Final Report
Informal Working Group on Cross-border Videoconferencing

D1 Final Report

Deliverable Id :	D1
Deliverable Name :	Final Report
Status :	Version 1.0
Dissemination Level :	EU Member States, Council and Commission
Date of deliverable :	02 March 2014
Organisation name of lead partner for this deliverable :	Austrian Federal Ministry of Justice
Author(s):	Delegations of AT, ES, FR, NL, SE, SI, UK, EUROJUST, CCBE. AVIDICUS 3 project
Partner(s) contributing :	CZ, DE, EE, EL, IE, HR, HU, IT, LV, MT, PL, Court of Justice, Council, Commission

Abstract:

This **final report** from the **Informal Working Group (IWG) on Cross-border Videoconferencing (VC)** aims to promote the practical use of and share best practice and expertise on the

- organisational,
- technical and
- legal aspects

of cross-border VC to help improve the overall functioning of e-Justice systems in Member States and at a European level.

The main topics of the work of this informal group were to:

- Identify the practical problems of real VC users;
- Identify best practices and solutions to solve these problems;
- Suggest concrete (short-term) actions to improve the situation;
- Suggest specific projects to improve the situation.

Table of contents

History ..... **Error! Bookmark not defined.**
Table of contents 2
List of Abbreviations 6
Executive Summary 7
Short summary of insights gained and needs identified 11
1. Goals and alignment with e-Justice Action Plan 14
1.1. Goals of the Informal Working Group on Cross-border Videoconferencing 14
1.2. Topics 14
1.3. Alignment with the e-Justice Action Plan 15
1.3.1. Videoconferencing in the European e-Justice Action Plan 15
1.4. Videoconferencing as a proven and efficient tool 15
1.4.1. Applying videoconferencing to simple and more complex judicial use-cases 17
1.5. Additional complexity of cross-border videoconferencing 18
1.6. Working method of the IWG on Cross-border Videoconferencing 19
2. Report of the Legal Sub-group 21
2.1. Context 21
2.2. Legal framework 22
2.3. Guiding principles 28
2.3.1. Limitations of hearings by videoconference 28
2.3.2. Added value of hearings by videoconference 29
2.4. Actors 31
2.4.1. Witnesses, victims and experts 31
2.4.2. Suspected and accused persons. The assistance of a lawyer 33
2.4.3. Interpreters 36
2.4.4. Direct contacts and negotiation of arrangements between the issuing and the executing Member State 37
2.4.5. The assistance and support of the European Judicial Network and Eurojust 37
2.5. Issuing, transmission and execution of rogatory letters requesting a hearing by videoconference 39
2.5.1. Issuing 39
2.5.2. Transmission 39
2.5.3. Execution 39

2.5.4. Relevant changes introduced by the Directive on EIO 40
2.6. The use of videoconference at the different stages of a criminal procedure 42
2.7. Additional use of videoconferencing - Using videoconferencing at hearings of children in criminal proceedings 43
2.8. Documentation 45
2.8.1. Documentation in accordance with European and international legal instruments 45
2.8.2. Documentation in accordance with national legal systems 45
2.9. Conclusions and recommendations 45
2.10. French experience on operational and technical aspects with videoconferencing 46
2.10.1. General Remarks 46
2.10.2. The verification of the users' roles and identities 47
2.10.3. The security of the exchange to guarantee data integrity and the protection of transmitted data 47
2.10.4. Suggested short-time actions 47
2.11. CCBE position regarding the use of videoconferencing in cross-border criminal proceedings 48
3. Report of the Organisational Sub-group 50
3.1. Findings: Key problem areas identified 50
3.2. Statistics on videoconferencing Questionnaires 50
3.3. Typical organisational problems identified 52
3.4. Specific short-time actions suggested 53
3.4.1. Organisational Action 1 – MS's overall position with videoconferencing 53
3.4.2. Organisational Action 2 – Information on videoconferencing contact point / contact person/s 54
3.4.3. Organisational Action 3 - Language 55
3.4.4. Organisational Action 4 – Formal process for mutual assistance 56
3.4.5. Organisational Action 5 – Time-zones 56
3.4.6. Organisational Action 6 – Exchange of technical videoconferencing parameters 56
3.4.7. Organisational Action 7 – Training of videoconferencing users 57
3.4.8. Organisational Action 8 – Step-by-step protocol for videoconferencing 58
3.4.9. Organisational Action 9 – Technical support 59
4. Report of the Technical Sub-group 60
4.1. Using a questionnaire as starting point 60

