should be preferred.

1. From high-tech to low-tech videoconferencing

[Rz 297] Before presenting the various uses of videoconferencing, it seems necessary to delve shortly into some technical aspects of this tool, in order to understand the main current types of technologies and the current evolutionary trends. Indeed, tremendous progress has been made since the radiofrequency-based systems used by

NASA during the first manned flights, which utilized for which two simple closed-circuit television systems, operating on standard, analog television technologies.

[Rz 298] First of all, it must be noted that the most challenging aspects of videoconferencing (from a technical point of view) is the digital compression technology, in real time, of the audio and video data transmitted. This compression is operated by software called a coder/decoder protocol (or codec), which achieves compression rates of up to 1:500. The other components of a videoconferencing system, such as the video camera, video display device, microphone, speakers or headset and high-speed data connection, also influence the quality and costs of an online meeting, but their importance is globally marginal in comparison with the codecs.

[Rz 299] Due to the rapid evolution of codecs throughout the 1990´s, videoconferencing systems have evolved from highly expensive proprietary equipment, software, and network requirements to standards-based technology that is readily available to the general public at a reasonable cost.

[Rz 300] There are fundamentally two kinds of videoconferencing systems, which correspond to two different technologies and two different types of codecs: dedicated systems and IP-based systems.

[Rz 301] Dedicated videoconferencing systems rely on a technical standard called H.320, which is the standard for public switched telephone networks or for ISDN videoconferencing. Such systems come as a global package, which include all required components in a single console. They exist in different «sizes», i.e. for groups of more than 10 persons, for smaller groups, and for individuals. Generally speaking, such systems may be said to be expensive, if not very expensive, costing easily several thousand euros. They allow, however, a particularly high quality of audio and video transmission.

[Rz 302] IP-based videoconferencing systems rely on a different technical standard, called H.323, developed in the late 1990´s in relation to Internet telephony (also called Voice over IP or VoIP). This new standard of data compression has enabled the development of videoconferencing systems working with standard (though relatively recent) personal computers. Anyone with a high-speed Internet connection, a webcam, a microphone and speakers or headphones, as well as a reasonably powerful computer, may now quite easily participate in videoconferencing sessions. Videoconferencing systems were thus brought to the masses and free services and software rapidly developed, among which one may count NetMeeting, MSN Messenger, and Yahoo Messenger. Most of these systems, however, are of relatively low quality and, above all, they do often not support multipoint conferencing, i.e. a videoconference involving more than two participants, which is technologically much more complicated to operate.

[Rz 303] Finally, it may be said that business, government, and military organizations still predominantly—though not exclusively—use dedicated videoconferencing systems.

2. The Geneva experiment

[Rz 304] In the spring and summer of 2005, the Geneva University Law School and MIRALab, a computer-science research center at the same university, specialized in virtual environments, conducted a proof-of-concept experiment seeking to demonstrate that videoconferencing in arbitration could be done using basic, everyday technical equipment.

A. General description

[Rz 305] This experiment used a commercial software application called ClickToMeet, configured so as to be best able to meet typical arbitration requirements. This application provided a videoconferencing platform featuring various online collaborative tools, such as document presentation and application sharing. It works on a standard PC. It was tested in simulations with arbitration practitioners and faculty members from both the Law School and MIRALab, so that it could be assessed from the perspectives of both legal practice and computer science[291]. The participants connected mainly from computers housed in the Law Faculty, although there were also connections from abroad, including Ireland and Korea.

[Rz 306] The test sessions comprised a short technical explanation (about 15-20 minutes), as one goal was to see if the system could be used almost intuitively, followed by a hearing on a simulated case, which included referring and viewing several exhibits in the form of pictures, affidavits, and expert opinions. The general result was that, despite several critical comments and suggested improvements, almost all participants concluded that the system was definitely usable in practice, and some even inquired when this system might be ready to be used for actual cases.

[Rz 307] The following paragraphs provide details on the scenario, and then review the technical aspects of the system, and it finally reports the main conclusions of the participants.

B. Scenario

[Rz 308] The scenario was based on an arbitration which took place at the 2000 Olympic Games in Sydney [292]. After a recapitulation of the main relevant information, such as the parties or the subject matters at issue, the following paragraph sets out the dialogue at the simulation hearing in bullet point format as it was provided to all participants to the test. This format was used to leave room for some improvisation.

Arbitration hearing in ***Rumyana Dimitrova Neykova* v. *International Rowing Federation and International Olympic Committee***

Parties

Claimant: Rumyana Dimitrova Neykova

Respondent: International Rowing Federation (IF) and International Olympic Committee

Participants

Counsel for claimant

Counsel for respondents

Arbitrator

Subject matters

Rowing regatta

Appeal against a decision of the IF

Accuracy of technical equipment

Olympics gold medal attribution and ranking modification

Exhibits

(1) Photo of the Swatch recording system
(2) Photo of the Sydney Olympic Broadcasting Organization´s video recording equipment
(3) Expert opinion by Mr Stein on the accuracy of digital and analog cameras
(4) Affidavit by Mr Bauman, a Swatch official, regarding the position of the Swatch camera and the TV camera.

Summary of the case

Neykova, a rowing athlete, finished second at the final of the Sydney Olympics, behind Ms Ekaterina Karsten, from Belarus. The time difference was approximately one hundredth of a second. The official photo and timing system, supplied by Swatch, showed Ms Karsten in first place. The Sydney Olympic Broadcasting Organisation´s video recording equipment, set up for the purpose of providing footage for TV audiences and not part of the official recording system, showed Ms Neykova in first place. Ms Neykova claims that the official Swatch recording system is defective.

Arguments

Introduction

Arbitrator:

- Introduces the case.
- Reminds parties that proceedings are conducted under rule for expedited arbitration, that no witnesses nor experts will be heard, that arbitral tribunal will rule immediately on its jurisdiction, and that award is rendered immediately after the end of the hearing, with a written decision containing the reasons to be issued shortly thereafter.
- Asks the parties to introduce themselves.

Jurisdiction

Arbitrator:

- Reminds parties that defendant notified intention to challenge jurisdiction.
- Opens the floor, first respondent, then claimant.

Respondent:

- Issue involves field of play rules: i.e. dispute not arbitrable. Technical decisions by sports officials made during sporting events cannot be submitted to arbitration. Refers to M. v. AIBA (CAS ad hoc division, Atlanta, OG 96/006):

  «Traditionally, doctrine and judicial practice have always deemed that game rules in the strict sense of the term, should not be subject to the control of judges, based on the idea that ´the game must not be constantly interrupted by appeals to the judge»

Claimant:

- Admits that this corresponds to most precedents.
- But field of play rules theory should be revisited, and this is occasion to do it.
- Field of play rules theory is in reality not a question of arbitrability. Arbitrability is in CH determined by art. 177 Swiss PIL act, which reads:

  «All pecuniary claims may be submitted to arbitration».

Many sports decisions, and the present one is no different, have substantial direct pecuniary implications. Hence, they are arbitrable.

- What the field of play rules theory in fact seeks to achieve is, as respondent suggested, to avoid «constant interruption of the game by the judge or the arbitrator». It is in reality a question of scope of consent given

to arbitration. In principle, consent does not cover field of play rules, precisely because the parties do not want interruptions of the game. But in this case, it is different.
- In this case, it is a question of the accuracy of technical equipment. Sanctioning such inaccuracy would not lead to any interruption of the game. In addition, this issue is fundamental enough to the competition that one may assume that the parties intented to allow a decision on equipment to be revised before an arbitrator. This dispute is arbitrable.

Arbitrator:

- Makes ruling on jurisdiction: dispute arbitrable.
- Case proceeds.

Merits

Arbitrator:

- Reminds parties that question is the validity of the official photography, which determines the winner.
- Reminds parties of the relief requested by claimant (ranking reconsidered, she be awarded co-gold medal, the race a tie between Neykova and Karsten, current gold medalist).
- Specifies that, according to the rules, one opportunity for each to make the case, and possibly short reply to each other´s argument.
- Opens the floor.

Claimant:

- Mechanical error, or at least inaccuracy in the photo finish, i.e. picture not taken at the right time. [shows exhibits 1 and 2, i.e. the two pictures of the finish, one showing Karsten in first place, the other one showing Neykova]
- On Australian television, based on the Sydney Olympic Broadcasting Organisation´s video recording equipment, Neykova won the race.
- On official cameras, Karsten won the race.
- Time difference only one hundredth of a second.
- If two cameras show different results, means that recording equipment cannot be accurate enough to single out a winner by one hundredth of a second.
- Unfair to proclaim a single winner with such a precision, as the technical equipment is manifestly unable to provide such accuracy.
- Arbitral tribunal should declare the race a tie between Neykova and Karsten. Neykova deserves co-gold medal.

Respondent:

First argument

- TV recording less reliable technology than the one used by Swatch.
- Swatch is digital, uses digital technology, stores electronic data which can later be used to create image like photographic image but more precise.
- Video tapes, which were used by Olympic Broadcasting Organisation, produce less accurate images, as tape needs to be moved across camera´s lens to create image on tape; this makes image much slower.
- Refers expert opinion by Mr Stein, a video engineer [shows exhibit no 3].

Second argument

- TV camera was located 10 centimeters in front of finish.
- Swatch camera exactly on line.
- When 10 centimeters projected across 200 meter width of course, perspective different. [shows exhibit 4]

- Camera located exactly on line should prevail.

Conclusion

- Official camera perfectly accurate, to the hundredth of a second.
- Other camera poorly located and uses a much less precise technology.
- Other camera should not be taken into consideration.
- Gold medal should stay with Karsten and with Karsten alone.

Arbitrator:

- Thanks for arguments
- Reminds parties that will now give conclusions and decision orally, which will be followed by written award.
- Conclusion and decision: Deficiency of mechanical operation of official photo finish equipment not established; ranking case will not be revised; Ms Neykova remains second.

C. The ClickToMeet videoconferencing platform. General description

[Rz 309] The application used for the Geneva experiment is called ClickToMeet. ClickToMeet is a particularly user-friendly videoconferencing application that works with a standard PC, a low-budget webcam, and an ordinary headset for Internet telephony (headphones and microphone).

[Rz 310] This application can display up to 16 participants at a time, and can allow them to share pictures, videos, and any other file, document, or recording. It also allows the collective editing of a document, for instance a Word document.

a. Security

[Rz 311] All access is password-protected and all participants, whether active (i.e. who transmit video and/or sound) or passive (i.e. who only watch and/or listen) appear on a list displayed on the screen. Consequently, if a password is stolen or intercepted, the person using it would reveal his or her presence on the platform by his or her name appearing on the list.

b. Properties

- Videoconferencing, in which participants may also intervene using a standard telephone or IP phone (i.e. videoconferencing and teleconferencing in the same virtual conference room).

- Application sharing: any application that one of the participants has on his or her computer can be viewed, and even used, by any other participant during an online conference: e.g. one participant can show a video recording even if no other participant has the software to play that recording, or the participants can collectively write a Word document. Virtually any kind of data can be transmitted using this system, as long as the participant transmitting it has the software to read it on his or her own computer.

- Mouse movements by one participant can be shown to all other participants, allowing a participant to point on a map, a plan, a drawing, a bill, etc.

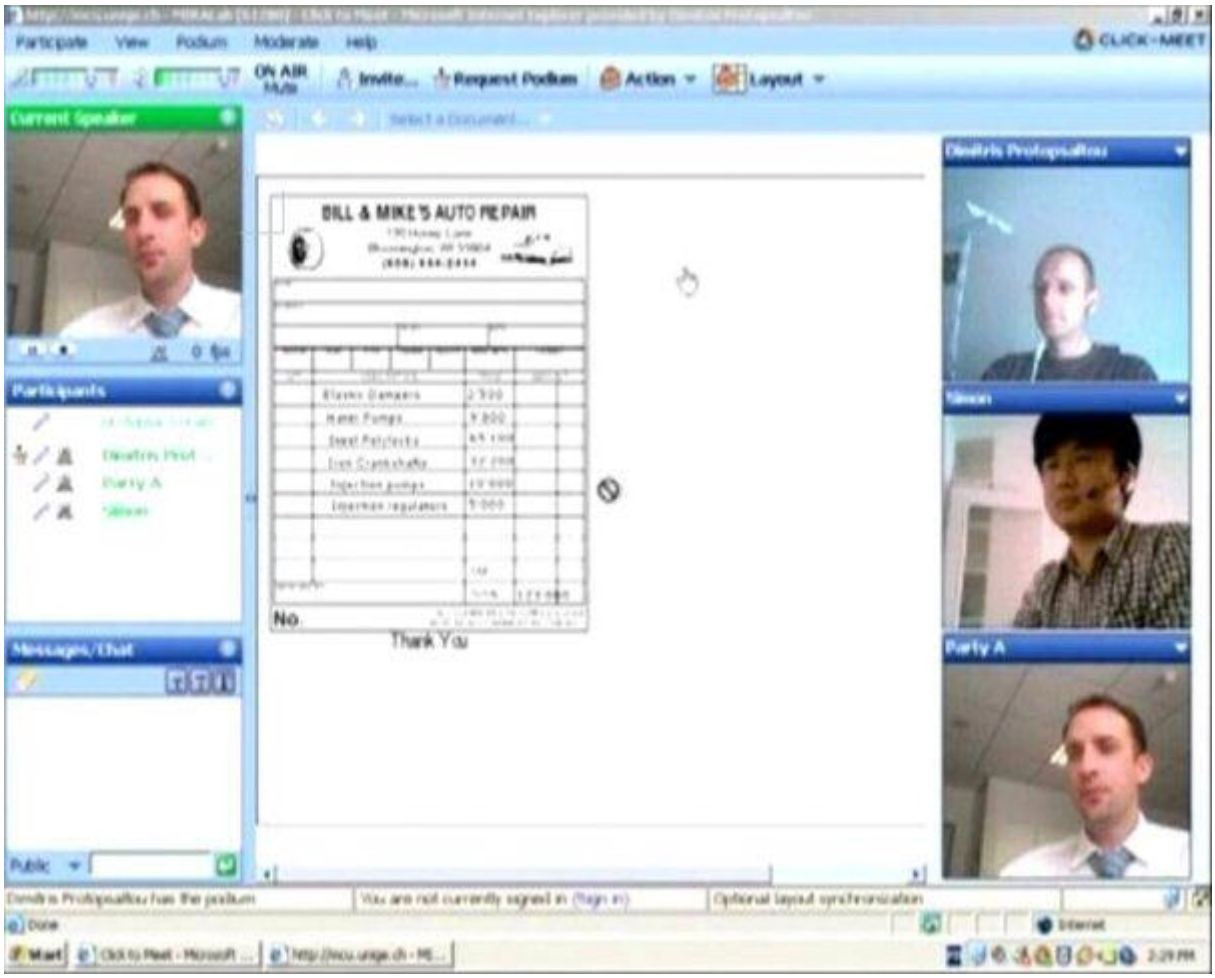
- Recording: entire sessions can be recorded in either audio or video format. Notes can of course also be taken by the secretary. Video recording, however, requires time-consuming editing, and consequently will be charged. Recordings are in principle prepared to be sent on a DVD, by courier.

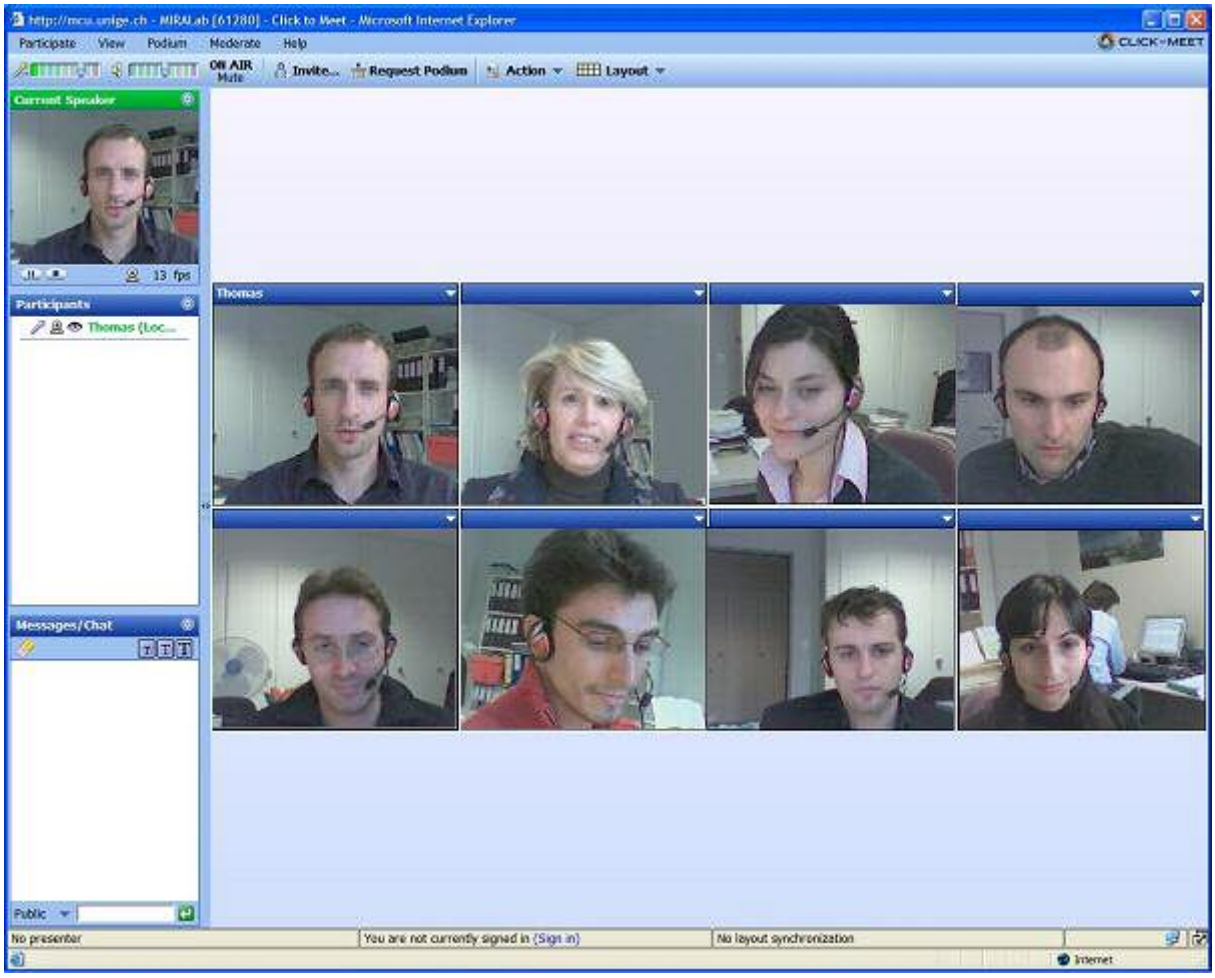
c. User capacity

- Up to 16 participants shown at the same time on platform while in videoconferencing only (i.e. «video-actors»); up to 5 participants shown at the same time when videoconferencing at the same time as application sharing / document presentation.

- Up to hundreds of participants who only watch and listen (i.e. «spectators»).

d. Screenshots





e. Technical requirements

[Rz 312] Hardware requirements for each participant:

Relatively recent Windows PC (roughly not more than 2-3 years old) (Windows 98/2000/XP; optimal configuration = Pentium 4, 2Ghz, 512Mb)	
Headset, including headphones and microphone, for instance Logitech Internet Chat Headset (approx. 30 euros)	

Standard webcam, for instance QuickCam® Communicate™ STX (approx. 30 euros)	

[Rz 313] Software requirements:

- Windows 2000/XP
- Internet Explorer v.6 or higher

[Rz 314] Other requirements:

- High-speed Internet connection (minimum requirement 600 Kbit/s in reception and transmission speed). This corresponds to a professional Internet connection. For comparison, most common broadband connections people have at home today have a download (reception) speed of 600Kbit/s, but their upload (transmission) speed is of only 150Kbit/s.

D. Summarized results

[Rz 315] At the end of each videoconferencing test session, a series of questions, was submitted to the participants and discussed live and in subsequent e-mail exchanges. Their compiled answers to these questions are set forth below in a rough summary. They will receive further consideration below, when discussing the advantages, disadvantages, and recommendations regarding the use of videoconferencing in relation with arbitral proceedings.

[Rz 316] The main question posed to the participants which deserves mention here is: «*Would you be willing to use it [this videoconferencing system] in practice?*» All participants but one answered «yes». The intuitive understanding of the fundamental advantages of videoconferencing, combined with the opportunity to witness that such systems actually work in practice with little effort, generally triggered much interest. Ironically, even some of the most skeptical participants inquired, after much criticism, if it were possible to use the system for one of their cases, as soon as possible. The criticism, in other words, suggested that the fact of holding a meeting online was somewhat unsettling, and that improvements of the platform and its concrete use could always be made. Save in one case, the criticism was never significant enough, however, for the person making the criticism not to be willing to use the system.