4.2. Findings of the Technical Sub-group 60
4.3. Security and data protection 62
4.4. Comparable or similar setup of technical videoconferencing architecture 63
4.4.1. Sweden 64
4.4.2. Slovenian video conferencing architecture 64
4.4.3. The Netherlands 65
4.4.4. United Kingdom – England and Wales 66
4.5. General advice: Implement the same international standards 67
4.6. Mutual recognition of national laws 67
4.7. Projects suggested during the meetings. 68
4.8. Specific (funding) projects suggested. 69
5. Security aspects 70
5.1. Basic ICT security principles 70
5.1.1. Confidentiality 70
5.1.2. Integrity 71
5.1.3. Availability 71
5.1.4. Accountability / non repudiation 72
5.2. Some practical guidelines 72
5.2.1. Risk assessment 72
5.2.2. The risk management framework 73
5.2.3. Potential measures as a part of profiles 74
5.2.4. Elements of the request for important for security 74
5.3. Conclusion 75
6. Videoconferencing with an interpreter (outcomes of the AVIDICUS projects) 76
6.1. Main configurations of bilingual videoconferencing with an interpreter 76
6.2. Videoconferencing and interpreting: communicative aspects 77
6.2.1. The AVIDICUS projects 78
6.2.2. Main outcomes of the AVIDICUS projects 80
6.2.3. Implications 84
6.3. Conclusions 85
7. Projects suggested 87
7.1. Content items for projects 87
7.2. Summary of the project "Multi-aspect Initiative to Improve Cross-border Videoconferencing" 89
7.2.1. Objectives 89

7.2.2. Activities 89
7.2.3. Type and number of persons benefiting from the project 90
7.2.4. Expected results 90
7.2.5. Type and number of outputs to be produced 90
7.3. Project Partners 91
8. Appendices 92
VC-ANNEX-01: All completed videoconferencing Questionnaires sorted by Member State and ID 92
VC-ANNEX-02: Sorted report on all completed videoconferencing Questionnaires sorted by Topic, Category, Priority and Usergroup 92
VC-ANNEX-03: Statistics on all completed videoconferencing Questionnaires 92
VC-ANNEX-10: Project description "Multi-aspect initiative to improve cross-border videoconferencing" 92

List of Abbreviations

Acronym	*Explanation*
AVIDICUS	AVIDICUS 3 is an EU funded project running from 2013 to 2015, which focuses on the use of videoconferencing in bilingual legal proceedings that involve an interpreter
CCBE	Council of Bars and Law Societies of Europe (CCBE)
Defence agent	Defence agents are external VC users in UK Scotland with responsibilities similar to a lawyer
EAW	European Arrest Warrant
EIO	European Investigation Order
H.239	H.239 is an ITU (International Telecommunication Union) Telecommunication Standardization Sector (ITU-T) recommendation from the H.32x Multimedia Communications' macro family of standards for multimedia communications over various networks. The H.239 recommendation is titled "Role management and additional media channels for H.3xx-series terminals". Practical importance of this recommendation is its setting forth a way to have multiple video channels (e.g., one for conferencing, another for presentation) within a single session (call). (Source: Wikipedia)
H.323	H.323 is a recommendation from the ITU-T that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signalling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences. (Source: Wikipedia)
IP	Internet Protocol (primary protocol in the Internet layer of the Internet protocol suite, has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers). (Source: Wikipedia)
ISDN	Integrated Services Digital Network (set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network). (Source: Wikipedia)
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IWG	Informal Working Group. Note: the Informal Working Group on cross-border videoconferencing was appointed by the Council Working Party e-Law (e-Justice)
SIP	Session Initiation Protocol (SIP) is a standardized set of formats for communicating messages used to initiate, control, and terminate interactive user sessions with multimedia services such as Internet telephone calls, video conferencing, chat, file transfer, and online games. (Source: Wikipedia)
sTESTA	secured Trans European Services for Telematics between Administrations
TESTA-ng	Trans-European Services for Telematics between Administrations – new generation
VC	Videoconferencing (sometimes also videoconference)
VTC	Video teleconference