[Rz 317] The fact that almost all participants in the simulations embraced the idea of using videoconferencing did not mean, of course, that this technology should be used as the new pen and paper (or computer and text-processing software) of arbitration, that it should or even could be used in any situation. Obviously, this type of videoconferencing is appropriate only for certain cases and situations. Identifying these cases and situations was actually the principal aim of the simulations. The purpose of the present section is neither to set forth a detailed analysis of these issues nor to provide a reasoned explanation of the pros and cons of videoconferencing, but rather to report the general impressions of the practitioners testing the platform. The exact answers and comments provided by these persons are integrated, in compiled fashion, in a subsequent section.

[Rz 318] Regarding the *overall usefulness* of videoconferencing, the recurring statement made by the testers was that this technology was without any doubt far better than a telephone conference, but that it would always remain second-best to face-to-face meetings —from the point of view of the quality of the communication. The comments amounted to this: videoconferencing is not the same as a face-to-face hearing, and consequently, if costs and time considerations do allow it, it is clearly preferable to hold an in-person hearing. On the other hand, it is better to

communicate using videoconferencing rather than not at all—hearing a witness using such technology, for instance, is better than simply not to hearing him or her. Videoconferencing is also often better than telephone conferences or e-mail exchanges, except when a paper trail is required.

[Rz 319] The comparison of videoconferencing and in-person meetings, on the on hand, and videoconferencing and telephone conferences, on the other hand, is to a large extent based on one specific characteristic: the capacity of the technology to create a *sense of reality*, a *feeling of the other participants´ presence*. The dominant comment of the testers was that they were positively surprised by the system,which provided an impression much closer to a face-to-face meetings than they had expected.

[Rz 320] Asked about their *perception of the other parties´ state of mind*, the replies were quite variable. Most confirmed that they could easily feel whether the other participants in a session were paying attention or were distracted, were rather nervous or at ease, and were happy with the functioning of the platform and the progress of the simulated case or not. On several occasions it was noticeable that the absence of physical presence lead the participants to be somewhat less inhibited, displaying more facial expressions than they probably would probably have in a real meeting. This may have compensated to some extent for the fewer clues that image transmission conveys compared to an in-person discussion. On the other hand, a few testers stated that they were unable to assess the other party´s and the arbitrator´s states of mind, and that it was even more difficult to do so than during a telephone conference, because they were distracted by the image. This seems to suggest two things. First, one factor of an individual´s ability to sense other people´s state of mind over a video linkup is the personal ratio of reliance on verbal as opposed to non-verbal aspects of communication. For instance, some testers admitted that not being able to make a real eye-to-eye contact—the camera was not placed behind the screen, but on top or beneath it—was disturbing, while others could barely understand that this was an issue at all. The second suggestion is that this form of communication requires that users get used to it. Indeed, the distraction some felt while using the system is without any doubt due to the novel aspect of the interface.

[Rz 321] The reverse situation was strictly unproblematic: all participants stated that they did not have any problem with their own expression. They all declared that they had felt able to express themselves, to *make their point*, to be heard, to have had «access» to the tribunal.

[Rz 322] More generally, the electronic form of the communications did not raise any issue with regard to the ability to *get attention* during the sessions or to *understand what was occurring*. This is especially remarkable considering that, as the screenshots above show, the windows in which the images of the participants appeared were relatively small: about one sixth of the total surface of the screen during most of the conferencing (i.e. except during document presentation, at which time they were even smaller) and the screens that were used were only 15 inches in dimension.

[Rz 323] One way to reduce the distraction and consequent lack of concentration due to the novelty of the environment in which the parties communicate is to involve a secretary of the arbitral tribunal to handle all technical aspects of the sessions. In the latter stages of the tests, one such person was. He did not appear on the screen but could see and hear the participants. If the testers wanted to change any aspect of the platform (size of windows, switching from conferencing mode with larger images to document-presentation mode with smaller images of the participants, uploading documents, etc), they would simply say so into their microphone and the secretary would take care of it. The result was that the testers only had to talk as they would in a traditional meeting. As they knew that they did not have to interact with the platform, they could better focus on the substance of the hearing. Nevertheless, although this measure largely facilitated attention, especially for those less at ease with computers, the testers still stated that such sessions required more effort concentrate than a normal meeting (like telephone conferences). The implication is that such sessions should be kept relatively short. In addition, it was clear from the behavior of the testers, which evolved during single sessions, that the videoconferencing itself, i.e. the fact of speaking to a screen, requires getting used to, regardless of the simplicity of the system.

[Rz 324] Finally, the usefulness of videoconferencing can be improved beyond the simple possibility of seeing the face of the person addressed. Technology allows adding specific features that can make a videoconferencing session more effective. For instance, with respect to the platform used during the tests, the feature most positively assessed was the document-presentation and application-sharing feature, i.e. the possibility to present any type of electronic

document, in any format, and to point on or highlight specific parts of the document with cursor movements which were reproduced on the other participants´ computers. The shared real-time drafting of documents was also highly valued, as it could be used for collaborative drafting from afar of terms of reference, procedural orders, or arbitral awards (if the videoconferencing were used for arbitrators´ deliberations).

3. Assessment of videoconferencing in arbitration and recommendations regarding its use

[Rz 325] This section assesses in which situations and under which conditions videoconferencing should be used in arbitration. In order to provide such an assessment, it is necessary to first review the main factors for and against its use After discussing these factors, the section sets forth the situations in which the use of this technology would be beneficial. Finally, it provides certain recommendation, which apply to several of these situations.

A. Factors in favor of and against the use of videoconferencing

[Rz 326] The factors in favor of and against the use of videoconferencing in arbitration may be considered in comparison to other means of communication or more generally to other ways of communicating. Videoconferencing will thus be compared, first, to telephone conferences, second, to in-person meetings and, third, to e-mail or letter exchanges.

a. Videoconferencing v. telephone conferencing

[Rz 327] The idea of starting this discussion with a comparison of videoconferencing and telephone conferencing may appear surprising. Indeed, videoconferencing is most of the time compared to in-person meetings. Nevertheless, videoconferencing appears in many ways as an improved alternative to telephone calls, in a spirit similar to the many science-fiction movies that feature this technology as the ordinary replacement of telephones. The clearest advantages of videoconferencing appear when taking this perspective.

[Rz 328] First of all, the use of videoconferencing bears no disadvantages compared to telephone calls, as the audio transmission is even better than that of a telephone connection because a higher number of frequencies are transmitted. Telephones actually only transmit a very limited number of sound frequencies, these frequencies having been identified as those necessary for a person with normal speaking and hearing capabilities to hold a conversation in his or her mother tongue; this explains the additional difficulties we experience when conversing on the telephone in an unusual language. Computer microphones and headphones, as well as most videoconferencing systems, do not operate the same restrictions in the frequencies transmitted, with the result that voices are carried over the network with more clarity in videoconferencing than when using a telephone.

[Rz 329] In addition to this lack of disadvantages, videoconferencing bears a number of advantages compared to telephone conferences. The most obvious advantage is the addition of images. Even in situations where the quality of such images is not outstanding, they provide additional clues as to the state of mind of the person one is speaking to. These clues are more or less significant depending on the quality of the video transmission, but even relatively low-quality images provide at least some indication of the general attitude of the other participants.

[Rz 330] Another advantage particularly appreciated by the testers of the videoconferencing platform used at the University of Geneva, was the possibility of adding visual demonstrations and collaborative document management capabilities to the platform. Visual demonstrations are presentations for instance of exhibits in the form of text documents, pictures, movies, audio recordings, simulations run on architecture or engineering programs, etc. Collaborative document management provides the possibility to work collectively on a single document, in real time. The research team utilized the videoconferencing platform used for the arbitration simulations to collectively draft, from afar, on scientific articles, research proposals, and even some parts of the present publication. In the context of arbitral proceedings, collaborative document management capabilities may be used to facilitate the drafting of documents such as the terms of reference or procedural orders. For instance, the president could prepare the bulk of such a document and leave more problematic parts in blank or highlighted. The latter parts may then be discussed and drafted in real time under the eyes of all the participants of the videoconferencing sessions, who may then immediately comment and approve the final version.

b. Videoconferencing v. in-person meetings

[Rz 331] Videoconferencing is most often suggested as a replacement for face-t-face meetings. Interestingly, it is precisely the comparison between these two types of communications which drew the most criticism to the disfavor of videoconferences. The reason is that, in this respect, videoconferencing shows as many advantages as disadvantages. The testers in the simulations referred to above generally considered that videoconferencing sessions could only be a second-best solution, compared to in-person meetings. The lack of a sense of reality and the consequent difficulty of discerning the other participants´ state of mind, though less significant than what most people had expected, lead consistently to the view that virtual meetings were not as good as real meetings. At the some time, testers found that virtual meetings do achieve a reasonable amount of the communication objectives that real meetings usually achieve, such as understanding the facts and issues (be they procedural or related to the merits) and clarifying the parties´ positions on specific issues.

[Rz 332] Fundamentally, the situation is therefore as follows: videoconferencing will always remain the second-best solution compared to in-person hearings, but it is useful in many respects. Moreover, as shown in the preceding paragraphs, such virtual hearings are preferable to telephone conferences. Hence, videoconferencing is adequate when a face-to-face meeting cannot be arranges, e.g., the witness cannot travel to the hearing site for medical reasons, or when it is not reasonable under the circumstances to hold an in-person hearing. This is obviously so when the cost, loss of time and inconvenience generated by the meeting are disproportionate with regard to (1) the disputed amounts, and (2) the expected benefits of the meeting.

[Rz 333] If the disputed amounts are low, meeting in person may easily generate costs that are disproportionate in view of the actual monetary value in the dispute. The disputed amount must of course not only be compared to the costs generated by one in-person hearing, but to the total costs of the procedure and assessed against the likelihood of recouping costs in the future.

[Rz 334] This brings us to the next point, which is that, the selection of the meetings which can be held online. That selection depends on the expected benefits of an in-person meeting as opposed to a videoconference, i.e. does the first one result in sufficient added value to justify the additional costs involved? In some situations, one needs something better than a telephone conference, but a face-to-face meeting is not essential. Procedural hearings, for instance, do not necessarily gain much from being held in the actual physical presence of the parties. An exception is often warranted for the first procedural hearing when arbitrators and counsel/parties do not know each other and holding a face-to-face meeting is useful to build confidence in the process.

[Rz 335] If one of these two conditions is met, i.e. either if the disputed amounts do not allow the expenses of a face-to-face hearing, or if the added value of holding the meeting in person does not require it to be held in such a fashion, then resorting to videoconferencing may provide significant costs advantages.

[Rz 336] The only costs specifically generated by a videoconferencing meeting are the investment in the hardware (which can be very modest)[293]; a fee for using the videoconferencing platform ; and possibly a fee for the assistance of a technician for the preparation of and during the meeting. By contrast, the costs saved by holding a videoconferencing session, rather than a real meeting, appear quite significant. They cover travel expenses of all participants and the rental of conference rooms.[294].

[Rz 337] The second situation in which in-person meetings cannot reasonably be arranged occurs when time is a problem. Time may be a problem in two respects. First, in urgent situations, it may simply not be feasible to gather all the participants involved on very short notice. This may occur if a party has requested urgent interim relief. Whatever its benefits, a face-to-face meeting must then be ruled out and a videoconference is certainly the second best solution, preferable to a telephone conference. Second, time lost before and after an in-person hearing may also play in favor of a videoconference. Because it requires more time overall, it is more difficult to find a time convenient to all participants for an in-person meeting than for a videoconference. Moreover, the purpose and contents of the hearing may not justify the loss of time involved in traveling to and from a face-to-face hearing. Saving time for all participant and allowing for a closer hearing date, are additional factors speaking for videoconferences rather than real hearings.

[Rz 338] The disadvantages of holding a meeting by videoconferencing rather than in-person all derive from the lessened sense of reality and the absence of the points of reference people usually use in a discussion. Indeed, as is generally acknowledged , videoconferencing is not a perfect substitute for in-person interactions. It does not transmit all the elements of non-verbal communication. For example, videoconferencing does not allow participants to make proper eye contact, making it more difficult to establish trust and to clearly direct attention, approval or disapproval [295]. This also has the effect of reducing the «vibes» between people during the meetings, thus reducing the ability to «feel» the other parties´ interests, intentions, and positions. If communications during the session can be expected to require many subtleties, the added value of holding a real hearing becomes more important.

[Rz 339] Further, it is more difficult to concentrate in a virtual meeting than in a real hearing, like in a telephone conference. The traditional environment of a real gathering provides many implicit clues that direct our level of attention. These clues being absent when facing a screen, most participants in videoconferencing sessions need more efforts to remain concentrated. This may be an issue in itself if the matters at issue are particularly complex. Furthermore, it implies that a virtual hearing should be scheduled for shorter periods than an in-person meeting.

[Rz 340] The final disadvantage may seem more trivial, but it is probably not: videoconferencing does away with coffee breaks and other informal discussions. Again, if the case involves subtle balances, unclear positions and interests, this disadvantage may be far from insignificant. This does not mean, however, that such social interactions are needed at every meeting or in every case. It simply means that in most cases, there should be a mix of virtual and real meetings.

[Rz 341] Finally, in addition to the factors that constitute clear advantages of videoconferencing vis-à-vis offline sessions, and other factors that amount to clear disadvantages, there are aspects of this form of communication which change the context of the meeting in a way that may be an advantage or a disadvantage depending on the situations or the personality of the participants.

[Rz 342] The first such factor is that a videoconferencing meeting is a less contextual situation, which is thus less impressive and less stressful for the participants. This may make no difference for most lawyers used to speaking before an arbitral tribunal, yet the same may not be true for witnesses or experts. Speaking in front of three senior arbitrators, two teams of lawyers and their clients, a secretary, a court reporter, etc, in rather formal proceedings, compared to sitting alone or with one observer in a room, possibly one´s usual office, will certainly bear significant consequences for many witnesses. On the other hand, many rhetorical tricks are unlikely to work from afar. Hence, one may suggest that rather shy witnesses are better served in a virtual hearing, while better speakers would deliver more convincing testimony in a real hearing. Hence, it may also be a question of strategy for a party to accept or to offer to hear a witness over a video linkup.

[Rz 343] The second such factor that can be both an advantage and a disadvantage is the fact that videoconferencing necessarily allows capturing the data (sound and images) in an electronic form, thus automatically generating a record.[296] It is certainly good that it be done; such a record may be used as an augmented form of transcript of the hearing, for instance when preparing post-hearing briefs and the award. Testimonies, for instance, can be watched several times if doubts remain.

c. Videoconferencing v. e-mail or letter exchanges

[Rz 344] The comparison of videoconferencing and e-mail or letter exchanges calls for much fewer comments. Suffice it to say that, on some occasions, instead of exchanging numerous e-mails or letters, for instance to organize procedural matters, it may be advisable to hold a brief hearing on a videoconferencing platform. The possibility of using shared applications allows collective work on agendas, or on drafting procedural terms in real time, for instance, and allows the parties to react instantaneously to organizational matters.

B. Situations of use

[Rz 345] On the basis of the discussions above, one may now envisage the situations in which the use of videoconferencing seems particularly advisable. One basic consideration should serve as a starting point to assess the situations in which videoconferencing should or should not be resorted to. These situations should be considered to

represent a sliding scale of appropriateness of using videoconferencing with, at one end of the scale, contexts in which there is every reason to use this means of communication and, on the other end, contexts in which the use of this technology seems highly unadvisable. These two extreme situations may be described as follows:

- Videoconferencing can always be used if the situation could also have been dealt with in a telephone conference. In such contexts, using videoconferencing bears in principle no disadvantages, as the sound transmission is in principle of the same quality, and often better.[297] Admittedly, technical breakdowns are more likely to occur in relation with video linkup sessions than with telephone conferences, be it only because of the fact that computers, rather than telephones, are used on each end. To guard against this eventuality, a back-up solution should always be ready. Such a back-up solution could for instance be a telephone conference, in which case it would be advisable to obtain in advance the information necessary to organize a telephone conference at very short notice (i.e. contact information and availability of telephone conference service providers and the telephone numbers of the participants in the discussions). Among the advantages of using video linkup rather than telephone conferences, are the presence of the images of the persons involved; possibly (depending on the videoconferencing system used) the availability of document presentation and shared document editing facilities; and a reduction of costs. The presence of images, except if the quality of transmission is poor to the point of becoming a nuisance, always conveys additional information that a pure audio connection does not transmit. The better the image, the more information will be conveyed, but even relatively low-quality images can help assess the other parties´ general state of mind or reactions to specific events. The possibility of presenting documents and maybe of collectively editing them may be particularly useful if the objective of the meeting is to discuss the specific contents of a document, for instance a procedural order. The reduction of costs depends on the fees charged by the provider of the videoconferencing platform, but it would be unsurprising to witness the development of annual or per case flat fees arrangements. The cost reduction factor inherent to using the Internet as a basis for communications has at any rate already lead many clients and lawyers alike to suggest the use of Internet telephony systems, such as Skype, which is free for communications involving no real telephones.

- Videoconferencing should never be used if there is no serious reason *not* to meet in person (which would essentially be reasons related to costs and time, as was discussed above). Video linkup, as the testers involved in the Geneva experiment reviewed above have repeatedly asserted, will always remain a second-best solution compared to face-to-face meetings. The following disadvantages of videoconferencing in opposition to in-person meetings may be recalled here: the sense of reality and the feeling of the other participants´ presence are inevitably weaker; the perception of the other participants´ states of mind, if better than on a telephone, is not as good as in reality; video-based meetings are more demanding in terms of concentration and thus must be held for shorter periods; people get fewer «vibes» from each other over a video linkup as images do not transmit all the elements of non-verbal communications; no eye contact can be made; and no off-track discussions take place, or informal chats at airports or during coffee breaks may occur.

[Rz 346] In all other situations, the suitability of resorting to videoconferencing should be considered by balancing the interests for and against its use, which first requires an assessment of the concrete needs of the situation in terms, on the one hand, of time and money and, on the other hand, of the richness of the information transfer. More precisely and in between these two radical situations where videoconferencing should either always or never be used, the following occasions can in principle be envisaged as being appropriate for video linkup sessions:

- When *a witness cannot be present in person*, especially but not exclusively if this problem occurs at very short notice, the possibility of hearing this person from afar, although less satisfactory than hearing him or her in person, may constitute a good solution.

- For *procedural matters*. Videoconferencing may be faster than exchanging written messages to organize procedural matters, and it may conveniently replace procedural meetings between the arbitrators and procedural hearings involving the parties, as these meetings and hearings are frequently held using telephone conferences. An exception must be made when the procedural hearing is also meant as an opportunity to meet for the first time.

- For *cases involving large distances* between the various participants in the arbitration and a rather *low-amount*

in dispute. Typical of the online dispute resolution movement, these situations call for every available means of communication that can reduce the costs (especially those related to travel),, which must always remain proportionate in regard to the amount in dispute.

- Drafting or reviewing the *terms of reference or mission statement*. This is often done over the telephone or by exchanging faxes. A videoconferencing system featuring document presentation and editing facilities may largely facilitate and accelerate this task, as the parties and the arbitrators would be able to discuss and amend the document in real time, with the text and its revisions right in front of the eyes of all participants in the session.

- *Deliberations* among the arbitrators. When preparing a procedural order or the award, the arbitrators may discuss the contents and amend the text in real time, if the videoconferencing system is equipped with document presentation and editing features. This may typically be done by one arbitrator (in principle the chairperson) preparing most of the text and highlighting the critical passages or those that may have to be debated.

- *Assessing and preparing witnesses*. Counsel may want to simulate a hearing with the witnesses they intend to hear during the proceedings, both to assess their credibility and their actual knowledge of the facts they will be called to testify on, and to prepare them for cross-examintion. Instead of travelling to meet these witnesses, or having them travel to the counsel´s location, it would save time and costs to assess and prepare them over a video linkup. The lack of sense of reality and possibility to feel their state of mind is unlikely to constitute any real disadvantage in this context.

- *Meetings with co-counsel*. When several teams of counsel work for one party, they may often be located in different countries if not on different continents. A videoconferencing meeting may provide a good opportunity to assess each other´s position and style, and to get each other´s ducks in a row.

- *Expedited arbitration*. Videoconferencing may meet the needs of expedited arbitration in several ways. First of all, there are situations in which decisions must be reached so quickly that they do not allow bringing in all the required participants—as is for instance typically the case during the Olympic Games, where the awards must in principle be rendered within 24 hours even though the case may require hearing witnesses literally residing on other side of the planet. In such situations, the only choices are to forego the in-person participation of these individuals. To allow these individuals to participate over videoconferencing, is obviously the best solution, preferably over hearing them by telephone. Second, there are less dramatic situations in which the travel time of the various participants could in principle be tolerable, but the difficulty of finding common availabilities may substantially delay the actual date for a possible meeting. Here again, the best solution is obviously to meet via a video linkup system.

- Serious problems of *availability* . It may happen that an arbitrator or a counsel is unexpectedly prevented from attending at the last minute. Rather than postponing the hearing altogether, a videoconference would ensure the presence, even though only virtual, of the missing person.

- *Hearings on interim measures*. By their very nature, hearings on interim measures must often take place on short notice. As a result, it may be difficult to identify an available date for an in-person hearing. Finding the time for a two-hour videoconference hearing would be much easier in most circumstances and may largely contribute to clarifying the parties´ positions and to grant them an opportunity to be heard. It is at any rate more profitable to hold a brief hearing over video linkup rather than not to hold a hearing at all and rely solely on the parties´ briefs.

C. Other recommendations of use

[Rz 347] Having thus defined the main situations in which videoconferencing may be useful, we will now make some concrete recommendations regarding the use of this technology. These recommendations are meant as additional considerations for evaluating if on a concrete situation, a video linkup would provide the required advantages and whether these advantages would outweigh the inherent disadvantages of not holding an in-person

meeting.

- When dealing with parties or arbitrators who are inexperienced with videoconferencing generally, and preferably also if they are *inexperienced with the specific platform* intended to be used, one should preferably schedule a videoconferencing *session that can be replaced by a telephone conference* if a problem occurs. A hearing necessarily requiring image transmission should not be scheduled as a videoconference if the parties do not have sufficient experience with the technologies being used. In other words, with inexperienced participants, one should start with particularly simple situations that could also be dealt with satisfactorily by a telephone conference. Moreover, with participants who have not yet used a specific platform intended to be resorted to with exactly the same computer they will be using during the session, a test session should be scheduled as much in advance as possible. For instance, during the experiment carried out at the University of Geneva, although the technology being used was quite simple and robust, some participants could not connect to the platform because of oversensitive security measures, or could not even install the application on their computer. On each occasion on which the test session was done at least a day in advance, the problem could be resolved (by using another computer or by connecting through another network). Furthermore, in addition to holding such a test session, it would be useful to provide the participants with an interactive demo before the first use, so that they can practice and become comfortable with the technology. Finally, if the budget allows it, it may often be prudent to involve a secretary in charge of the manipulation of the software, so as to allow the participants to focus on the meeting, and not on how the platform works.

- To increase the sense of reality and to allow at least for some «vibes» between the participants, videoconferencing should only be resorted to, whenever possible and especially in larger cases which in any event entail several meetings, *after all the participants have met at least once in person* during a previous meeting. This reduces the effect of «dehumanization» of the communications, as the participants can more easily associate the image they hear and the voice they hear with a real person whose personality they know at least a little.

- Videoconferencing should preferably not be used in *situations of conflict* or when the assessment of the other participants´ *states of mind is particularly important* (e.g. some key witness hearings). In such situations, the disadvantages of not meeting face-to-face would be particularly important. On some occasions however, as was suggested above, it will simply not be realistic to hold an in-person meeting; hence, this is only a recommendation, and not a strict rule.

- As to the selection of the appropriate videoconferencing platform, consideration should be given to the *availability of document presentation and sharing facilities*, including the possibility of pointing at specific parts of documents, highlighting sections of the text, and if possible sharing other applications. These features largely contribute to the overall benefits of videoconferencing, allowing participants to show exhibits during hearings and to work collectively, during procedural meetings or deliberations, on a document that is instantly updated version before the eyes of all participants.

- Regarding the presentation of documents, it must be said that most document presentation and sharing technologies will become rather difficult to handle if a *large number of documents* are used (if a figure must be suggested, one may roughly assess the critical limit at some 30 documents). Hence, the more numerous the documents expected documents to be viewed during the meeting, the less convenient a virtual meeting will become.

4. Issues and concerns

[Rz 348] Some concerns about the use of videoconferencing arise continuously. They are voiced, in principle, by those individuals who have little or no experience with this technology. These concerns call for clarification; some of them correspond to real issues or to actual limitations of this means of communication, while others merely constitute exaggerated apprehensions caused by a lack of knowledge in this field. The concerns met most often are technological insufficiencies and limitations; security, privacy, and confidentiality; and legal issues in general.

A. Technological insufficiencies and limitations

[Rz 349] Many practitioners fear that the technology will not work properly when they need it most, that the quality of the image will not be sufficient, and that an image transmitted by a camera can never be trusted entirely, as it shows only what the camera sees, and not everything that occurs in the room in which a participant is located.

[Rz 350] The issue of technical breakdowns is a real issue. Imagine being in the meeting room of a hotel somewhere with all other parties, arbitrators, witnesses, experts, and running the risk of becoming suddenly blind, deaf, and dumb. Indeed, such a risk puts a damper on the enthusiasm of many people. But it should be remembered that the handicaps we just mentioned are reversible and that the risk that they incur can be significantly reduced by implementing the measures suggested above, such as testing the equipment beforehand. According to the principle of dedication presented in the first chapter of this study,[298] one should be very careful when using a computer for anything else than video linkup meetings, and should possibly even reserve a specific computer for the exclusive use of videoconferencing. The principle of redundancy, also presented earlier,[299] would suggest that for each participant two computers should be equipped so as to be perfectly interchangeable and they should be available at all times. If possible, but this is admittedly much more difficult to achieve, these two computers should connect over two different high-bandwidth networks. Moreover, provisions should always be made for fallback solutions, such as telephone conferences or alternative dates. Finally, it should be remembered that videoconferencing should not be planned for situations of major importance if an in-person meeting can reasonably be arranged instead.

[Rz 351] The broadcast quality of videoconferencing depends essentially on the bandwidth used. The quality of the hardware and software used is much less important in this regard. This issue is indeed a fundamental limitation of the technology. Without a high-speed connection, an online video meeting may not contribute to establishing interpersonal rapport and will cause frustration. However, this problem is decreasing as compression rates for images are being improved and connections gradually become faster. Nevertheless, bandwidth considerations remain a knockout factor; below approximately 500 Kbps, the quality of the image transmission becomes poor enough to make the whole exercise useless.

[Rz 352] The fact that the participants cannot see what lies outside of the field of the camera is certainly a genuine issue, but it seems highly overrated. The reason why it is a concern in the first place is the fear that a participant—especially a witness or an expert—is being prompted answers or a general line of conduct during his or her examination or cross-examination, or that he or she is being threatened by a person positioned just outside of the field of the camera. A series of measures can be taken to reduce this risk. For instance, one may utilize cameras that can be controlled from afar to pan, tilt and zoom; hence, one may at irregular intervals scan the entire room in which the person in question sits. Such cameras may be standard webcams mounted on a rotating and inclining platform that can be controlled by a distant computer; both together should not cost more than a few hundred euros. Another measure may be to use two webcams, one in its traditional function, that is with a close-up on the participant´s face and upper body, and the other one sitting in the corner of the room, capturing a wide-angle image that shows everything that goes on in the room. Finally, if there are indications of a possible risk under the specific circumstances, the tribunal may order the other party to send an observer to sit in the room with the witness, or delegate an observer itself. That observer can then be given special instructions about how to contact the tribunal during the conference if anything suspicious occurs. Eventually, to place this concern in context, one should not forget that silent pressure and latent threats are certainly not inexistent in face-to-face hearings either.

B. Security, privacy, and confidentiality

[Rz 353] The issue of security, which seeks to ensure privacy and confidentiality, is the subject of the most diverse reactions of practitioners. Some believe it is of the utmost importance and that every connection to the Internet amounts to a serious security risk, that one can never be sure that the data transmitted for the videoconferencing session is not being intercepted, while others state that bugging a conference room in a hotel is probably far easier than breaking into a reasonably secured videoconferencing platform. Suffice it to say that the latter are, by and large, right. From a hacker´s point of view, the task is made even more difficult by the fact that in most circumstances, the hacker will only have the time of the videoconferencing session itself to perform his or her exploit, as the data being transmitted does not remain on the platform or the server. Even if it is recorded, it will in principle be edited and prepared to be sent to the participants on a DVD (as downloading a videoconferencing session is likely to be quite

lengthy because of the amount of data involved) on a local machine, which has no reason not to be perfectly protected against intrusions. One should nevertheless always enquire about the security measures incorporated in the videoconferencing software one plans to use.[300]

C. Legal issues

[Rz 354] The legal issues raised by the use of videoconferencing are relatively unproblematic. As they have been addressed above,[301] we will only summarize here the main results in this respect:

- A technical failure in a videoconference could result in ex parte communications, which is a violation of a party´s due process right to rebut its opponent´s case. This right guarantees each party an opportunity to comment on its opponent´s case and to produce evidence in rebuttal, and also requires that the arbitral tribunal has no private or ex parte communications (communications with one party only). However, this risk can be significantly reduced by using certain tools, such as software that automatically signals when a participant is disconnected, or a direct telephone line parties can use to report a breakdown to the arbitral tribunal.

- The use of videoconferencing may also raise equal treatment issues. Under this due process right, no technology may be used that is inaccessible or too complicated to be used by both parties. A tool´s compatibility, costs of acquisition and the parties´ familiarity with it must be discussed before its use. In addition, the use of a similar size broadband connection by both parties will help avoid significant differences in transmission quality that would put one party at a disadvantage.

5. Setting up a videoconferencing session

[Rz 355] As suggested in the above, working with IT involves some technical and legal concerns that should be managed before any problem arises. This can be done by scheduling the videoconference in advance and by taking some preventive actions. The following considers some such actions.

[Rz 356] As a basic rule of thumb and urgent situations excepted, one may suggest that a videoconference session should be scheduled at least a month in advance. This will allow the parties and the arbitrators the opportunity to examine any technical problems in advance and to solve them in time. Before the conference two test phases should be carried out to ensure that things will work as expected and that the risks of breakdown are mastered.

[Rz 357] *First phase*: this phase should take place more or less at the time the conference is agreed upon, i.e. a month in advance; its goal is to determine the following features of the videoconference:

- date, time and duration;

- number of terminal stations and their location;

- number of participants present in every conference room[302] (on the day of the conference, a formal and recorded statement should be required from the parties confirming that there are no other persons in the room);

- a procedure to verify the identity of the participants, if they are not known by both parties, including witnesses and experts: e.g. showing IDs to the camera or as scanned documents, personal identification by a trustworthy and known third party, etc.;

- arrangement of the participants in relation to the camera and audio equipment[303] (due to the limited angle of webcams, it may be recommended to use a second one placed in the corner of the room showing the whole room, if hearing the individual in question requires certainty that no person is secretly in the room, for instance when hearing witnesses or experts);

- the use of support material such as physical blackboards (if no electronic blackboard feature is included in the videoconferencing software) and if any other materials or documents should be available in each conference

room.[304] If any such material is expected to be used frequently it would also be important to have a camera dedicated to it, in order to avoid having to redirect the camera each time;

- the presence or availability of technicians;[305]

- fall-back solutions in case of communication disruption: for instance duplicate computers and conferencing hardware, possibly a duplicate videoconferencing platform; or more simply an audio link-up (i.e. telephone conferencing) instead of a visual link-up; dates for a postponed meeting;

- if desired, the means of recording the videoconference and the availability of the records to the parties and the arbitrators.

[Rz 358] A *second phase* should take place thereafter, i.e. some one or two weeks before the videoconferencing session. The purpose of this second phase is to evaluate the quality and reliability of the infrastructure in place. It basically consists of a short test run: connecting all the required hardware, logging into the platform, exchanging a few words, maybe showing a few safe documents, and thereby verifying that all terminals, systems and peripherals are well configured and work correctly. This test must be done enough in advance to allow technicians to replace any material and to solve any technical issue. During this test the arbitral tribunal and the parties should familiarize themselves with the general controls, functions, peripherals necessary to log in, communicate, show documents, and use any other function provided by the platform.[306] Obviously, this is also the time to acquire missing pieces of hardware or maybe licenses to use the platform. If a party does not wish to invest in such equipment, it is possible to resort to a videoconference services provider to organize the online meeting. Such a course of action has the advantage of efficacy and efficiency, as these providers have at their disposal tested rooms and equipments, and the disadvantage of costs, as this kind of service may be quite expensive. [307]

[Rz 359] Just before the conference it is advisable that the arbitral tribunal and all other participants are in place long enough in advance to be able to receive any technical instructions from technicians.[308] Some minutes could be also used again to find one´s bearings and to toggle on and off the different components to ascertain that they work correctly and that the sound and image transmission can be disconnected if some participants wish to confer privately (the arbitrators among themselves, or a party and its counsel).

[Rz 360] During the videoconference other issues should be considered:

- light: to have a good quality image the light source, preferably artificial, should be placed behind the camera.
- corporal expression: it is necessary to avoid quick movements as the transmission rate (the number of images per second) is lower in even the best videoconferencing systems than, for instance, on television. Quick movements may thus seem jerky.[309]

[Rz 361] Meeting these guidelines is not a guarantee that no problems will arise, since technology is unpredictable, but rather a way to minimize the risks of such problems occurring.

III. Shared virtual workspaces

[Rz 362] Shared virtual workspaces are not currently used in arbitration at all. Nevertheless, it may be useful to give an insight into this technology as an exploration into possible future developments of IT in arbitration.

1. Description

[Rz 363] The following sketches the concept of a shared virtual workspace, then lists the potential uses of this technology during arbitral procedures. To help understand the main use of this technology, it then briefly describes, using a scenario, a concrete case where it may be used. Finally, it addresses the current research showing the value of sharing visual information, which is precisely what participants in shared virtual workspaces do.[310]

A. The concept

[Rz 364] Solving a dispute implies the reconstruction of what has happened, in order to determine who is right and who is wrong. Today´s cutting edge technology in computer graphics and virtual reality offers a number of tools, where, rather than trying to describe an inaccessible environment or an event using words, sketches, or pictures, the entire object or scene can be reconstructed in three dimensions, viewed from various angles and modified according to the users´ needs.

[Rz 365] A shared visual workspace is one where multiple people can see the same objects at roughly the same time. A shared visual space assists participants in understanding the current state of a task and enables them to communicate and ground their conversations efficiently. These processes are associated with faster and better task performance. Delaying the visual update in space reduces benefits and degrades performance. The shared visual space is more useful when tasks are visually complex or when actors have no simple vocabulary for describing their world.[311]

B. The uses of shared virtual workspaces in arbitration

[Rz 366] In the context of arbitral procedures, shared virtual workspaces could be used during the hearings with the parties and during the deliberations of the arbitrators.

[Rz 367] In regard to hearings, shared virtual workspaces may constitute an additional tool that increases the possibilities of the parties to make their case. In complex factual situations, the ability to share visual information about an object that forms part of the facts of the case may allow the party to make a clearer, more convincing allegation of the facts and to better explain the evidence it puts forth.

[Rz 368] After the hearings and before the award is rendered, the arbitrators usually meet–face-to-face or virtually–to discuss the case and to deliberate on the facts alleged by the parties, the evidence submitted and the rights invoked. With respect to facts and evidence, the discussion among the arbitrators may be improved if they have the possibility of sharing the visual representation of what they are discussing. One arbitrator can for instance manipulate an object–for the other arbitrators to see–to express his or her point of view on the case.

[Rz 369] The use of a shared virtual workspace may also provide the parties and the arbitrators with a better sense of reality. In addition, shared workspaces improve collaboration, as will be shown below. While it is obvious that deliberations are a form of collaboration, there is no doubt that the same is true for hearings, which imply a cooperation between the arbitrators and the parties.

[Rz 370] Figure 1 below shows the shared virtual workspace developed by MIRALab at Geneva University, currently at the experimental stage.

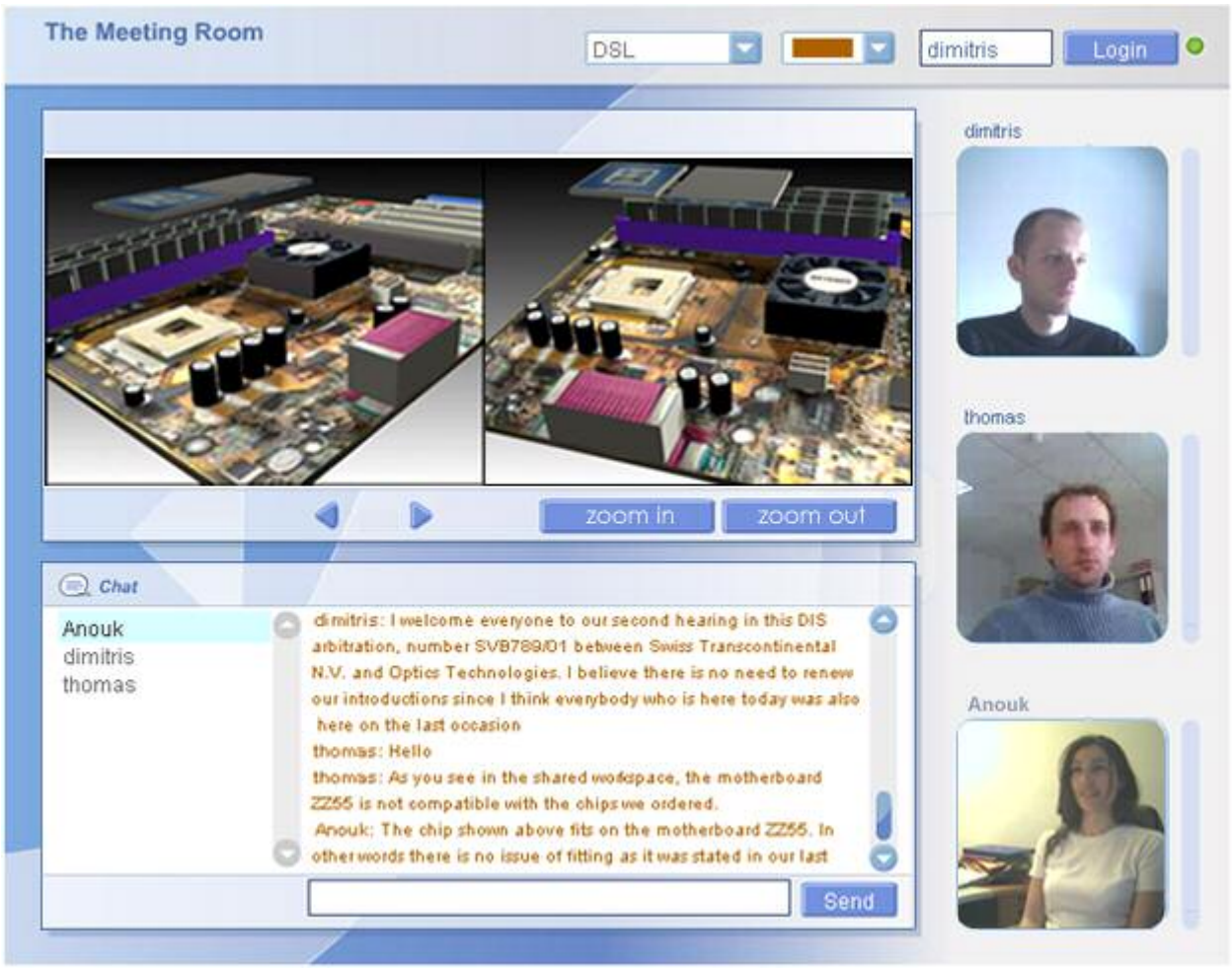


Figure 3: The arbitration environment prototype

C. A scenario of the use of shared virtual workspaces during arbitral hearings

[Rz 371] The following scenario may assist in understanding how shared virtual workspaces may be used during hearings.

[Rz 372] Let us assume that the parties and the arbitrators examine a 3D object that constitutes evidence related to the case being arbitrated. The parties, the arbitrators, the witnesses and the experts share a visual space consisting of a view of the work area rendered on each of their computer screens.

- The facts of the dispute on which this sample scenario is based are the following. Party A orders a load of custom-made computer chips, graphic cards and other interfaces from party B. A specifies that the chips must be adapted to the motherboard type ZZ55. B builds and delivers the chips, graphic cards and other interfaces. A installs them, but the computer system they are meant for does not work.

- A claims that the chips do not fit correctly onto ZZ55 motherboards, because the chips do not have the correct number of pins. B claims that A is not using the chips correctly, that the fact that the computer system does not work is due to a bad interconnection of the chips, the graphic cards and the other interfaces. The interconnection, B claims, is unusual and B could not have known that A wanted parts built for that specific use.

- The dispute is over the question of whether the number of pins constitutes a defect or not. The purpose of the 3D visualization of the motherboard and the chips, which simulate the fitting, is to help the arbitrators determine whether the number of pins is correct or not.

- Once constituted, the arbitral tribunal orders a double exchange of written briefs. The parties file these briefs, which contain their description of the facts and legal arguments, and the reactions to the statements of their opponent. After the second round of briefs, both parties, the arbitrators, the witnesses and the experts (some of which have been appointed by the arbitrators, others by the parties) gather in a shared virtual workspace for a hearing. There, the parties argue their case in turn, question the witnesses and experts, and answer the arbitrators´ questions. During the hearing, all parties utilize, among other technologies, a 3D modelling feature, which helps them explain their views or questions about the interconnection of chips, graphic cards, other interfaces and motherboards. The 3D feature allows a visual demonstration, instead of a verbal explanation, the problem from the participants´ different points of view. Finally, the arbitrators meet among themselves, using the shared virtual workspace, to deliberate upon the case.