Table 1: Abbreviations

Executive Summary

This report from the informal working group (IWG) on cross-border videoconferencing (VC) aims to promote the practical use of and share best practice and expertise on the organisational, technical and legal aspects of cross-border VC to help improve the overall functioning of e-Justice systems in Member States and at a European level.

As outlined in the action plan for a Strategy on European e-Justice 2014 – 2018, going to court and initiating extrajudicial proceedings in cross-border situations should be facilitated through the availability of communication by electronic means between courts and parties to proceedings, as well as witnesses, experts and other participants. There are many benefits to be gained, for example in oral hearings where VC can remove the need to travel to court to take part in judicial proceedings, in particular in cross-border cases.

The main topics of the work of this informal group were to:

- Identify the **practical problems** of real VC users;
- Identify **best practices and solutions** to solve these problems;
- Suggest concrete **(short-term) actions** to improve the situation;
- Suggest specific **projects** to improve the situation.

To avoid duplication of work, this report contains references to other VC projects and useful materials from other sources including:

- Potential **synergies with other projects,** e.g. European e-Justice Portal, e-CODEX, AVIDICUS projects (interpretation during a videoconference) and the European Judicial Training Network;
- **Existing useful material on VC,** e.g. VC materials already available at the European e-Justice Portal videoconferencing pages, VC materials from Member States (e.g. VC configurations and experiences) and from EUROJUST (e.g. security considerations with VC).

The objective of this report is to bring together current practice in Member States on the organising and running of cross-border videoconferences. The main findings and conclusions demonstrate that, while legal aspects need to be respected, the majority of immediate problems and issues that arise when using cross-border VC are the technical and organisational aspects. These are outlined below:

Technical

Some of the potential technical issues that can occur include:

- Incompatible technical standards;
- Insufficient bandwidth on IP connection / ISDN bandwidth restrictions;
- Security measures like firewalls that prevent contact being established;
- Insufficient technical support;
- Maintaining the security of the network while allowing links to outside organisations and individuals.

In order to improve the quality of VC sessions the following technical standards are recommended:

- Use a hardware-based video conferencing system (H.323/videoconference SIP);
- VC session to be IP–based;
- Use firewall traversing infrastructure;
- Use encrypted communications (AES-128);
- Receive the presentation as a duo video (H.239).

Organisational

Difficulties can arise when one Member State (MS) tries to communicate with another MS to organise a VC session:

- The contact information of the relevant people and the details of relevant competent courts must be readily available and kept up to date;
- A common language needs to be agreed along with appropriate translation and interpretation services and agreement on which time-zone will be used to determine when the VC starts;
- The process can also be hindered by the time it can take to process an application to use VC in mutual assistance cases;
- Effective mechanisms need to be in place to exchange relevant technical parameters, particularly information that is confidential and must only be exchanged securely.

It is important that effective training is available for all users, including judges and prosecutors, along with clear protocols and ongoing technical support for all phases of testing, initiating and running the VC.

Legal

Videoconferencing offers a convenient option to ensure the hearing of witnesses, experts and accused persons without the need to compel them to travel to the Member State where the investigation or trial is being conducted.

VC has gained legal recognition through international conventions and more recently European Union law, with the European Investigation Order Directive.

While bringing added protection to witnesses and vulnerable persons, the use of VC also has the potential to be detrimental to defence's rights and special care must be taken to ensure the principles of immediacy, equality of arms and contradiction are respected,

The following further actions are therefore proposed:

- Assess the impact of the European Investigation Order in relation to current procedural rules;
- Devise tools to help judicial authorities to identify the legal instrument applicable for the organisation of a particular videoconference;
- Devise tools to help judicial authorities to identify the competent authority for the organisation of a given videoconference;
- Ensure legal support for the proposed practical results of the working group, in line with the overarching principles of European law e.g. contradictory principle, immediacy, equality of arms and proportionality.