D. The value of sharing visual information

[Rz 373] Recent research is starting to identify the conditions under which visual information is valuable, and how a shared visual environment improves communication.[312] One conclusion of this research is that the benefit of visual information comes from allowing participants to share the work area, rather than from seeing one another.

[Rz 374] This conclusion was derived first from comparing pairs performing a referential communication task using only an audio channel, with pairs working face-to-face or using an audio/video connection. Pairs could see each other, but not the objects they worked on.[313] Further research then shifted the focus from a view of the participants´ faces to the work area. Studies using this new approach differ primarily on how realistic or stylized the task is. For example, one experiment used a stylized task, in which a «Director» instructed a «Matcher» on how to construct a simple Lego form.[314] When the Director could see what the Matcher was doing, the pair was substantially faster, in part because the pair could precisely time their words to the actions they were performing.

[Rz 375] Several studies have tried to disentangle which features of shared visual space help influence its value by comparing different videoconferencing configurations to a side-by-side condition. Each videoconferencing configuration makes available a subset of the visual clues present when people are collocated [315] and thus allows testing of the value of these specific visual cues for communication and performance. For example, one experiment involved dyads repairing a bicycle while conversing side-by-side, using a head-mounted camera, or via audio only. Pairs were substantially faster when they worked side-by-side.[316] They were faster in part because they could more efficiently refer to parts of the bike when they could see the work area, while pairs in the audio-only condition spent more time coordinating their messages and acknowledging their partner´s messages.

[Rz 376] Research by Brennan and Lockbridge[317] experimentally manipulated features of the shared visual space under more rigid laboratory control. In their experiment, «Directors» instructed «Matchers» to place a series of picture cards in a specific order. Their research showed that seeing the staging or work area improved performance by enabling more rapid entrainment on pair-specific referring expressions, but that seeing the partner´s face had little benefit.

2. Technicalities of the use of a shared virtual workspace in arbitration

[Rz 377] This section seeks to model a shared virtual workspace for application to arbitral proceedings. It first identifies the different actors implied in the workspace and their functionalities.

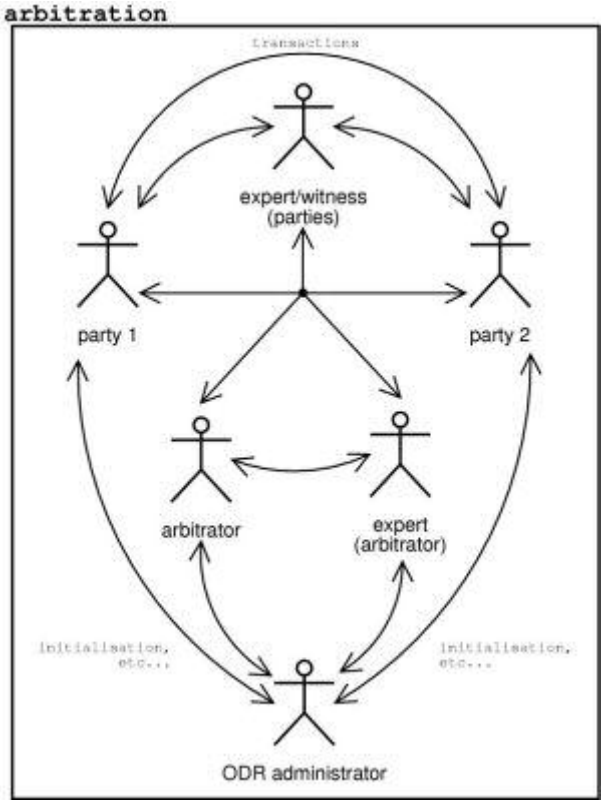


Figure 2: Communication flow in arbitration

[Rz 378] Parties, arbitrators, experts and witnesses are all directly implicated in the arbitration process. The workspace administrators are indirectly implicated in the process because they are not bound to any particular interaction but to the whole system.

A. Collaboration and sharing issues in online arbitration

[Rz 379] For coordination of interactions between participants in arbitral proceedings, seven issues are important with regard to behavior. Implications for the provision of functionality can be derived from the respective behavior desired. For example, on the technical side, the speaking permission implies a suitable floor control mechanism for coordination of the activities of participants, especially if the activities are synchronous. Table 1 lists the behavioral issues in relation to their implications for technical implementation in a groupware system.

Behavioral issues	**Implementation issues**
Who speaks during interaction?	Responsibility for creating data, audio or video information.
What is being said?	Syntax, semantics, pragmatics of information.
Who is being spoken to?	1-to-1, 1-to-many or 1-to-all communication.
When does someone speak?	Floor control, role of people.
How long and how often interaction occurs?	Simultaneous communication, bandwidth of communication.
What is the medium used during interaction?	Multimedia.
What method is used for decision-making?	Voting, negotiating.

Table 1: User behavioral issues

[Rz 380] We make the following assumptions in order to define the behavioral roles of our users:

- Only one person can speak at a time.
- The president of the arbitral tribunal has control of the floor.
- Interaction occurs only when the arbitrators allow a party to get involved.
- During interactions, users can see each other with a videoconference setup available in the system. At any time, they can mute the audio and/or video link.
- Any data (3D object) can be visualized in the virtual workspace.
- Any party can upload 3D objects to the workspace.
- Users interact with the workspace with rotate and zoom options.
- The arbitrators reach a decision after deliberations.

IV. Believability measures

[Rz 381] The goal of a virtual reality system, in our case a shared virtual space, is to simulate sensory information in such a way that the participant feels that the generated experience resembles the real world. Using the concept of «believability of the virtual environment» is one way to measure the achievement of this goal.

[Rz 382] Measuring the believability of shared virtual spaces is based upon two main elements. The first one is maintaining awareness of the task state. The second one is facilitating conversation and grounding. Grounding refers to the interactive process by which people exchange evidence about things they understand over the course of a dialogue. Thus the ability of a shared virtual space to influence those elements provides references to evaluate the level of believability of our system.

Perceptual believability measures
1. Are the collaborative parties performing a task more quickly when they have a shared view of the work area?
2. Does the shared view have more benefits when the evidence is visually complex?
3. Does the shared view have more benefits when the described scene is changing rapidly?
4. How much is the value of the shared view diminished due to the delay in transmission?
5. How much do the parties need to change the structure of their communication to be more efficient?

Table 2: Questions to evaluate the shared view

V. The technology

[Rz 383] Replicated application sharing is a very flexible technique for collaboration. In replicated application sharing, separate copies of single-user applications are run on each collaborator´s computer. Events from one copy (e.g., mouse events, keystrokes) are broadcast to the other copies where they are processed as if they had been generated locally, allowing the distributed applications to stay synchronized (see figure 3).

[Rz 384] Since our application needs to send only information that has changed, we divide the data among multiple slots. This implementation reduces network traffic and thus enhances the performance of the application. It also minimizes the need for conflict resolution code, as multiple slots can be updated simultaneously without data collision.

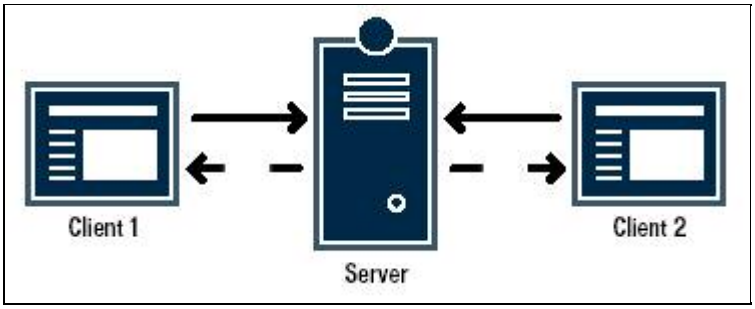


Figure 3: Shared objects

[Rz 385] Since more than one client (or a server application) can change the data in a single slot of the shared object at the same time, we had to implement a conflict resolution strategy. We defined a single client as the owner of a property in the shared object for a limited period of time. We implemented a server code to create a «lock» object, where a client can request ownership of a slot. When the server reports that the request was successful, the client knows that it will be the only client changing the data in the shared object.

[Rz 386] We used the Macromedia Communication Server MX 1.5 platform to build our shared objects. The system is made up of two parts: the server, which provides the means of communication, and Macromedia Flash Player. The application consists of a client Macromedia Flash movie (SWF) and a server component that communicates with the client. The server component consists of an application folder we created on the server running Communication Server. The server and the client communicate over a persistent connection using Real-Time Message Protocol (RTMP). In our scenario, the Flash client is delivered to the Flash Player by a web server over HTTP. The Flash client then establishes a persistent connection to Communication Server using RTMP, allowing an uninterrupted data stream to flow between client and server.

CHAPTER 5

PRACTICE GUIDELINES

[Rz 387] The preceding chapters discuss a number of technologies which may be used in relation to arbitration proceedings, explaining how they operate, what their advantages and disadvantages are, in which situations they may best be resorted to, and how they should be used. Drawing on such discussions, this chapter presents guidelines, as a convenient reference tool in practice. It seeks to address the different situations in which a practitioner may face questions related to the use of IT in arbitration. As a result some topics, which come up in different situations, are addressed more than once in different places.

[Rz 388] This chapter begins with a protocol for the use of information technology, i.e. an overview of which technologies can be used in different aspects of arbitration proceedings. The second section of this chapter consists of several checklists to be used either when planning for or resorting to IT. The third and fourth sections suggest recommendations related to the drafting of arbitration agreements providing for the use of electronic communication technologies during the proceedings, and procedural forms and orders. This chapter then contains a section explaining concretely how to use encrypted e-mails and digital signatures. Finally, a review of ad hoc videoconferencing systems is provided.

I. Communications protocol

[Rz 389] Different aspects of an arbitration procedure correspond to different types of communications, which all require or allow for specific technologies. Organized according to the main types of communications usually taking place in arbitral proceedings, this section suggests recommendations for the most frequently used technologies. Before doing so, it asks however a threshold question, i.e. who decides about the use of IT in arbitration?

1. Who decides?

[Rz 390] Before entering into the substance of the It solutions, a threshold question arises: who decides about the use of IT in arbitration? In theory, the answer is the same as for any procedural matter: the parties, if they agree and if they do not agree, the arbitrators. In practice, the answer is more nuanced. Even if the parties agree, it would be preferable to secure the arbitrators´ approval before making a final choice. Indeed, forcing an IT option on an unwilling arbitrator, is unlikely to further the _smooth conduct_of the proceedings. It is not devisable either that computer-literacy and It considerations become the prevailing issues when choosing an arbitrator. Other factors (e.g., expertise, experience, availability, nationality) are undoubtedly more important for the management of the arbitration and the quality of the outcome. Hence, the practical answer to the threshold question may be further elaborated as follows:

- if the parties wish to resort to an existing case management website such as NetCase or ECAF, they may certainly so agree in advance without first seeking the Tribunal´s consent. Indeed, these applications, ready-made and user-friendly, are likely to become common practice and arbitrators should accept using them;

- if the parties wish to use other institutional procedural rules on the use of IT they may state so in general terms, but should leave the actual implementation to be discussed with and, if need be, determined by the tribunal;

- if the parties wish to use IT means without reference to specific rules, they may state so, e.g. by providing that hearings may be held by videoconference or that submissions may be filed electronically and that specifications will be agreed upon or decided by the tribunal at the outset of the proceedings.

[Rz 391] The following sections must be read bearing these clarifications in mind. The parties may consider the different uses of IT and its practicabilities and make joint or separate proposals to the tribunal. In response to proposals or if no proposals are forthcoming out of its own initiative, the tribunal may review the available options and make suggestions, usually by submitting a draft procedural order providing for IT solutions to be discussed at an initial procedural hearing.

2. Submissions (briefs, memorials, applications). and documentary evidence

[Rz 392] The parties and the arbitrators should examine different methods of sending documents, such as by mail, fax, e-mail with or without attachments; on diskettes and/or CD-Roms (labeled with contents, author, intended recipient, date, compression software used if applicable). The size of a document and the availability of document compression systems should also be taken into consideration in choosing one method or another. Generally, it is impractical to send and receive very long documents such as memorials with or without exhibits by e-mail (the same is true for fax transmissions). Hence, it is preferable to provide that such documents will be communicated on a CD-Rom, with or without a paper version depending on the wishes and habits of the tribunal members, counsel and party representatives

[Rz 393] When using electronic methods, the parties should also think about the format of the document and whether to use doc, pdf or rtf formatting, and maybe specific software for word processing and spreadsheets. It is recommended to use either pdf or rtf format.[318]

[Rz 394] If parties intend to use electronic means as their primary method for filing documents, they should define an alternative backup method for sending them, such as postal mail or fax, in the event of difficulties with the electronic means. A safe solution is to send a hard copy of the most important documents by post or special courier after they have been sent electronically. That solution has the disadvantage, however, of practically defeating the efficiency that electronic communications may otherwise achieve.

[Rz 395] The parties should also decide on other aspects of document submission, such as preparing a database of documents (including the allocation of costs for creating this database), labelling and identifying files and physical data carriers such as diskettes and/or CD-Roms, checking for viruses (specifying the anti-virus software to be used)

before sending a document, and acknowledging the receipt of an e-mail and/or document (frequently an e-mail reaches the addressee but the attachment cannot be opened).

[Rz 396] Security is another important issue that should be discussed by all parties, including the methods for authentication and non-repudiation, and encryption technologies. When deciding on such items, the parties should specify the procedure to be followed. The parties may also define a certain protection technology to be used against internal and external security threats, in order to prevent documents from being intercepted.

3. Other communications

[Rz 397] Any other communications, be it from the parties to the tribunal, between the parties with copy to the tribunal, from the tribunal to the parties, can generally be handled by e-mail (or fax). All explanations given with respect to e-mails apply to these other communications as well.

4. Hearings

[Rz 398] To prepare hearings adequately, the parties and arbitrators should first agree on which situations call for which type of meeting: in person, videoconferencing, or teleconferencing.

[Rz 399] If teleconferencing or videoconferencing is to be used, all required documents should be made available to the participants, which may for instance be achieved by a case-management system, by the file-sharing application of the videoconferencing software, by e-mail if the number of documents is limited, or on a CD-Rom or another physical data carrier if recourse to IT is to be kept to a minimum or some of the data require software different from the one agreed by the parties (such software can then be included on the data carrier). This data carrier should be sent by registered mail specifying the compression system used.

[Rz 400] If videoconferencing is used for hearings, a number of recommendations should be followed. They are set forth in the proposed procedural order below. They include providing a list of the persons to attend the conference, the situation of the cameras (location, angle, rooms in which they are installed), the identity of all persons who are in the same room as the participants, the authentication of the identity of the participants who are not known by another trustworthy participant, the documents to be shown, etc.

5. Deliberations between arbitrators

[Rz 401] The arbitrators are free to decide how they intend to organize their deliberations and in which form they will hold them. This being said, the parties and the arbitrators may wish to address specific provisions regarding the treatment of confidential documents for the event that deliberations or the drafting of the award are made electronically. In this case, the parties and the arbitrators should agree on a protocol for protecting against interception (password-protected documents, encryption, etc).[319]

6. Form and notification of the award

[Rz 402] An arbitral award should always be sent in paper form. For the sake of convenience an advance copy may be sent in electronic format. However, the still uncertain status of the validity of awards in electronic form suggests that the absence of paper may lead to difficulties at the stage of enforcement or recognition.[320] As this safety measure is easy to implement and does not generate any significant cost, it should always be respected, even if the idea that arbitral proceedings may be carried out entirely online seems an attractive concept.

II. Checklists and reminders

[Rz 403] This section aims at reminding the practitioner about the main questions that should be posed either when planning for IT-usage or when actually resorting to such technologies. By nature, it cannot to be exhaustive. It is organized in three parts: first, it provides main recommendations that essentially relate to all forms of IT-usage. Second, this section reviews the main elements related to the use of e-mails, suggesting which precautions should be taken while sending and receiving e-mails. Third, it suggests steps to follow when planning for and organizing a videoconference.

1. Main tasks

[Rz 404] In general:

- Take time to plan for and organize IT usage, especially if it involves a technology that participants are not familiar with (e.g. a videoconferencing session should never be scheduled without providing for time to test the equipment and remedy any unsatisfactory aspects);
- Before using a new technology, take time to test and play with it, as not having mastered it may constitute a significant disadvantage and waste of time;[321]
- Have IT support available at all times, in case of technical deficiencies (a risk which can never be totally suppressed);
- Have back-up solutions available;[322]
- Keep IT solutions as simple as possible.[323]

[Rz 405] The parties:

- Consider the respective advantages of resorting to institutionalized IT services (ICC, AAA, WIPO)[324], which require less time investment, or implementing ad hoc IT solutions, which may be tailored more precisely to the specificities of the case and the parties;
- Use very broad technical provisions in pre-dispute arbitration agreements;
- Use broad technical provisions in post-dispute arbitration agreements;
- Do not bind as yet unknown tribunal to specific IT solutions.

[Rz 406] The tribunal:

- Consult with counsel and render a procedural order on the use of IT covering:[325]
  - Exchange of electronic documents;
  - Admissible file formats;
  - Available fonts;
  - File naming and classification system;
  - Scanning documents not available electronically;
  - Breakdown management;
  - Videoconferencing;
  - Costs allocation for the acquisition and use of IT tools; and
  - Revision of technical rules if needed.
- When ordering the selection of a given technology, provide a clear description of the process in a complete and easily understandable manner.
- Always conduct the proceedings ensuring that the use of IT does not deprive a party from:
  - A real opportunity to present its allegations of facts, submit legal arguments, and tender pertinent evidence on relevant facts.
  - A real opportunity to rebut the opponent´s case, which implies equal access to the record and that the arbitral tribunal does not have *ex parte* communications with any party.

2. E-mailing

A. Sending e-mails

- Give the e-mail a descriptive title;
- Mark an e-mail as important only if it really is;
- Preferably use text format rather than HTML for the e-mails;
- Use a final signature indicating phone numbers to call in case of technical problems;
- Check language once again;
- Double-check the addressee(s), also in cc and bcc options;
- Use rtf, .pdf or .html format for attachments;
- Remove unnecessary attachments;[326]
- Check the existence of metadata in attachments (i.e. check if the option «Track changes» is on, check information in the «File/Properties» section, and maybe use a meta-data remover); [327]
- Check attachments for viruses (if not automatic);[328]
- Protect confidential files sent as attachments with a password;
- Consider using a digital signature;[329]
- Consider using encrypted e-mails.[330]

B. Receiving e-mails

- Use the preview option if available;
- Do not open any suspicious attachment of any e-mail—e.g. be cautious when following a URL address or opening a .exe or even a .doc file, as they may contain viruses; [331]
- Classify e-mail efficiently;
- Always acknowledge receipt.

3. Videoconferencing

A. General reminders

- Videoconferencing is *not a perfect substitute* for in-person interactions, as it does not transmit all elements of nonverbal communication. For example, it may take users a few minutes to get used to the lack of «normal» eye contact during a hearing that may make it more difficult to direct attention clearly. [332] Unexperienced participants should be informed of this beforehand.
- *Sufficient broadcast quality* (i.e. sufficient line speed and CPU power) must always be provided, as low-quality image transmissions will make it difficult to establish on inter-personal rapport and may cause frustration and be counter-productive.[333] What constitutes a sufficient broadcast quality depends on the videoconferencing platform being used, but as a general rule one may recommend opting for 400-500Kbps for both sending and receiving and, for CPU, at least a Pentium III and preferably a Pentium IV.

B. Videoconference or in-person meeting?

[Rz 407] The advisability of meeting by way of videoconferencing rather than in person depends on a variety of factors, including the general constraint on costs and time, the geographical distance between the parties, the availability of the participants, and the contents of the meeting. For detailed explanations of these elements, the reader is referred to their earlier discussion above. [334] For present purposes, it will suffice to give a summary overview of the situations in which it seems a priori advisable or not to consider videoconferencing.

- The following situations or factors may in general call for videoconferencing:
  - Hearing a witness who cannot be present at the location of the hearing;
  - Allowing an arbitrator or counsel who is prevented from attending in person (e.g., because of cancellation of flight) to participate rather than having to postpone the hearing;
  - Evaluating and preparing a witness;
  - Long distances separate the parties and the dispute is of low value;
  - The collective drafting or editing of a document whose contents are not sensitive enough to require the presence of all drafters (certain contracts, for instance);

  - Finalizing the terms of reference and procedural calendar or dealing with other procedural issues with the parties when an in-person meeting is not possible/desirable;
  - Deliberations among the arbitrators;
  - Meetings among co-counsel;
  - Hearings in certain expedited proceedings;
  - Hearings on interim measures;

- On the contrary, if the following factors are present, videoconferencing is inappropriate, and in-person meetings should be preferred:
  - Perception of state of mind of the participant(s) is important (e.g., examination of a crucial witness suspected of hiding facts);
  - A very large number of documents is to be used;
  - The situation requires visual perception and the parties are absolutely inexperienced with videoconferencing technology and cannot provide sufficient guarantees in relation to the preparation of such a conference;
  - The parties and the arbitrators have never met and it appears desirable for them to have an opportunity to meet in person, especially at the early stage of the arbitration.

[Rz 408] Some situations may at the same time call for videoconferencing because of one factor and oppose it as a result of another factor (e.g. hearing a witness whose state of mind needs to be precisely assessed but who cannot travel to an in-person meeting without causing major delays in a time-driven procedure). In such situations, a part of the solution follows from other factors, such as the experience of the participants with videoconferencing (as it becomes easier with experience to assess a state of mind through this technology).

C. Preparing a videoconference

[Rz 409] A videoconference takes time to prepare. The exact amount will depend on the contents of the hearing and on the experience of the participants with the technology. For experienced participants, i.e. for persons who have already used the same technology on the same computers and the same Internet lines several times, setting up a videoconference may not require any more preparation than organizing a teleconference. As a rule of thumb, for inexperienced parties, one may suggest the following time-line: [335]

- About 30 days before the scheduled conference, determine:
  - Date, time, and duration;
  - Number of terminal stations and their location;
  - Number of participants in each conference room;
  - Procedure to determine the identity of the participants;
  - Physical position of the equipment in relation to the participants;
  - The presence and availability of technicians;
  - Alternatives in case of communication disruption;
  - Whether and how the videoconference should be recorded.

- One week before the conference, run a test, which involves:
  - Connecting the required hardware;
  - Launching the application and logging into the server;
  - Exchanging a few words to test the audio capacity of the system (time-lag, clarity, volume, sound disruptions);
  - Showing irrelevant documents.

- Half an hour before the conference:
  - Have a technician ready and at hand;
  - Launch the application and connect to the server;
  - Toggle in and out the components;
  - Check lighting (should be behind the camera and bright enough);
  - Mute microphone in order not to be overheard during the preparation for the conference and turn camera

to show an irrelevant image, while waiting for the other to connect;
- Possibly upload to a private part of the server the documents that will be shown during the conference.

- During the conference:
  - Avoid quick movements;
  - Be disciplined and wait for one´s turn to speak.

III. Drafting suggestions for arbitration agreements

[Rz 410] This first section provides advice on the way to provide for IT-usage in arbitration agreements. This topic is examined in relation to both pre-dispute clauses and post-dispute agreements, and ad hoc as well as institutional arbitration.

1. Pre-dispute arbitration agreement referring to the use of IT tools

[Rz 411] Generally speaking, pre-dispute arbitration agreements providing for IT-usage should not be too precise. The main reason for this is that technology evolves; the available IT tools may change quite radically between the time an arbitration agreement is signed and the start of the proceedings. It may nevertheless be helpful to mention in the parties´ intent to resort to IT in the arbitration agreement already.

[Rz 412] In this respect, one should distinguish between an arbitration clause providing for arbitration administered by an institution offering IT services, such as the ICC, the AAA, or WIPO, and arbitration by an institution making no such services available or ad hoc arbitration. In the former case, reference should be made to the services offered by the institution chosen, more precisely to the pertinent rules of the institution. If such rules offer several alternatives, it will most often be preferable not to effect a strict choice at the time of entering into the contract. Moreover, the parties should avoid specifying the procedural rules and IT services as they stand at the time of the conclusion of the contract. Indeed, technologies that are outdated at the time they come into play may do more harm than good.

[Rz 413] If the arbitration clause provides for *ad hoc* arbitration or arbitration under the auspices of an institution which offers no IT services, it may make sense to provide for a duty to consider the use of IT and to negotiate its implementation, at the outset of the proceedings. The wording of such a provision may for instance be as follows:

> «In the event of any dispute arising out of or in connection with the present contract, the parties agree to refer such dispute to arbitration by […] In relation to such arbitral proceedings, the parties agree to discuss and consider resorting to electronic means of communication.»

2. Post-dispute arbitration agreement referring to the use of IT tools

[Rz 414] Post-dispute arbitration agreements providing for IT-usage may be more precise than pre-dispute agreements. Nevertheless, arbitral proceedings may have a long duration and a door should be left open in case technology evolves significantly during the proceedings and a new instrument becomes more appropriate.

[Rz 415] Here again a distinction must be made between arbitrations administered by an institution offering It services and other arbitrations. In the first case, the parties may of course agree to resort to the IT procedural rules of a specific institution (ICC, AAA, WIPO). In such event, it is advisable to use the standard clause proposed by the institution.

[Rz 416] If the parties choose *ad hoc* arbitration or other institutional arbitrations, they may provide for IT-usage in their agreement. However, the provision should not give detailed specifications. These should not be determined without prior consultation with the members of the arbitral tribunal, as it would not make sense to provide for solutions with which the arbitrator is not willing to work. Hence, the following wording may be appropriate:

> «The parties agree to use IT means of communication for submissions, including exhibits, and other communications. They also agree to hold hearings by videoconference whenever appropriate. They shall request the tribunal to give pertinent directions after communication with the parties.»

IV. Drafting suggestions for procedural forms

[Rz 417] This section provides two types of standard procedural forms: forms to be used by the parties to initiate IT-usage (i.e. to propose the use of specific technologies during the procedure) or to report a technical problem to the other party and the arbitral tribunal, and a standard procedural order by which the tribunal makes a determination as to which technology will be used.

1. Sample procedural forms for the parties

[Rz 418] The first form provided below is to be used by one party to suggest the use of IT to the other party and to the arbitral tribunal, with a mention of preferences for specific technologies. It may be noted that the arbitral tribunal must in principle abide by the IT agreement of the parties and use the technologies specified therein. The form is thus meant as a basis of negotiation for the parties. The idea is that once the proposing party has filled in the form, it should be sent to the other party, jointly with a blank copy, so that the addressee can in turn fill in the fields. This will allow a good evaluation of the technical capabilities of the parties and help focus their attention on the aspects of IT-usage that they may want to defined in advance.

[Rz 419] The second form is to be used in case of a technical deficiency, to alert the sender of an electronic communication of the poor reception of the communication or lack thereof.

[Rz 420] Both of these forms, and especially the second one, are inspired by those of the ICC, as published in the 2004 Special Supplement on «Using Technology to Resolve Business Disputes» to the ICC International Court of Arbitration Bulletin. However, the forms provided here are largely simplified with respect to those of the ICC (especially the first one), so as to be accessible to persons who are not IT-specialists.

A. Initiation form

Case _____

Reference _____ Our reference _____

Date _____

Participant initiating IT-usage _____

Contact details:

- Participant initiating IT-usage: _____
  _____
  _____
- Technician in charge: _____
  _____
  _____

This initiation form is sent to the following persons and/or entities:

Name	_____	Name	_____
Address	_____	Address	_____
	_____		_____
Telephone number	_____	Telephone number	_____
Fax number	_____	Fax number	_____
E-mail address	_____	E-mail address	_____

Name	_____	Name	_____
Address	_____	Address	_____
	_____		_____
Telephone number	_____	Telephone number	_____
Fax number	_____	Fax number	_____
E-mail address	_____	E-mail address	_____

The IT solutions mentioned in this form relate to the following areas:

- Technologies to be used for communications
- Specifications regarding the format of electronic documents
- Specifications regarding the naming of electronic documents
- Specifications regarding videoconferences
- Form of the award

1. Technologies to be used for communications
1.1 We propose that all notifications and communications other than written memorials and exhibits be made by:

- Standard e-mail
- Secure e-mail (encrypted and digitally signed)
- Using the following case-management website:
- On a CD-Rom
- On a DVD

- All transmissions in one of the formats listed above must be accompanied by a paper copy, sent on the same day as the electronic copy
- All transmissions in one of the formats listed above must be accompanied by a notification by fax providing that the electronic copy has been sent

1.2 We propose that all memorials and exhibits be exchanged by:

- Standard e-mail
- Secure e-mail (encrypted and digitally signed)
- Using the following case-management website:
- On a CD-Rom
- On a DVD

- All transmissions in one of the formats listed above must be accompanied by a paper copy, sent on the same

day as the electronic copy
- All transmissions in one of the formats listed above must be accompanied by a notification by fax providing that the electronic copy has been sent

2. Specifications regarding the format of electronic documents

- We propose the use of the following formats for electronic documents:

Type of document	***Format***
Text documents	DOC
	RTF
	PDF
Spreadsheets	XLS
Images	JPEG
	GIF
	BMP
Sounds	MP3
	WAV
	AIFF
	WMA
Video	AVI
	MPEG
	MOV
	DivX

2. Specifications regarding the naming of electronic documents

- We propose the following system to name documents:

XY.000.----------.DDMMYYY.***

Where:

- XY is the abbreviation of the sender, where
  - CL is the claimant
  - RD is the respondent
  - CH is the chairman of the arbitral tribunal
  - AC is the arbitrator appointed by the claimant
  - AR is the arbitrator appointed by the respondent
  - AT is the arbitral tribunal as a whole
- 000 is the abbreviation of the nature of the document according to the following categories:
  - MEM: memorial
  - DEV: documentary evidence
  - OEV: oral evidence (transcript or audio recording)
  - AWA: award
  - POR: procedural order
  - NOC: notice and communication
  - OTH: other documents
- ---------- is a short description of the document
- DDMMYYYY is the date of production of the document
- *** is the format of the document

3. Specifications regarding videoconferences

- We propose the use of the following videoconferencing system:
  - Name of system:
  - Approximate costs involved for each participant (in addition to equipment):
  - Equipment required:
  - More information available at:
- We have tested the system and certify that we have the equipment necessary to use it.

The preparation of videoconferencing sessions will in principle, except specific agreement by both parties, follow these steps:

Action[336]	Time before conference
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

4. Award

We propose that the arbitral tribunal forward a copy of the award to the parties in ___ format.

Such an award shall have only informational purposes. It shall not constitute the original award, which will be sent in paper form.

B. Incident form

Case _____

Reference _____ Our reference _____

Date _____

Participant initiating IT-usage _____

Contact details:

- Participant initiating IT-usage: _____
  _____
  _____
- Technician in charge: _____
  _____
  _____

Copies to:
-
-
-

DESCRIPTION OF THE INCIDENT

A. Date of the incident:
B. Time of the incident:
C. Person that detected the incident:
D. Areas concerned by the incident:

Technologies to be used for communications
Specifications regarding the format of electronic documents
Specifications regarding the naming of electronic documents
Specifications regarding videoconferences
Form of the award

E. Detailed description of the incident:

F. Suspected origin of the incident:

G. Proposed solution:

2. Procedural order relating to the use of IT[337]

ARBITRATION _____ ____(DATE)___

Party A

v.

Party B

PROCEDURAL ORDER N. __

The Arbitral Tribunal, having consulted with the parties, directs that the following procedural rules on the use of IT shall apply to these arbitration proceedings.

1. DETAILS OF PARTIES AND ARBITRATORS

1.1 Claimant

Recipient 1: Name: _____
Address: _____
_____
_____
Fax: _____
E-Mail: _____

Recipient 2: Name: _____
Address: _____
_____
_____
Fax: _____
E-Mail: _____

1.2 Respondent

Recipient 1: Name: _____
Address: _____
_____
_____
Fax: _____
E-Mail: _____

Recipient 2: Name: _____
Address: _____
_____
_____
Fax: _____
E-Mail: _____

1.3 Arbitral tribunal

Chairperson:	Name:	_____
	Address:	_____
		_____
		_____
	Fax:	_____
	E-Mail:	_____
Arbitrator appointed by Claimant:	Name:	_____
	Address:	_____
		_____
		_____
	Fax:	_____
	E-Mail:	_____
Arbitrator appointed by Respondent:	Name:	_____
	Address:	_____
		_____
		_____
	Fax:	_____
	E-Mail:	_____

2. NOTIFICATIONS
2.1 All notifications and communications other than written memorials and exhibits shall be made by e-mail.
2.2 Notifications subject to a time limit and made by e-mail shall be accompanied by a fax stating that the e-mail has been sent.
2.3 Notifications made by e-mail to the parties shall be deemed received upon arrival of the e-mail in the recipient´s e-mail server, at the local time of the recipient. Notifications made to the arbitral tribunal shall be deemed received upon arrival of the e-mail in the chairman´s e-mail server, at his local time.

3. SECURITY
3.1 E-mails shall be encrypted.
3.2 E-mails shall be digitally signed to authenticate the identity of the sender.
3.3 Before sending an e-mail, it shall be checked using a standard and up-to-date anti-virus software.
3.4 All the stations used during these proceedings shall be equipped with a firewall providing adequate security.

4. WRITTEN MEMORIALS AND EXHIBITS

4.1 Written memorials and exhibits shall be submitted in the following form [choose one, two or more options] [338]:

[- E-mail accompanied by a paper copy]
[- E-mail accompanied by a copy on CD-Rom or DVD]
[- CD-Rom or DVD]
[- In paper copy]

4.2 All submissions mentioned in Paragraph 4.1 shall be sent at the latest on the last day of the time limit. Submissions in paper or on electronic carrier (e.g. CD-Rom or DVD) shall be sent by special courier.

4.3 All submissions sent by e-mail shall be subject to the provisions of Section 3 above. Submissions made by

e-mails accompanied by a copy on paper or electronic carrier (e.g. CD-Rom/DVD) shall be deemed received at the time of arrival of the e-mail in the recipient´s e-mail server, at the local time of the recipient.

4.4 All documents not available electronically may be scanned and saved in .pdf format.

4.5 In addition to the virus check of e-mails under Section 3 above, the parties shall check for viruses, using appropriate software, any written submission or document that is intended to be attached to an e-mail or to be saved on a CD-Rom/DVD, diskette, USB drive, or any other physical data carrier.

4.6 Files shall be identified according to the following formula:

XY.000.----------.DDMMYYY.***

Where:

- XY is the abbreviation of the sender, where
  - CL is the claimant
  - RD is the respondent
  - CH is the chairman of the arbitral tribunal
  - AC is the arbitrator appointed by the claimant
  - AR is the arbitrator appointed by the respondent
  - AT is the arbitral tribunal as a whole
- 000 is the abbreviation of the nature of the document according to the following categories:
  - MEM: memorial
  - DEV: documentary evidence
  - OEV: oral evidence (transcript or audio recording)
  - AWA: award
  - POR: procedural order
  - NOC: notice and communication
  - OTH: other documents
- ---------- is a short description of the document
- DDMMYYYY is the date of production of the document
- *** is the format of the document

5. HEARINGS, WITNESSES AND EXPERTS

5.1 This section shall apply to any hearing or portion of hearing to be held by videoconference.

5.1.1 At the request of either party or of its own motion, the tribunal may direct that a videoconference may be held for the hearing of witnesses of fact, expert witnesses, oral arguments, procedural session, or any other purpose. Except in urgent situations, such as the scheduling of a hearing on interim measures, the tribunal will give the parties at least one month advance notice. When ordering the videoconference, the tribunal will address the following elements:

5.1.1.1 Date, time, and anticipated duration of the videoconference.

5.1.1.2 Purpose of the videoconference.

5.1.1.3 Identification of terminal stations.

5.1.1.4 Participants at each station, including whether an observer of one party may be present.

5.1.1.5 Identification of the files, documents, and notes that may be available at each station, especially to witnesses and experts testifying by videoconference.

5.1.2 At least one week before the scheduled videoconference, the tribunal and the parties shall run a test to evaluate the infrastructure and the capabilities of the network.

5.1.3 During the videoconference, the participants [or the witness] shall always be in view of the camera. [One camera shall be placed to provide a view of the entire room.]

5.1.4 Unknown participants shall identify themselves showing a piece of identification to the camera. The tribunal may request other forms of identification.

5.1.5 A technician shall be present [available] at every station, whose identity shall be communicated to the tribunal at least three days before the videoconference.

5.1.6 The videoconferences shall be recorded (image and sound).

5.1.7 In case of failure of the videoconferencing system, the tribunal shall reschedule the videoconference or take any other appropriate step.

6. AWARD
Awards shall be notified to the parties by registered mail or special courier. The tribunal, at its discretion, may circulate a copy by e-mail for informational purposes.

7. COSTS ALLOCATION
Each party shall provisionally bear the costs that it incurs to comply with this order. The parties shall advance in equal shares the costs incurred by the tribunal to comply with this order. The tribunal will make a final cost allocation in the award, taking into account all circumstances, e.g. the extent to which each party had available or lacked the required equipment (software and hardware) at the outset of the arbitration and possible future uses of acquisitions made for these proceedings.

8. EXCEPTIONS AND REVISION OF THESE RULES

8.1 Upon a reasoned request, the tribunal may authorize a party to transmit a notification, communication, memorial or exhibit in a format or using a program different than those provided for herein. Subject to contrary directions from the tribunal, the party so authorized shall provide the other parties and the tribunal with all necessary hardware, software and technical support at its own expense.

8.2 The arbitral tribunal may proceed to revise, amend and complete these rules at any time during the procedure. [Upon request of a party or of its own motion, the tribunal may in particular, after consultation with parties, provide for the use of new technologies.]

Place and date
Signatures

V. Setting up encrypted and digitally-signed e-mail

[Rz 421] Imagine you are in a country whose government you do not trust and you need to exchange e-mails with your secretary or team in an arbitration involving that government. Or one of the recipients of your e-mails relating to an arbitration is located in one such country, be this person a witness, an expert, a party, member of a team of counsel, arbitrator, secretary. In such case, but also if you simply have special security concerns,[339] extra security measure may be required. The most obvious measure is the use of encrypted e-mails. As the technology to produce such e-mails is very similar to digitally signing e-mails, the following present concrete examples of how to set up the related programs.

[Rz 422] The following is organized in two parts. This first part relates to e-mail clients, which are e-mail programs on a computer that download e-mails to the hard-disk. The best known programs are Outlook, Lotus Notes, Eudora, Mozilla Thunderbird, or Pegasus Mail. The procedure which needs to be followed in order to set up encrypted and digitally signed e-mails is similar for each program. This section provides specific instructions for the most widely used e-mail client. The second part below concerns webmails, which are web-based or browser-based e-mail applications, such as Hotmail and Gmail. In this context, specific instructions are provided in relation to one of the

rare webmails that supports encryption and digital signatures, i.e. HushMail.

[Rz 423] This part will not provide explanations on the operation of encryption and digital signatures, public and private keys, as this has been discussed extensively above.[340]

1. E-mail clients: setting up Outlook

[Rz 424] The first step before sending a secured e-mail is to obtain a digital certificate. . There are three possibilities:

- First you can create your own digital certificate using Selcert.exe. These certificates are considered non-authenticated, however, and a computer will issue a security warning if its security level is set to medium or high. To create a self certificate:
  - Launch the file called Selfcert.exe.
  - If you do not find it, use the search tool in the Start menu.
  - Once you find it, double click on it and the following window will appear:

- Enter the name of your certificate

- Second, you can also obtain a certificate from a commercial authority. There are a number of authorities which provide this service: VeriSign, Inc; AOL; Securesign; SecureNet; and others. These certificates must be paid for, and the price varies greatly depending on the duration and trustworthiness of the certificate. To get a digital certificate, you will be asked to submit a request providing information about your company. It will then be necessary to install the certificate.

- Third you can obtain an internal certification if your company has its own administrator acting as certification authority for your company.

[Rz 425] Once you have a digital certificate you can write your e-mail. Before sending it, it will be necessary to modify the security parameters. To do this click on the **Options** bar.

[Rz 426] Then click to modify the security parameters. The following window will appear:

[Rz 427] Select the different options to encrypt the attachments and to add a digital signature. If you wish an acknowledgment of receipt also select this option.

[Rz 428] Then, click on security parameters to modify them in case the one appearing is not the correct one. On the following window, you will have the option to choose the certificates for the digital signature and for the encryption.

[Rz 429] Once you have completed these steps, you may proceed to send an e-mail as usual.

2. Webmail: resorting to HushMail

[Rz 430] Most webmails, i.e. most websites providing access to e-mails, do not support sophisticated security technologies such as e-mail encryption and digital signatures. The reason is that the process of encoding the message

(using a private key on a specific part of the message for digital signatures and using a public key on the entire contents of the message for e-mail encryption) is a rather complex operation, which is considered too arduous by most webmail providers because of the high volume of e-mails they process.

[Rz 431] Moreover, it is in principle not possible to add encryption or digital signature features to webmails that do not originally support it (for instance hotmail or Gmail). Hence, if one insists on using webmail instead of an e-mail client, the only solution is to create an account with a webmail provider that supports such technologies, and maybe to set up a connection between the new webmail and the one the user usually utilizes (auto-forward, redirection, automated reception notification, etc). The following explains how to do this with such a webmail provider, i.e. Hushmail.

- The first step is to create an account with Hushmail:
  - go to www.hushmail.com;
  - click on «Create Free E-mail Account»;
  - choose your e-mail address @hushmail.com (or other Hushmail domains);
  - accept the security certificate;
  - enter a passphrase;
  - generate random data to create a pair of keys (one public, one private), which is achieved by randomly moving the mouse within a specific field prompted by the website.
  - either upgrade to premium services (for a fee of 10-20 euros; the advantage is primarily the absence of a time limitation for the use of the webmail and storage space) or use the free services.