Next steps

This report summarises a number of insights gained, identifies a number of needs and contains suggestions for short-term actions to improve cross-border VC. These actions should be implemented by Member States in close cooperation with the European Commission, e.g. improving VC contact information in the European e-Justice Portal videoconferencing pages along with the other organisational improvements suggested.

Additional activities and specific content have also been identified that could help with these improvements. These will require more effort and time than the short-term actions. A sub-set of the Member States participating in the informal working group on cross-border videoconferencing are submitting a funding proposal to the Justice Funding Programme to address several of these. The funding proposal aims to:

- identify which cases would benefit most from increased and better use of cross border VC;
- develop a step-by-step protocol with instructions for specific cross border VC use cases;
- perform practical testing of point to point and multi point VC between different Member States;
- summarise recommended technical standards from a practical perspective; and
- develop a form to request and/or confirm a cross-border VC between Member States.

Finally, the following suggestions should be implemented by follow-on projects if further resources are available:

- support for the training and motivation of cross-border VC users through demonstration of typical VC use cases;
- perfecting VC between pairs of Member States; and
- Implement electronic sending of forms for cross-border mutual legal assistance, e.g. starting with forms for "direct taking of evidence" using the European e-Justice Portal and e-CODEX.

Short summary of insights gained and needs identified

Insights gained
VC is a proven cost-efficient tool applicable to many different national and cross-border use-cases in criminal and civil/commercial (taking of evidence) matters, e.g.: • Avoiding the transport of persons in custody • Taking remote witness or victim testimony • Hearing expert's opinion • Suspects and accused person's statements • Hearing of a party or representative of the party Added value of VC: • Less intrusive measure than the European Arrest Warrant (EAW) and temporary surrender • Access to justice and added protection for remote victims, vulnerable victims (e.g. children) and witnesses • Cost-effectiveness

Insights gained

Majority of current practical problems fall into the organisational and technical category.

Organisational difficulties:

- Finding the right contact point/contact person in the other country, missing or outdated contact information
- Language for communication: Translation / interpretation / language skills already needed when organising a cross-border videoconference
- Time taken by the formal process for requests for mutual assistance
- Missing an effective mechanism for exchange of relevant technical parameters
- VC users need a detailed step-by-step description ("protocol") for planning, organising and running VC, which combines organisational, legal and technical elements for typical judicial VC cross-border use-cases
- Potential internal and external VC users might lack confidence, motivation and training in carrying out a VC

Technical difficulties:

- Incompatible technical standards
- Insufficient bandwidth on IP connection / ISDN bandwidth restrictions
- Security measures like firewalls that prevent contact being established
- Insufficient technical support
- Maintaining the security of the network while allowing links to outside organisations and individuals

Legal frame-work:

- VC has gained more and more recognition through international conventions and recent European Union law (European Investigation Order Directive)
- Formal processes for requests for mutual legal assistance must be followed, which might be time-consuming
- National law places restrictions on the use of VC for the hearing of accused or suspected persons – especially for the main tribunal phase
- Care must be taken for not violating defence's rights and to ensure the principles of immediacy, equality of arms and contradiction are respected

Needs identified

Improving organisation, preparation and running of cross-border VC:

- Improving the information on national VC contact points and improving the organisation contact points at national and court level – e.g. introducing a national VC contact point in each MS
- Improved form for the effective exchange of variable and/or confidential VC parameters in conjunction with public and static information on VC facilities for each MS to be published on the European e-Justice Portal.
- VC users need guidance on typical judicial use-cases which would benefit most from increased and better use of cross-border VC
- VC users need a clear step-by-step description for preparing and running cross-border VC which fits with their typical judicial cross-border VC use-cases and combines all organisational, technical and judicial elements needed.
- VC users and technical planning and support staff need guidelines on the recommended technical standards from a practical perspective
- VC interoperability between MS is to be improved by carrying out systematic practical tests between pairs of MS to document working parameters. These can then be re-used to establish more reliable VC between MS with sufficient audio and video quality.
- The use of VC facilities at the European Level (e.g. multi-point control units at Eurojust or at the Commission) by creating secure "virtual VC meeting rooms" where the participating MS could dial-in should be considered.
- Internal and external potential VC users should be motivated and trained to increase their confidence and ability to run cross-border VC.
- Electronic sending of forms for requests for cross-border mutual legal assistance should be considered further by combining dynamic forms functions from the European e-Justice Portal with e-CODEX, e.g. forms for "direct taking of evidence" and "(indirect) taking of evidence".