- Next, create a connection between your ordinary webmail and Hushmail:
  - log in to www.hushmail.com;
  - click on «Preferences»;
  - click on Preferences Index -> 7. E-mail Notification;
  - check the box «enable notifications at an alternate e-mail address when you receive mail at this address»;
  - enter the e-mail address corresponding to your ordinary webmail, which will receive an alert if you have received an encrypted or digitally-signed e-mail on your Hushmail address.

- To send encrypted e-mails, you will in principle need to ask your recipient to upload his or her public key to Hushmail´s keyserver. An easier alternative, but not as satisfactory, is to enter a secret question and answer—the recipient will have to provide the secret answer in order to decrypt the message. To do this, simply click on «Compose Message Options». Reverting to the first solution, in order to upload the public key to Hushmail´s keyserver, the recipient should follow these steps, as described by Hushmail: [341]
  - export his or her public key in text format;
  - go to www.hushtools.com -> Key Management -> Advanced -> Upload a public key;
  - paste the public key in text form in the box indicated;
  - the website then requires associating the uploaded key with an e-mail address.

- For you to be sent encrypted e-mails, the sender will simply need to download your public key from Hushmail´s keyserver, which for recent versions of encryption software means following these steps: [342]
  - right-click the PGP icon in the system tray;
  - select Options -> Servers -> New -> PGP Keyserver LDAP;
  - enter «keys.hush.com» in the «Name» field, and click OK.

- To send digitally signed messages:
  - the sender simply needs to click on Compose -> Message Options -> Sign Message;
  - the recipient will then need to go to www.hushtools.com in order to verify the authenticity of the signature. This also allows users to check the integrity of the message (i.e. that it has not been tampered with).

- For you to receive digitally signed messages, the sender will need to upload his or her public key to Hushmail´s keyserver, following these steps:[343]
  - export his or her public key in text format;

- go to www.hushtools.com -> Key Management -> Advanced -> Upload a public key;
- paste the public key in text form in the box indicated;
- the website then requires users to associate the uploaded key with an e-mail address.

VI. Examples of videoconferencing software

[Rz 432] This section provides a series of summary descriptions of various videoconferencing technologies. These descriptions are not meant to be complete presentations; their purpose is merely to provide an overview of different technologies and services, allow a general understanding of these tools and constitute a first reference for parties, arbitrators, or arbitral institutions contemplating the use of a specific videoconferencing application.

1. ClickToMeet

[Rz 433] For a complete description of this software, see Chapter 4, Section II.2.C The ClickToMeet videoconferencing platform. General description, above.

2. Windows NetMeeting

[Rz 434] Windows NetMeeting is one of the most rudimentary, and thus user-friendly videoconferencing applications available. It can only transmit image to and receive image from one other station, i.e. NetMeeting allows only for point-to-point videoconferencing involving two users or user groups. The quality of the image being transmitted is, in addition, quite low. It nevertheless has the advantage of being extremely easy to install, as it comes pre-installed with the most recent version of Windows; it may thus be used if a point-to-point videoconferencing session needs to be scheduled on very short notice.

[Rz 435] NetMeeting offers a variety of features:

- Point-to-point videoconferencing, in which participants only need appropriate video, sound and voice hardware. Calls are placed mainly through the MSN Messenger Service.
- Text-chatting, that can be used to submit written messages to other participants during a conference.
- Sharing applications and transferring files, which can be very useful to create a collective document.
- Remote Desktop Sharing, allowing control over one computer from another.

[Rz 436] To install NetMeeting, the following simple steps should be followed:

- In the Start menu, select Run.
- Type «Conf» and hit return.
- The NetMeeting Wizard will launch and ask you to supply information such as name, e-mail address, and geographical location, and will then create a shortcut on the desktop or in the Quick Launch bar.

3. Ivisit

[Rz 437] Ivisit is multipoint (i.e. multi-user) videoconferencing software totally compatible with Windows and Apple Macintosh. Its light version is available for free. Depending on the version, different features are available:

- Videoconferencing, allowing up to 16 persons to participate at the same time in a private videoconference room.
- Sharing desks and files with the other participants.
- Other possibilities such as recording sessions, chatting, address book.

4. Festoon

[Rz 438] Festoon is a multipoint videoconferencing application running on Skype, the popular IP-telephony application. It is currently available only in beta (i.e. test) version. A simple plug-in installed on top of Skype allows users to add images to the traditional Skype audioconferences. The main characteristics of Festoon are:

- Videoconferencing, allowing up to 8 persons to be shown in video windows at the same time.
- In total, 200 people can join a session only to watch and listen (i.e. «spectators»).
- Application-sharing and desktop-sharing.

5. Earthlink Videoconferencing Software

[Rz 439] Earthlink is a free client/server videoconferencing system allowing multiple participants to take part in a videoconference. It is as of yet only available in beta (see corrections GKK) version. In its current version, its main features are:

- Multipoint videoconferencing.
- File transfers to other participants.
- Private chat and instant messaging.
- Compatibility between Windows, LINUX and Mac OS X.
- Firewall protection.

6. Megameeting

[Rz 440] For the time being, the Megameeting videoconferencing system is available in one of three versions: personal, professional, andenterprise.

[Rz 441] Their professional and enterprise versions include:

- Multipoint videoconferencing allowing up to 11 people to participate actively (sending and receiving image and sound), with an apparently unlimited number of «spectators».
- Sharing applications, documents and desktops among participants, including remote desktop control.
- Security via RTMP/RTMPT/RTMPS.
- Compatibility between Windows, LINUX and Mac operating systems.
- Browser-based software (i.e. it does not require downloading any software).

Gabrielle Kaufmann-Kohler; Thomas Schultz (Geneva University Law School)
with the collaboration of:
Eleanor Loukass; Victor Bonnin (Geneva University Law School)
Dimitris Protopsaltou; HyungSeok Kim (Geneva University MIRALab)

report of a project supervised by
Gabrielle Kaufmann-Kohler (Geneva University Law School)
Nadia Magnenat-Thalmann (Geneva University MIRALab)

---

[1] T. Friedman, *The Lexus and the Olive Tree*, New York 2000, p. xvi («this globalization system is also characterized by a single word : *the Web*»).

[2] Online dispute resolution covers all dispute resolution methods whose essentials elements of procedure take place using electronic means of communication. See G. Kaufmann-Kohler and T. Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice*, The Hague 2004, p. 7

[3] See for instance T. Schultz, *Does online dispute resolution need governmental intervention? The case for architectures of control and trust*, 6 North Carolina Journal of Law & Technology 71 (2004), pp. 84-87.

[4] R.G. Johnson, *Negotiating the Dayton Peace Accords Through Digital Maps*, 8 Virtual Diplomacy Report Series (2000), at www.usip.org/vdi/vdr/rjohnsonISA99.html.

[5] For concrete examples of such tools being used, see for instance SmartSettle www.smartsettle.com and The Claim Room www.theclaimroom.com. For a description of the former One Accord, see for instance Thiessen/McMahon, *Beyond Win-Win in Cyberspace*, 15 Ohio St J on Disp Resol 643 (2000). See also the consumer filing forms proposed by many ODR providers (e.g. ECODIR and SquareTrade), and T. Schultz, *Connecting complaint filing processes to online resolution systems*, 10 Commercial Law Practitioner 307 (2003).

[6] E. Katsh and J. Rifkin, *Online Dispute Resolution. Resolving Conflicts in Cyberspace*, San Francisco 2001, p. 93 and E. Katsh, *Online Dispute Resolution: The Next Phase*, 7-2 Lex Electronica (2002), at www.lex-electronica.org/articles/v7-2/katsh.htm.

[7] Katsh, *supra* note 6, para. 16.

[8] *Id.*, para. 18.

[9] *See generally* M.J. Mustill, *Arbitration: History and Background*, 6 JintArb 43 (1989); B. Yngvesson and L. Mather, *Courts, Moots, and the Disputing Process*, in K.O. Boyum and L. Mather (eds), Empirical Theories About Courts, New York 1983, p. 51; L.M. Friedmann, *Courts Over Time: A Survey of Theories and Research*, in *id.*, p. 9; R.L. Abel, *Western Courts in Non-Western Settings: Patterns of Court use in Colonial and Neo-Colonial Africa*, in S.B. Burman et B.E. Harell-Bond (eds), The Imposition of Law, New York 1979, p. 167.

[10] On these two lines of development, see E. Katsh and A. Gaitenby, *Introduction: Technology as the «Fourth Party»*, in E. Katsh and D. Choi (eds), Online Dispute Resolution (ODR): Technology as the «Fourth Party» Papers and Proceedings of the 2003 United Nations Forum on ODR, Amherst and Geneva 2003, www.odr.info/unece2003/pdf/Intro.pdf, p. 3.

[11] See Katsh, *supra* note 6, para. 23.

[12] See D. Protopsaltou, T. Schultz, and N. Magnenat-Thalmann, *Taking the Fourth Party Further? Considering a shared virtual workspace for arbitration,* Information and Communication Technology Law, 2005, publication forthcoming.

[13] For a definition of ODR, *see for instance* Kaufmann-Kohler and Schultz, *supra* note 2, p. 7 and American Bar Association Task Force on Electronic Commerce, *Addressing Disputes in Electronic Commerce: Final Recommendations and Report*, 58 Bus. Law. 415 (2002), p. 419.

[14] For a more developed discussion of this concept of a ´fourth party´, see Protopsaltou/Schultz/Magnenat-Thalmann, *supra* note 12.

[15] See Section I.1 ICC – NetCase, below.

[16] See Section I.2 AAA – WebFile, below.

[17] See Section I.3 WIPO – ECAF, below.

[18] IT tools for offline arbitration are provided by the following ventures: the American Bar Association, see www.abanet.org/tech/ltrc/home.html and www.elawyering.org; NetTech, see www.nettechinc.com/lawtech.htm; CaseCentral, see www.casecentral.com/cc/home; Documentum, see www.documentum.com/eroom; iManage, see www.imanage.com; LegalFiles, see www.legalfiles.com/main.htm, NetDocuments, see www.netdocuments.com; EliteManager, see www.eliteis.com/solutions/prod_casemanager.asp; CaseShare, see www.caseshare.com; Eversheds, see www.eversheds.com; and Allen & Overy, see www.newchange.com.

[19]

See for instance E. Schäfer, *Der Einsatz von Informationstechnologie in der Handelschiedsgerichtbarkeit*, available at www.e-global.es/arbitration/documents.htm; *Online Arbitration: What Technology can do for Arbitral Institutions*, report of the E-Arbitration-T Consortium, 20 January 2003 www.e-arbitration-t.com/papersadr/ubrun_seminar_content.pdf; M. Klang, *Improving Arbitration with Information Technology*, in N. J. Buch et. al. (ed.) Information Systems Research in Collaboration with Industry. Proceedings of the 21th Information Systems Research Seminar in Scandinavia.Saeby, Denmark, August 1998, also available at www.viktoria.se/~7Eklang/text/iris98.pdf; E. Rholl, *Web-enabled ADR and extranets*, National Law Journal, 2 December 2002, at www.nlj.com; International Chamber of Commerce, Commission on Arbitration, *Report by the Section on Information Technology on Special It Requirements in International Arbitration*, 18 March 2002, Doc. 420/21-005; E. Katsh, *Online Dispute Resolution: Some Lessons from the E-Commerce Revolution*, 28 N. Ky. L. Rev. 810 (2001). See also the empirical research carried out by the E-Arbitration-T consortium on the effects of IT on arbitration, with respect to rapidity, costs and over quality of justice, report available at www.brunel.ac.uk/~csstade/eat/ubrun-2046-1/index.html. See also the numerous articles published in the related field of IT in court proceedings, for instance M. D. Roth, *Laissez-Faire Videoconferencing: Remote Witness Testimony and Adversarial Truth*, 48 UCLA L. Rev. 185(2000); R. D. Friedman, *Remote testimony*, 35 U. Mich. J.L. Ref. 695 (2002), P. Raburn-Remfry, *Due Process Concerns In Video Production Of Defendants*, 23 Stetson L. Rev. 805 (1994), S. Nauss Exon, *The Internet Meets Obi-Wan Kenobi In The Court Of Next Resort*, 8 B.u. J. Sci. & Tech. L. 1 (2002); J. Crowell, *The Electronic Courtroom*, 4 B.u. J. Sci. & Tech. L. 10 (1997); L. Helland, Remote Testimony - A Prosecutor´s Perspective, 35 U. Mich. J.L. Ref. 719 (2002); F. I. Lederer, *The Road to the Virtual Courtroom? A Consideration of Today´s - and Tomorrow´s - High-Technology Courtrooms*, 50 S.C. L. Rev. 799 (1999).

20 See generally G. Kaufmann-Kohler, *Arbitration at the Olympics: Issues of Fast-Track Dispute Resolution and Sports Law*, Kluwer 2001.

21 See further Kaufmann-Kohler/Schultz, *supra* note 2, p. 61

22 N. Wühler, *The United Nations Compensation Commission: A new contribution to the process of international claims resolution*, 2 J. Int´l Econ. L. 249 (1999).

23 The same idea has been experimented in the context of online mediation, in the well-publicized Frankfurt airport mediation. Frankfurt airport, one of the world´s largest airports, had gone through a series of extensions in the 1980´s, much against the public opinion. As a result, strong social pressure had built up against any further addition of new runways. But in 1998, Lufthansa claimed that the airport had reached its maximal capacity and that delays and unsatisfactory transport conditions through Frankfurt were now to be expected. Lufthansa threatened to withdraw completely its operations from this airport, which until then had been its «hub», i.e. its home base. In reaction, the local government set up a wide-ranging, multiparty mediation between nearby residents, economic stakeholders, and government representatives, on the question of whether, where, and when a new runway should be built. The mediation, which involved an extremely large number of participants, was partly held online through discussion forums. This was considered to be the most appropriate way to provide everyone with a voice and thus to allow state authorities to understand the variety of issues that the airport´s extension would raise. This example showed how a dispute resolution process can be organized with a number of participants exceeding what would be feasible offline. See www.mediationflughafen.de and www.gew-frankfurt.de/index.php?id=91&backPID=91&tt_news=88.

24 See Section I.3 WIPO – ECAF, below.

25 See L. Zhuang, F. Zhou, and J. D. Tygar, *Keyboard Acoustic Emanations Revisited* (University of California, Berkeley, November 2005).

26 See Section VI.1.E E-mail encryption, digital signatures, and digital certificates, below, and Chapter V, Section V Setting up encrypted and digitally-signed e-mail, below.

27 On biometric systems, see Section VI.1.D.c Biometrics, below.

28 www.tripwire.com.

29 The document itself is never infected, but the template.

30 See L. Bellenger and M.-J. Couchaere, *Plus efficace et moins stressé*, Issy-les-Moulineaux 2004.

31 A. Kandra and A. Brandt, *The Great American Privacy Makeover*, PCWorld Magazine, November 2003, available at www.pcworld.com/reviews/article/0,aid,112468,pg,1,00.asp, p. 3.

32 http://news.zdnet.com/2100-1009_22-5142144.html.

33

ID theft is the use of personal information such as name, credit card number, IND number or any other personal data without the authorization of the concerned person to commit fraud or any other crimes. One may think that ID theft is a rare delict. However, ID theft generates a loss of approximately $1 billion per year to the banks: http://msnbc.msn.com/id/3078480.

34 G.L. Grant, *Understanding Digital Signatures: Establishing Trust over the Internet and other Networks*, New York 1998, p. 14.

35 Hence, if non-repudiation by the recipient is considered particularly important and registered letters cannot be used, one may suggest, as was done in another context, the following solutions: «First, the rules of procedure could provide that a specific e-mail program allowing non-repudiation must be downloaded and installed on the parties´ computers and used for all communications with the arbitral tribunal. Second, the arbitral tribunal might send e-mails that only invite the parties to consult their case status on the website used for the arbitration, on which the award would be posted. The website would be password-protected and could thus record the parties´ logins. The parties would then be notified at the time they consult the award online»: Kaufmann-Kohler/Schultz, *supra* note 2, p. 219.

36 On protecting word-processing documents with a password, see Section IV.1 Security, above.

37 See Section VI.1.E E-mail encryption, digital signatures, and digital certificates, below, and Chapter V, Section V Setting up encrypted and digitally-signed e-mail, below.

38 Albert van den Berg, during a presentation made at Use of IT in Arbitration – The State of the Art and the Future, ASA Conference, Berne, 5 September 2003.

39 See e.g. Montani/Kummer, *Vor E-Mail sind wir alle gleich. Vom Ärger im Umgang mit elektronischer Post*, Jusletter, 21 June 2004.

40 See further VI.2 Privacy risks through metadata, below.

41 See http://codebook.jot.com/WikiHome.

42 See Auckland District Law Society, *Electronic mail. Guidance for Practitioners*, at www.adls.org.nz/profession/guidelines/guide1.asp.

43 Montani/Kummer, *supra* note 39.

44 Id.

45 For examples, see ib-IS (iButton - Biometric Integration System) www.maxim-ic.com/products/ibutton/solutions/product.cfm?id=341 and Ruggedized Biometric Readers www.maxim-ic.com/products/ibutton/solutions/product.cfm?id=430.

46 For a world wide list of CAs, see J.A. Avellan, *Certification Authorities, CA Initiatives and Authentication Products and Services*, at www.qmw.ac.uk/~tl6345/ca.htm.

47 See for instance www.cacert.org.

48 F.C. Rice, *Protecting Personal Data in your Word Documents*.

49 See further, e.g., Kaufmann-Kohler/Schultz, *supra* note 2, pp. 217-223.

50 *See for instance* Poudret/Besson, *Droit comparé de l´arbitrage internationa*, Brussels 2002, p. 499; C. Liebscher , *The Healthy Award*, The Hague 2003, pp. 243–273,344

51 See for instance J. Hörnle, *Online Dispute Resolution*, in Bernstein´s Handbook of Arbitration and Dispute Resolution Practice 787 (J. Tackaberry and A. Marriott eds., London 2002), § 12-043.

52 For a discussion of such waivers, see for instance Kaufmann-Kohler/Schultz, *supra* note 2, p. 204.

53 See for instance T. Schultz, *Réguler le commerce électronique par la résolution des litiges en ligne* (forthcoming 2005).

54 Poudret/Besson, *supra* note 50, pp. 499–500; 779.

55 On the influence of the ECHR on the concept of due process in arbitration, see e.g. Kaufmann-Kohler/Schultz, pp. 198 et seq., 204 et seq. and T. Schultz, *«Human Rights: A Speed Bump for Arbitral Procedures? An exploration of safeguards in the acceleration of justice»*, in F. Werro, M. Hottelier and S. Besson (eds), *L´impact des droits de l´homme sur les différentes disciplines du droit*, Zurich 2005, publication forthcoming.

56 *Schuler-Zgraggen* v. *Switzerland*, European Commission on Human Rights, 7 April 1992, 16 Eur. H.R. Rep. para. 96 (1993); *Zumtobel* v. *Austria*, European Court of Human Rights, 21 September 1993, 17 Eur. Ct H.R. 116 (ser. A), para. 34. See also Liebscher, supra note 50, pp. 96–97 and 109.

[57] This is generally the law of the seat of the arbitration: Redfern/Hunter, *The Law and Practice of Commercial Arbitration*, London 1989, pp. 81, 277 and A.J. van den Berg, *The New York Convention of 1958,* The Hague 1981, p. 307 .

[58] See Section 34(2)(h) English Arbitration Act 1996, which provides that it shall be for the tribunal to decide all procedural and evidential matters, subject to the right of the parties to agree any matter. (2) Procedural and evidential matters include […] (h) whether and to what extent there should be oral or written evidence or submissions´.

[59] See U. v. Epoux G., Swiss Federal Tribunal, 1 July 1991, RO 117 II 346, 9 ASA Bulletin 415 (1991). See Poudret/Besson, supra note 50, pp. 500; 780–781. See also Fouchard/Gaillard/Goldman, On International Commercial Arbitration, (E. Gaillard and J. Savage eds., 1999), The Hague 1989, § 1296.

[60] Art. 1047 German *Zivilprozessordnung*.

[61] See *Compagnie Honeywell Bull S.A.* v. *Computacion Bull de Venezuela C.A*, Paris Court of Appeal, 21 June 1990, Rev. Arb. 96, 100 (1991) and *Boccard*, v. *S.A.R.L. Stapem*, Paris Court of Appeals, 26 January 1990, Rev. Arb. 125 (1991). *See also* Poudret/Besson, *supra* note 50, p. 500; C. Kessedjian, *Principe de la contradiction et arbitrage*, Rev. Arb. 381, 405 (1995). Contra Fouchard/Gaillard/Goldman, *supra* note 59, § 1296.

[62] See P. Bernardini, National report: Italy, in International Handbook on Commercial Arbitration 23 (J. Paulsson ed., 2000).

[63] See Art. 1039(2) Dutch *Wetboek van Burgerlijke Rechtsvordering*.

[64] Art. 1694(3) Belgian *Code Judiciaire* and see J. Linsmeau, *L´arbitrage volontaire en droit privé belge*, Brussels 1991, § 245; P. de Bournonville, *Droit judiciaire: l´arbitrage*, Brussels 2000, p. 175.

[65] Section 24(1) Swedish Arbitration Act 1999.

[66] Art. 24(1) UNCITRAL Model Law on International Commercial Arbitration.

[67] See generally Girsberger/Schramm, *Cyber Arbitration und prozessuale Fairness*, in Geschäftsplattform Internet IV. Open Source – Multimedia – Online Arbitration 198 (R.H. Weber et al. eds., 2003); Hörnle, *supra* note 51, para. 12-024.

[68] See for instance Poudret/Besson, *supra* note 50, p. 792; K.P. Berger, *International Economic Arbitration*, Boston 1993, p. 374; Fouchard/Gaillard/Goldman, *supra* note 59, § 1638; C. Kessedjian, *supra* note 61, pp. 389–390. See also Art. 190(2)(d) Swiss PIL Act (providing that the award can be challenged if ´the equality of the parties or their right to be heard in an adversarial proceeding was not respected´); Art. 1502(4) French New Code of Civil Procedure (providing for a ground to set aside the award if the principle of contradiction has not been respected); and Section 33(1) English Arbitration Act 1996 (stating that the parties must be granted a ´ *reasonable opportunity of putting his case and dealing with that of his opponent´*).

[69] See for instance Redfern/Hunter, *supra* note 57, pp. 217–218 *(´In principle all communications with only one of the parties should be reduced to writing and furnished to the other party, and in no event should there ever be discussions regarding the merits of the case´)*.

[70] See Girsberger/Schramm, supra note 67, p. 198

[71] O. Cachard, *´Electronic Arbitration´*, module of the UNCTAD Course on Dispute Settlement in International Trade, Investment and Intellectual Property, UNCTAD/EDM/Misc.232/Add.20 www.unctad.org/en/docs/edmmisc232add20_en.pdf (United Nations Publications, New York and Geneva, 2003), p. 36.

[72] The use of such an agent is planned in the E-Arbitration-T online arbitration platform, see E-Arbitration-T, ´Online Arbitration: What Technology can do for Arbitral Institutions´, IST-2000-25464/11.5/UBRUN/2048/R/2 www.e-arbitration-t.com/papersadr/ubrun_seminar_content.pdf, 20 January 2003, p. 12.

[73] See e.g. Art. 18 UNCITRAL Model Law on International Commercial Arbitration; Art. 182(3) Swiss PIL Act; Redfern/Hunter, *supra* note 57, p. 425; Poudret/Besson, *supra* note 50, pp. 507–508; Fouchard/Gaillard/Goldman, *supra* note 59, § 1638–1639. In ´Dombo Beheer´, the Eur. Ct H. R. held that equal treatment *´implies that each party must be afforded a reasonable opportunity to present its case—including evidence—under conditions that do not place it at a substantial disadvantage vis-à-vis his opponent´*: *Dombo Beheer* v. *Netherlands*, European Court of Human Rights, .27 October 1993, 274 Eur. Ct H.R (ser. A).

[74] Poudret/Besson, *supra* note 50 , at, p. 507.

[75]

See for instance O. Cachard, *supra* note 71, p. 36 (providing that oral statements of claim and statements of defense must be made from identical electronic hearing rooms in order not to put due process at risk). See also J. Hörnle, *supra* note 51, § 12-042 and 12-054–12-056.

76 For smaller disputes, see for instance Kaufmann-Kohler/Schultz, *supra* note 2, pp. 203–204.

77 By analogy, one may mention that, eight years ago, in *Yukiyo Ltd* v. *Watanabe*, 111 Fed 3d 883 (Fed. Cir. 1997), the US Court of Appeal for the Federal Circuit held that a brief submitted on a CD Rom while the other party was not equipped to read it was a violation of due process. Nowadays, in 2005, it has become exceptional indeed that a law office is not equipped to read CD Roms. Examples of usual standards include RTF for text documents (rather than DOC documents, which more easily carry viruses and might require the use of proprietary software or a compatible version of the same software program) or PDF. For images, typical formats are GIF, JPEG, and BMP (although BMP encodes every pixel and thus produces very large files).

78 Redfern/Hunter, *supra* note 57, p. 415.

79 *Id.*, p. 426.

80 Poudret/Besson, *supra* note 50, pp. 779–780.

81 Raeschke-Kessler/Berger, *Recht und Praxis des Schiedsverfahren*, Coln 1999, p. 229; Huys/ Keutgen, *L´arbitrage en droit belge et international*, Brussels 199, p. 358; Swiss law is an exception to this general rule: *see U.* v. *Epoux G.*, *supra* note 59.

82 Poudret/Besson, *supra* note 50, pp. 780, 782.

83 D. Hascher, *Principes et pratique de procédure dans l´arbitrage commercial international*, 279 Collected Courses of the Hague Academy of International Law 50, 126–133 (1999).

84 On the challenge of an award on the ground of a violation of fundamental procedural rights, *see* Poudret/Besson, *supra* note 50, p. 779 and Berger, *supra* note 68, p. 664.

85 See in general Fouchard/Gaillard/Goldman, *supra* note 59, § 1696–1699, van den Berg, *supra* note 57, pp. 306–311; Poudret/Besson, *supra* note 50, pp. 886–888; Redfern/Hunter, *supra* note 57, pp. 463–464.

86 van den Berg, *supra* note 57, pp. 297, 306; Poudret/Besson, *supra* note 50, p. 887; Fouchard/Gaillard/Goldman, *supra* note 59, § 1698.

87 *See* Poudret/Besson, *supra* note 50, pp. 890–891.

88 Fouchard/Gaillard/Goldman, *supra* note 59, § 1701.

89 *Compagnie des Bauxites de Guinée* v. *Hammermills Inc.*, 1992 WL 122712 (D.D.C. 1992) and *Agri* v. *Balli*, Queen´s Bench, 2 Lloyd´s Rep. 76 (1998).

90 van den Berg, *supra* note 57, p. 323 and Poudret/Besson, *supra* note 50, p. 892.

91 Raeschke-Kessler/Berger, *supra* note 81, p. 249; van den Berg, *supra* note 57, p. 366; Lew/Mistelis/Kröll, *Comparative International Commercial Arbitration*, The Hague 2003, pp. 721, 729; Fouchard/Gaillard/Goldman , *supra* note 59, § 1710–1711.

92 Fouchard/Gaillard/Goldman, *supra* note 59, § 1713; Lew/Mistelis/Kröll, *supra* note 91, pp. 723–729.

93 *Firm P* v. *Firm F*, Oberlandesgericht of Hamburg, 3 April 1975, 2 Yearbook Comm. Arb´n 241 (1977).

94 Poudret/Besson, *supra* note 50, p. 907.

95 Art. 14 Arbitration Act 1996: *«(1) Subject to subsection (2), an arbitration agreement, unless otherwise agreed by the parties, is deemed to provide that the parties shall not publish, disclose, or communicate any information relating to arbitral proceedings under the agreement or to an award made in those proceedings».*

96 Art. 24 Spanish Arbitration Act 2003: *«2. The arbitrators, the parties and the arbitral institutions, if applicable, are obliged to maintain the confidentiality of information coming to their knowledge in the course of the arbitral proceedings».*

97

See further Paulsson/Rawding, *´The Trouble with Confidentiality´* , Arbitration International, Vol. 11 No. 3 (1995), p. 303 (concluding that specific provisions should be drafted on the confidentiality of information generated during the proceedings and the award, and on the duties of participants in the arbitration); Y. Fortier, *´The Occasionally Unwarranted Assumption of Confidentiality´* , Arbitration International, Vol 15 No.2 (1999) p. 132 (*´The issues of privacy and its corollary, confidentiality . . . have, in fact been the subject of much heated debate recently, in various jurisdictions and institutions. The conclusions reached in those instances demonstrate what might be called a definite lack of consensus´*) and p. 138 (*´What is evident today is that, with respect to confidentiality in international commercial arbitrations, nothing should be taken for granted´*), and Redfern/Hunter, *supra* note 57, pp. 27–30 (discussing the importance of confidentiality and the confidentiality of hearings, documents produced in arbitration and awards), C. Müller, *La confidentialité en arbitrage commercial international; un trompe-l´oeil?*, in 23 ASA Bulletin 2/2005, June, p. 217.

98 F. Fracassi, *Confidentiality and NAFTA Chapter 11 Arbitrations*, 2 Chicago Journal of International Law, p. 213, 2001

99 E. C. Chiasson, *Confidentiality and Arbitration*, 58 Advocate 417 (2000).

100 Kaufmann-Kohler/Schultz, *supra* note 2, p. 49.

101 *Aita v. Ojjeh*, Judgment of 18 February 1986, REV. ARB. (1986), p. 583, note Georges Flecheux, in which the court more precisely found that it is in «the very nature of arbitral proceedings that they ensure the highest degree of discretion in the resolution of private disputes.» See also Brown, *Presumption Meets Reality: An Exploration of the Confidentiality Obligation in International Commercial Arbitration*, 16 Am. U. Int´l L. Rev. 969, 2001, pp. 969 ss. and Paulsson/Rawding, *supra* note 97, p. 312.

102 C. Müller, *supra* note 97, p. 219; *Nafimco c. Foster Wheeler Trading Company AG*, Paris Court of Appeal (1st Chamber), Judgment of 22 January 2004. The court held that the party complaining of the violation of confidentiality in the appeal of an award under the ICC did not show the *«existence and the reasons of an existing confidentiality principle in international arbitration under French law whatever the nature of arbitration is»*.

103 *Dolling-Baker v. Merrett* 1 W.L.R., pp. 1213-14 (Eng. C.A. 1990). See also J. Rosell, *Global Development: Confidentiality and Arbitration*, 9 Croat. Arbit. Yearb. 19, 2002, p. 20. It should be noted that, in England, the right to privacy is considered to be an implicit right that attaches to all arbitration agreements unless it is expressly excluded by the parties: Michael Collins Q.C., *Privacy and Confidentiality in Arbitration Proceedings* , 30 Tex. Intl L.J. 121, Winter 1995, referring to, e.g., Redfern/Hunter, *supra* note 57. See also, Fracassi, *supra* note 98, p. 213, citing 1 Lloyd´s 651 (Eng Ct App 1998).

104 *Ali Shipping v. Shipyard Trogir*, 2 All ER 136 (1998), the Court also expressly found that the duty of confidentiality applies not only to the arbitral award, but also to «*pleadings, written submissions, and the proofs of witnesses as well as transcripts and notes of the evidence given in the arbitration*.» The Court did however recognize several potential exceptions to the duty of confidentiality: *«the consent of the parties, a court order, the ´reasonable necessity´ to protect or enforce a party´s legal rights, and ´the interests of justice´»*. See also Brown, *supra* note 101, p. 969.

105 *United States v. Panhandle Eastern Corp*, 118 FRD 346 (D Del 1988). See also Fracassi, *supra*note 98.

106 *Esso Australia Resources Ltd v. Plowman*, 128 Austl L Rep 391 (1995). See also Fracassi, *supra* note 98.

107 *Esso Australia Resources Ltd, supra* note 106, § 34-35.

108 A. C. Brown, *supra* note 101, pp. 970-71, citing L.Y. Fortier, *supra* note 97.

109 Id.

110 Rosell, *supra* note 103, p. 19.

111 *Id.* p. 24. In the United States some private organizations publish maritime awards, most labor awards and awards in securities cases, usually without identifying the parties. In France excerpts of awards identifying the names of the parties and other features can also be published. Weigand, *Practitioner´s Handbook on International Arbitration, Brussels*, Bruylant 2002, p. 675 and 1131.. See also art. 43 Swiss Rules, *infra* 127

112 Rosell, *supra* note 103, p. 21.

113 Rosell, *supra* note 103, p. 22, citing AAA, Belgian CEPANI, ICC, Russian ICAC and SCC Rules.

114 Id.

115 Michael Collins Q.C., supra note 103 referring to, e.g., Redfern/Hunter, supra note 57.

116 *«Hearings are private unless the parties agree otherwise or the law provides to the contrary. The tribunal may require any witness or witnesses to retire during the testimony of other witnesses. The tribunal may determine the manner in which witnesses are examined.»* International Arbitration Rules Article 20.4, American Arbitration Association, 1 July 2003.

117 *«The Arbitral Tribunal shall be in full charge of the hearings, at which all the parties shall be entitled to be present. Save with the approval of the Arbitral Tribunal and the parties, persons not involved in the proceedings shall not be admitted.»* Rules of Arbitration of the ICC, Art. 21(3), 1998. ICC Rules do not expressly mention any general duty of confidentiality. However, everyone working in the ICC Court has a duty of confidentiality: *«The work of the Court is of a confidential nature which must be respected by everyone who participates in that work in whatever capacity. The Court lays down the rules regarding the persons who can attend the meetings of the Court and its Committees and who are entitled to have access to the materials submitted to the Court and its Secretariat.»* ICC Rules Appendix I Art. 6. The internal rules of the ICC Court also provide that the work of the ICC Court is confidential.

118 «*The Arbitral Tribunal shall maintain the confidentiality of the arbitration»,* Rules of the Arbitration Institute of the Stockholm Chamber of Commerce, Art. 20(3), 1 April 1999.

119 «*The hearing of the case shall be conducted in private. With permission of the arbitral tribunal and with the consent of the parties persons not participating in the proceedings may be present at the hearing.»* Art. 27 Rules of the International Commercial Arbitration Court at the Chamber of Commerce and Industry of the Russian Federation, Further, there is an obligation imposed on arbitrators, reporters and the staff of the Secretariat to ensure the confidentiality of the information about the disputes: «*The arbitrators, the reporters and the staff of the Secretariat must ensure the confidentiality of information which has become known to them about the disputes examined by the ICAC which can impair interests of the parties*», Art. 8 Rules of the International Commercial Arbitration Court at the Chamber of Commerce and Industry of the Russian Federation.

120 *«Les audiences ne sont pas publiques. Sauf accord du tribunal arbitral et des parties, elles ne sont pas ouvertes aux personnes étrangères à la procédure.»* Règlement pour montants inférieur à € 12.500, Art. 18(5), and Règlement pour montants supérieur à € 12.500, Art. 17(5), Centre Belge d´Arbitrage et de Médiation (CEPANI).

121 *«Hearings shall be held in camera unless the parties agree otherwise. The arbitral tribunal may require the retirement of any witness or witnesses during the testimony of other witnesses.»* UNCITRAL Arbitration Rules, Art. 25(4), 1976.

122 Besides the privacy of the hearings, the AAA provides for the confidentiality of the award and the duty of confidentiality of arbitrators: *«An award may be made public only with the consent of all parties or as required by law»* International Arbitration Rules, Art. 27.4, American Arbitration Association. *«Confidential information disclosed during the proceedings by the parties or by witnesses shall not be divulged by an arbitrator or by the administrator. Except as provided in Article 27, unless otherwise agreed by the parties, or required by applicable law, the members of the tribunal and the administrator shall keep confidential all matters relating to the arbitration or the award»*, International Arbitration Rules, Art. 34, American Arbitration Association.

123 *«Unless the parties expressly agree in writing to the contrary, the parties undertake as a general principle to keep confidential all awards in their arbitration, together with all materials in the proceedings created for the purpose of the arbitration and all other documents produced by another party in the proceedings not otherwise in the public domain - save and to the extent that disclosure may be required of a party by legal duty, to protect or pursue a legal right or to enforce or challenge an award in bona fide legal proceedings before a state court or other judicial authority»* Art. 30.1 Arbitration Rules, London Court of International Arbitration, 1 January 1998; *«The deliberations of the Arbitral Tribunal are likewise confidential to its members, save and to the extent that disclosure of an arbitrator´s refusal to participate in the arbitration is required of the other members of the Arbitral Tribunal under Articles 10, 12 and 26»* Art. 30.2; and *«The LCIA Court does not publish any award or any part of an award without the prior written consent of all parties and the Arbitral Tribunal»* Art. 30.3.

124 Arts. 73-76, WIPO Arbitration Rules, World Intellectual Property Organization. See H. Smit, *Breach of Confidentiality as a Ground for Avoidance of the Arbitration Agreement*, 11 Am. Rev. Int´l Arb. 567, 2000, p. 567,

125

«For cases heard in closed session, the parties, their arbitration agents, witnesses, arbitrators, experts consulted by the arbitration tribunal and appraisers appointed by the arbitration tribunal and the relevant staff-members of the secretariat of the Arbitration Commission shall not disclose to outsiders the substantive or procedural matters of the case.» Arbitration Rules of the China International Economic and Trade Arbitration Commission (CIETAC), Art. 37, CIETAC, 1 October 2000. *«The record [of the hearing] in writing or by tape-recording is only available for use and reference by the arbitration tribunal.»* Arbitration Rules of the China International Economic and Trade Arbitration Commission (CIETAC), Art. 43, CIETAC, 1 October 2000.

126 *«The arbitrators, the officers and staff of the Association, the parties and their representatives or assistants shall not disclose facts related to arbitration cases or facts learned through arbitration cases except where disclosure is required by law or required in court proceedings.»* Commercial Arbitration Rules, Rule 40.2, Japan Commercial Arbitration Association, 1 March 2004.

127 *«1. Unless the parties expressly agree in writing to the contrary, the parties undertake as a general principle to keep confidential all awards and orders as well as all materials submitted by another party in the framework of the arbitral proceedings not otherwise in the public domain, save and to the extent that a disclosure may be required of a party by a legal duty, to protect or pursue a legal right or to enforce or challenge an award in legal proceedings before a judicial authority. This undertaking also applies to the arbitrators, the tribunal-appointed experts, the secretary of the arbitral tribunal and the Chambers. 2. The deliberations of the arbitral tribunal are confidential. 3. An award may be published, whether in its entirety or in the form of excerpts or a summary, only under the following conditions: (a) A request for publication is addressed to the Chambers;*
(b) All references to the parties´ names are deleted; and (c) No party objects to such publication within the time-limit fixed for that purpose by the Chambers». Swiss Rules of International Arbitration, Art. 43.

128 Spanish Arbitration Act, Art. 24, *supra* note 96.

129 A. Jolles and M. Canals de Cediel, *Confidentiality*, in G. Kaufmann-Kohler and B. Stucki (eds), *International Arbitration in Switzerland*, The Hague 2004, 89, pp. 93-94.

130 Section. 52(3) English Arbitration Act.

131 § 1054(1) ZPO

132 See Rosell, *supra* note 103, p. 21. Under Art. 1469 NCPC, for instance, arbitrators´ deliberations are confidential.

133 Art. 34 AAA International Arbitration Rules.

134 Art. 37, CIETAC, 1 October 2000, *supra* note 125.

135 Commercial Arbitration Rules, Rule 40.2, Japan Commercial Arbitration Association (JCAA), 1 March 2004, *supra* note 126.

136 *«The Arbitral Tribunal shall maintain the confidentiality of the arbitration»,* Rules of the Arbitration Institute of the Stockholm Chamber of Commerce (SCC), Art. 20(3), 1 April 1999.

137 Art. 30 LCIA *supra* note 123.

138 Art. 43 Swiss Rules *supra* note 127.

139 *«Unless the parties agree otherwise, the Center and the arbitrator shall maintain the confidentiality of the arbitration, the award and, to the extent that they describe information that is not in the public domain, any documentary or other evidence disclosed during the arbitration, except to the extent necessary in connection with a court action relating to the award, or as otherwise required by law.»* WIPO Arbitration Rules, Art. 76(a), World Intellectual Property Organization (WIPO).

140 The New Zealand Arbitration Act of 1994, apparently, does make such a provision, art. 14, *supra* note 95. See Rosell, *supra* note 103, p. 21. See also Spanish Arbitration Act, art. 24, *supra* note 96. In Switzerland no specific provision provides for an obligation of confidentiality concerning the parties, but it is recognized that this obligation is implied under the agreement to arbitrate since they agree on arbitration to dispose of disputes confidentially, despite of the existence of some exceptions. See A. Jolles and M. Canals de Cediel, *supra* note 129, p. 100.

141 Arbitration Rules, Art. 30.1, London Court of International Arbitration (LCIA), 1 January 1998.

142

«(a) Except to the extent necessary in connection with a court challenge to the arbitration or an action for enforcement of an award, no information concerning the existence of an arbitration may be unilaterally disclosed by a party to any third party unless it is required to do so by law or by a competent regulatory body, and then only: (i) by disclosing no more than what is legally required; and (ii) by furnishing to the Tribunal and to the other party, if the disclosure takes place during the arbitration, or to the other party alone, if the disclosure takes place after the termination of the arbitration, details of the disclosure and an explanation of the reason for it. (b) notwithstanding paragraph (a), a party may disclose to a third party the names of the parties to the arbitration and the relief requested for the purpose of satisfying any obligation of good faith or candor owed to that third party.» WIPO Arbitration Rules, Art. 73. *«In addition to any specific measures that may be available under Article 52, any documentary or other evidence given by a party or a witness in the arbitration shall be treated as confidential and, to the extent that such evidence describes information that is not in the public domain, shall not be used or disclosed to any third party by a party whose access to that information arises exclusively as a result of its participation in the arbitration for any purpose without the consent of the parties or order of a court having jurisdiction.»* WIPO Arbitration Rules, Art. 74(a). *«The award shall be treated as confidential by the parties.»* WIPO Arbitration Rules, Art. 75.

143 CIETAC Arbitration Rules, Art. 37.

144 JCAA Commercial Arbitration Rules, Rule 40.2.

145 Brown, supra note 101, at p. 969 ss., citing *Hassneh Insurance Co. of Israel v. Steuart J. Mew*, *2 Lloyd´s Rep. 243, 246 (Q.B. 1993).*

146 Art. 43, for tribunal-appointed experts.

147 CIETAC Arbitration Rules, Art. 37.

148 *«The confidentiality of any document created in arbitration will be observed by either the Court, the parties, their lawyers, counsels, or the experts and eventual witnesses».* Art. 9 Spanish Court of Arbitration New Rules.

149 *«To the extent that a witness is given access to evidence or other information obtained in the arbitration in order to prepare the witness´s testimony, the party calling such witness shall be responsible for the maintenance by the witness of the same degree of confidentiality as that required of the party.»* WIPO Arbitration Rules, Art. 74(b).

150 *«The SCC Institute shall maintain the confidentiality of the arbitration and shall deal with the arbitration in an impartial, practical and expeditious manner.»* SCC Arbitration Rules, Art. 9, .

151 *«Unless the parties agree otherwise, the Center and the arbitrator shall maintain the confidentiality of the arbitration, the award and, to the extent that they describe information that is not in the public domain, any documentary or other evidence disclosed during the arbitration, except to the extent necessary in connection with a court action relating to the award, or as otherwise required by law.»* WIPO Arbitration Rules, Art. 76(a).

152 Müller, *supra* note 97, p. 226.

153 Art. 73 WIPO Rules.

154 Brown, *supra* note 101, p. 1003.

155 *United States v. Panhandle Eastern Corp,* 11 FRD 346 (D Del 1998) and *Esso Australia Resources Ltd. V. Plowman,* 128 Austl L Rep 391 (1995); *A.I. Trade Finance Inc. v. Bulgarian Foreign Trade Bank* (Svea App. 1999). *See also* Fracassi, *supra* note 98, pp. 213 and 214-15; Smit, *supra* note 124, p. 567.

156 *See Ali Shipping,* 1 Lloyd´s Rep. pp. 651-52. See also Brown, *supra* note 101, p. 969.

157 Brown, *supra* note 101, p. 1005.

158 Id.

159 Müller, *supra* note 97, p. 227.

160 Art. 30.1 LCIA, *supra* note 123, Art. 74 WIPO Rules; Art. 37 CIETAC Rules *supra* note 125; Art. 34, International Arbitration Rules, American Arbitration Association, *supra* note 122, Art. 9 Spanish Court of Arbitration New Rules, *supra* note 148.

161 Art. 74 WIPO Rules, *supra* note 142, grants confidential privilege to evidences. See also 43 Swiss Rules, *supra* note 127, Art. 37 CIETAC Rules, *supra* note 125.

162 See section II.1 Basis for a duty of confidentiality above.

163

Only the New Zealand Arbitration Act 1994 prohibits parties from disclosing any information regarding an arbitral award: Rosell, *supra* note 103, p. 19, Brown, *supra* note 101, p. 1012.

164 Fouchard/Gaillard/Goldman, *supra*note 59, § 384.

165 Art. 32.5 UNCITRAL Arbitration Rules, Art. 75 WIPO Rules, *supra* note. 142, Art. 30 LCIA Rules, *supra* note 123, Art. 27.3 AAA International Arbitration Rules.

166 Injunctive relief is discouraged when the party making the disclosure had a legitimate interest in doing so. In such a case, it is preferable to impose damages, if they are warranted: Fouchard/Gaillard/Goldman, *supra* note 59, § 1412.

167 Exemplary damages may be appropriate if a disclosure was improper and a legitimate interest of the complainant was harmed: *id*.

168 Fouchard/Gaillard/Goldman, *supra* note 59, § 1412.

169 For the moment, NetCase is only intended for use in proceedings subject to the ICC Rules of Arbitration. M. Philippe, *NetCase: A New ICC Arbitration Facility* in ICC International Court of Arbitration Bulletin, Using Technology to Resolve Business Disputes – Special Supplement 2004, p. 53.

170 Id.

171 *Id.* p. 56.

172 *Id.* p. 56.

173 *Id.* p. 54.

174 Id.

175 *Id.* p. 55. On the requirement of a written award, see e.g. J. Arsic, *International Commercial Arbitration on the Internet – Has the Future Come Too Early?*, 14 J. Int´l Arb. 209 (1997), p. 217, M.E. Schneider and C. Kuner, *Dispute Resolution in International Electronic Commerce*, 14 J. Int´l Arb. 5 (1997), p. 24, and Kaufmann-Kohler/ Schultz, *supra* note 2, pp. 216–223.

176 Philippe, *supra*note 169, p. 55.

177 Including information about the constitution of the arbitral tribunal, the CVs of arbitrators and their declarations that they will act independently.

178 Including information about securities, payments made by the parties, fees paid to arbitrators, and arbitration fees.

179 Used for expert procedures and containing experts´ contact data and financial information regarding these specific proceedings.

180 Philippe, *supra*note 169, p. 56.

181 Id.

182 The specificity of XML formats is that they inform about content, and not merely display: HTML files tell the browser information about the style and display of text on a web page, but XML informs the browser about what the text on a web page actually represents. An XML tag may for instance indicate that some piece of text is in fact the price of an object, or a deadline, or the name of an individual, etc. For further information on XML, see for instance www.w3.org/XML and N. Walsh, *XML.com: A Technical Introduction to XML*, www.xml.com/pub/a/98/10/guide0.html, 3 October 1998.

183 Philippe, *supra*note 169, p. 60.

184 American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide02.htm.

185 https://apps.adr.org/webcase2/index.jsp.

186 American Arbitration Association, *Frequently Asked Questions*, https://apps.adr.org/webcase2/index.jsp.

187 American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide05.htm.

188 Id.

189 Id.

190 American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide06.htm.

[191] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide07.htm.
[192] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide08.htm.
[193] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide09.htm.
[194] American Arbitration Association, *Frequently Asked Questions*, https://apps.adr.org/webcase2/index.jsp.
[195] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide10.htm.
[196] *See* American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide11.htm, https://apps.adr.org/webcase2/demo/pages/Slide12.htm, https://apps.adr.org/webcase2/demo/pages/Slide13.htm.
[197] American Arbitration Association, *Frequently Asked Questions*, https://apps.adr.org/webcase2/index.jsp.
[198] *Id.*.
[199] *Id. See also,* American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide14.htm.
[200] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide15.htm.
[201] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide16.htm.
[202] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide17.htm.
[203] American Arbitration Association, *AAA WebFile: all online*, https://apps.adr.org/webcase2/demo/pages/Slide18.htm.
[204] American Arbitration Association, *Frequently Asked Questions*, https://apps.adr.org/webcase2/index.jsp.
[205] See http://arbiter.wipo.int/center/index.html.
[206] World Intellectual Property Organization (WIPO), *The WIPO Arbitration and Mediation Center*, http://arbiter.wipo.int/center/background.html.
[207] WIPO, *WIPO Electronic Case Facility (ECAF)*, http://arbiter.wipo.int/ecaf/introduction.jsp.
[208] Id.
[209] Id.
[210] Id.
[211] Id.
[212] *Id.*
[213] Id.
[214] Id.
[215] Id.
[216] Further on the ACJ and the 32nd America´s Cup, see e.g. T. Schultz, *Dispute Resolution at the America´s Cup*, JusLetter of 5 September 2005.
[217] World Intellectual Property Organization, *Frequently Asked Questions: Internet Domain Names*, http://arbiter.wipo.int/center/faq/domains.html#7.
[218] ICC Section on IT Mission Statement, 24.1.01, cited in ICC Commission on International Arbitration Forum on Arbitration Issues and New Fields, Section on Information Technology, *Special IT Requirements in International Arbitration*, para. 2, March 2002.
[219] ICC Commission on International Arbitration Forum on Arbitration Issues and New Fields, Section on Information Technology, *Special IT Requirements in International Arbitration*, March 2002, para. 5.
[220] *Id.* § 7.1.
[221] *Id.* § 7.2.

[222] *Id.* § 7.3.
[223] *Id.* § 7.4.
[224] *Id.* § 8.1.
[225] *Id.* § 8.2.
[226] *Id.* § 9.1.
[227] *Id.* § 10.
[228] *Id.* § 11.
[229] *Id.* § 12
[230] *Id.* para. 13. The «lowest common denominator» refers to the fact that participants may have different levels of technical capability (related to hardware, software and technical skills). A more IT-capable participant may have to align himself to the level of less capable counterparts.
[231] *Id.* § 14.
[232] *Id.* § 15.
[233] *Id.* § 16.
[234] *Id.* § 17.
[235] *Id.* § 18.
[236] *Operating Standards for Using IT in Arbitration,* in *Using Technology to Resolve Business Disputes – Special Supplement 2004*, ICC International Court of Arbitration Bulletin (hereinafter «*ICC Operating Standards*»).
[237] *ICC Operating Standards*, Part A.
[238] *ICC Operating Standards*, Part B.
[239] *ICC Operating Standards*, Standards G1 and G3.
[240] *ICC Operating Standards*, Part C.
[241] *ICC Operating Standards*, Part D.
[242] *ICC Operating Standards*, Standard G4.
[243] *ICC Operating Standards*, Standard G5.
[244] *ICC Operating Standards*, Standard G6.
[245] *ICC Operating Standards*, Standard G7.
[246] *ICC Operating Standards*, Standard G8.
[247] *ICC Operating Standards*, Standard G9.
[248] *ICC Operating Standards*, Standards G10-11.
[249] *ICC Operating Standards*, Standard G12.
[250] *ICC Operating Standards*, Standard G13.
[251] *ICC Operating Standards*, Standard P1.
[252] *ICC Operating Standards*, Standard P3.
[253] *ICC Operating Standards*, Standard P4.
[254] *ICC Operating Standards*, Standard P5.
[255] *ICC Operating Standards*, Standards P6.1-2.
[256] *ICC Operating Standards*, Standard P6.3.
[257] *ICC Operating Standards*, Standards P9-11.
[258] *ICC Operating Standards*, Standard P8.
[259] *ICC Operating Standards*, Standard P15.
[260] *ICC Operating Standards*, Standards P12-13.
[261] See further Chapter 2, Section I Due process issues, above.
[262] *ICC Operating Standards*, Standard P 14.
[263] *ICC Operating Standards*, Standard E1.
[264]

ICC Operating Standards, Standard E5.

265 *ICC Operating Standards*, Standard E10.

266 *ICC Operating Standards*, Standard E8.

267 *ICC Operating Standards*, Standard E6.

268 *ICC Operating Standards*, Standards E7-8.

269 *ICC Operating Standards*, Standard E9.

270 *ICC Operating Standards*, Standard E13.

271 *ICC Operating Standards*, Standards E13-15.

272 *ICC Operating Standards*, Standard E17.

273 *ICC Operating Standards*, Standard E18.

274 *ICC Operating Standards*, Standard E23.

275 *ICC Operating Standards*, Standard E24.

276 *ICC Operating Standards*, Standard V2.

277 *ICC Operating Standards*, Standard V3.

278 *ICC Operating Standards*, Standard V4-5.

279 *ICC Operating Standards*, Standard V6.

280 *ICC Operating Standards*, Standard A2.

281 *ICC Operating Standards*, Standard A4.

282 *ICC Operating Standards*, Standard A5.

283 *See* Section III.A.1 above.

284 *See* Section III.A.2 above.

285 *See* Section III.A.3 above.

286 *See* generally Chapter 2 Legal framework, above.

287 For examples, see e.g. www.kilchenmann.ch/de/telematik/videoconferencing/produkte-anwendung/einzelplatz.

288 See e.g. E. Schäfer, *«La visioconférence dans l´arbitrage»*, Bulletin de la cour d´arbitrage, 2003, vol. 14/1, p. 37, 38. For an example of such videoconferencing service providers, see e.g. www.demorum.com.

289 Id.

290 *Id.*

291 The following persons participated in simulations:
Arbitration practitioners: Michael E. Schneider (Lalive and partners), Pierre-Yves Gunter (Python Schifferli Peter), Matthias Scherrer (Lalive and Partners), Dr. Antonio Rigozzi (Schellenberg Wittmer), Pierre Kobel and Laurent Hirsch (Hirsch Kobel), Lorine Meylan (Lalive and Partners);
Academics (all active in the field of arbitration): Christine Chappuis, Professor, Geneva University Law School, Brian Hutchinson, Vice-Dean, University College Dublin, Juan-Carlos Landrove, Geneva University Law School, Silja Schaffstein, Geneva University Law School;
Members of the research team: Gabrielle Kaufman-Kohler, Law School, Thomas Schultz, Law School, HungSeok Kim, MIRALab, Dimitris Protopsaltou, MIRALab.

292 The award is reported in Court of Arbitration for Sport CAS Awards – Sydney 2000, The decisions delivered by the ad hoc Division of the Court of Arbitration for Sport during the 2000 Olympic Games in Sydney, Lausanne 2000, pp. 123-130; the arbitrability issues raised by this case, are also discussed in Gabrielle Kaufmann-Kohler, Arbitration at the Olympic Games – Issues of Fast Track Dispute Resolution and Sports Law, the Hague (Kluwer) 2001, pp 25ff.

293 See Section II.2 The Geneva experiment, above.

294 On the general economic efficiency of using electronic communication technologies in arbitration, see Chapter 1, Section III.1.A Efficiency, above. See also B. A. Lenox, *Personal Jurisdiction in Cyberspace: Teaching the Stream of Commerce Dog New Internet Tricks: Compuserve, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996)* , 22 Dayton L. Rev. 331, 347 (Winter 1997), citing F. I. Lederer, Trial by TV, USA TODAY, April 25, 1996, p. A13.

295

L.J. Gibbons, R.M. Kennedy, and J.M. Gibbs, *Frontiers of Law: The Internet and Cyberspace: Cyber-mediation: Computer-mediated Communications Medium Massaging the Message,* 32 N.M.L. Rev. 27 (2002), p. 34, citing J. Lanier, *Virtually There*, Scientific American, p. 66.

296 W. Krause, *Do You Want to Step Outside? An Overview of Online Alternative Dispute Resolution*, 19 J. Marshall J. Computer & Info. L. 457 (2001), p. 489. See also H.H. Perritt, Jr., *Dispute Resolution in Cyberspace: Demand for New Forms of ADR*, 15 Ohio St. J. on Dis. Res. 675 (2000), pp. 680-81 and B. Park Sunoo, *Hot Disputes Cool Down in Online Mediation*, Personnel J. 48 P 3 (available at 2001 WL 11690279) (Jan. 1. 2001).

297 See Section II.3.A.a Videoconferencing v. telephone conferencing, above.

298 See in Section IV.2 Technical failures, breakdowns, above.

299 Id.

300 For technical information on security in videoconferencing, see e.g. M. Brandl et al., *IP Telephony Cookbook*, University of Bremen, 9 March 2004, available at www.informatik.uni-bremen.de/~prelle/terena/Cookbook.pdf and TANDBERG and Security, D50172, Rev 3.1, available at www.tandbergusa.com/collateral/white_papers/whitepaper_TANDBERG_Security.pdf.

301 See generally Chapter 2 Legal framework, above.

302 Schäfer, *supra* note 288, p. 40.

303 *Id.*

304 *Id.*

305 *Id.*

306 *Id.*

307 *Id* p. 40-41.

308 Id.

309 *Id.* p. 41-42.

310 This section is based on D. Protopsaltou, T. Schultz, and N. Magnenat-Thalmann, *Taking the Fourth Party Further? Considering a shared virtual workspace for arbitration,* in Information and Communication Technology Law, 2005, publication forthcoming.

311 R.E. Kraut, S.R. Fussell, S.E. Brennan, and J. Siegel, *Understanding effects of proximity on collaboration: Implications for technologies to support remote collaborative work*. P. Hinds and S. B. Kiesler (eds), *Distributed work*, Cambridge, MA, 2002, p. 137 et seq.

312 S.E. Brennan, *How conversation is shaped by visual and spoken evidence*, in World Situated Language Use: Psycholinguistic, Linguistic and Computational Perspectives on Bridging the Product and Action Traditions (J. Trueswell and M. Tanenhaus eds., publication forthcoming 2005); Clark/Brennan, *Grounding in communication* , in Perspectives on socially shared cognition pp. 127–149 (L.B. Resnick, R.M. Levine, and S.D. Teasley eds., 1991); Fussell/Kraut,/Siegel, *Coordination of communication: Effects of shared visual context on collaborative work* 21–30 (2000); P.-G. Maillot. *Using quaternions for coding 3D transformations*, in Graphic Gems 498–515 (A.S. Glassner ed., 1990); L. Karsenty, *Cooperative work and shared visual context: An empirical study of comprehension problems and in side-by-side and remote help dialogues* , 14-3 Human-Computer Interaction 283 (1999); Veinott/Olson/Olson/Fu, *Video helps remote work: Speakers who need to negotiate common ground benefit from seeing each other. Proceedings of CHI´99* 302–309 (1999); S. Whittaker and B. O´Conaill, *The role of vision in face-to-face and mediated communication*, in Video-mediated communication 23–49 (K. Finn, A. Sellen and S. Wilbur eds., 1997).

313 Short/Williams/Christie, *The Social Psychology of Telecommunications* (John Wiley and Sons Ltd., 1976); Chapanis/Ochsman/Parrish/Weeks, ´The effects of four communication modes on the behavior of teams during cooperative problem-solving´ [1972] 14-6 *Human Factors* 487.

314 Clark/Brennan , supra note 312.

315 Kraut et al., *supra* note 311.

316 Fussell/Kraut,/Siegel, *supra*note 312.

317 Brennan/Lockridge, *How visual co-presence and joint attention shape speech planning*. (in preparation), at www-2.cs.cmu.edu/~kraut/RKraut.site.files/articles/kraut02-VisualInfoInSharedVisualSpaces.pdf.

[318] See Chapter 1, Section IV.1.D.b Macro Virus, above.
[319] See Chapter 1, Section IV.1 Security, above.
[320] On these issues, see Kaufmann-Kohler/Schultz, *supra* note 2, pp. 217–223.
[321] See further Chapter 1, Section III.3.B First master it, then use it, above.
[322] See further Chapter 1, Section IV.2 Technical failures, breakdowns, above.
[323] See further Chapter 1, Section III.3.A Do not overdo it, above.
[324] See further Chapter 3, Section I State of practice, above.
[325] For a proposal of procedural order, see Section IV.2 Procedural order relating to the use of IT, below.
[326] On all the above, see Chapter 1, Section VI.1.A Sending e-mail, above.
[327] See Chapter 1, Section VI.2 Privacy risks through metadata, above.
[328] See Chapter 1, Section IV.1.D.a Viruses, above.
[329] See Chapter 1, Sections IV.3 Issues of authentication and non-repudiation and VI.1.E E-mail encryption, digital signatures, and digital certificates, above, and Section V Setting up encrypted and digitally-signed e-mail, below.
[330] See Section V Setting up encrypted and digitally-signed e-mail, below.
[331] On these two recommendations, see Chapter 1, Section VI.1.B Receiving e-mail, above.
[332] Gibbons/Kennedy/Gibbs, *supra* note 295, p. 34, citing J. Lanier, *Virtually There*, Scientific American, p. 66.
[333] Kaufmann-Kohler/Schultz, *supra* note 2, p. 64.
[334] See Chapter 4, Section II.3 Assessment of videoconferencing in arbitration and recommendations regarding its use, above.
[335] See Chapter 4, Section II.5 Setting up a videoconferencing session, above.
[336] Standard actions are: determination of date and time, terminal stations, and participants, followed by testing.
[337] This order can either be issued as a separate ruling or incorporated into a first procedural order dealing with the relevant matters of procedure. Language in brackets is suggested or an optional addition.
[338] One can also make a distinction between memorials (e.g. by e-mail and CD-Rom) and exhibits (e.g. only on CD-Rom).
[339] See Chapter I, Section IV.1 Security, above.
[340] See Chapter I, Section VI.1.E E-mail encryption, digital signatures, and digital certificates, above.
[341] See www.hushmail.com -> Support -> Using PGP with Hushmail.
[342] For a more complete description, including older encryption software, see www.hushmail.com/help.php?subloc=pgp&l=454.
[343] See www.hushmail.com -> Support -> Using PGP with Hushmail.

Rechtsgebiet:	Rechtsinformatik
Erschienen in:	Jusletter 5. Dezember 2005
Zitiervorschlag:	Gabrielle Kaufmann-Kohler / Thomas Schultz, The Use of Information Technology in Arbitration, in: Jusletter 5. Dezember 2005
Internetadresse:	http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4410