1. GOALS AND ALIGNMENT WITH E-JUSTICE ACTION PLAN

1.1. Goals of the Informal Working Group on Cross-border Videoconferencing

Following instruction from the Council **Working Party e-Law (e-Justice),** the main focus of this informal working group has been on **cross-border** videoconferencing.

The **goal** of the "Informal Working Group on Cross-border Videoconferencing" was therefore to:

- **Promote the practical use of cross-border videoconferencing (VC) and share experience about cross-border VC.**

Note: even when focussing on cross-border videoconferencing, the work carried out is as relevant for national videoconferencing as many of the problems and best practices identified are identical: e.g. in stimulating and motivating judges and other legal professionals to use VC.

1.2. Topics

The main topics covered by the informal working groups were:

- **Identify the practical problems of real VC users**

  Not only judges, but also other internal and external users and partners, e.g. prosecutors, detention centres, police, hospitals, experts, lawyers, defence-agents, witnesses, parties, suspected and accused persons.

- Identify **best practices and solutions** to solve these problems
- Suggest concrete (short-time) **actions** to improve the situation
- Suggest specific **projects** to improve the situation
- Identify **synergies with other projects** (e.g. European e-Justice Portal, e-CODEX, AVIDICUS projects, European Judicial Training Network)
- Identify and promote useful **existing materials on VC** (e.g. useful VC materials already available at the European e-Justice Portal, useful VC materials of other VC projects).

1.3. Alignment with the e-Justice Action Plan

As this informal working group was founded by and reports to the Council "Working Party e-Law (e-Justice)", it's work is fully aligned with the e-Justice Action Plan.

1.3.1. Videoconferencing in the European e-Justice Action Plan

Specific actions for videoconferencing in the e-Justice Action plan are:

Project	**Responsibility for action**	**Actions to be taken**	**Timetable**	**Category**
30. Videoconference • Organising and running cross-border videoconferences (in all MS) • IT tools helping to support and organise videoconferences • enhancing interoperability for videoconferencing • form for requesting/ confirming a cross-border videoconference • Network for exchange of experience and sharing best practice on videoconferencing, including training (participation of legal practitioners: judges, public prosecutors, lawyers, mediators, legal interpreters)	Member States and the Commission	Informal group	2014 to 2016	A

1.4. Videoconferencing as a proven and efficient tool

At the national level videoconferencing is used in most Member States as a well-established tool of the judiciary which can be applied in all kinds of judicial proceedings – e.g. in criminal prosecutions and also in civil/commercial – depending on the national law and the priorities of the specific Member State.

Typical VC use-cases in criminal and prosecution proceedings are to:

- Avoid the transport of persons in custody by hearing them via videoconference.
    - Note: this is one of the use-cases with the highest benefits in terms of cost-savings and helping to increase security.
    - Many MS used this as starting point for the development of their VC infrastructure as investment can be directly justified by the cost-savings achieved.
- Take witness testimony
- Hear experts opinion via VC
    - VC enables the Judiciary to respect the time management of external experts by avoiding travel times and by minimising the impact of proceeding-delays on time-constrained important experts (e.g. medical experts like forensic doctors and psychiatrists).
    - Therefore the use of VC is often more efficient also for the affected stakeholders themselves – and not only more efficient for the Judiciary.
- Take suspects and accused person's statements
    - Note: in some Member States (see chapter 2.4.2 Suspected and accused persons. The assistance of a lawyer) the use of VC with the defendant is limited. E.g. in Austria the use of VC is limited (by national law and a court decision, see chapter 2.3.1 Limitations of hearings by videoconference) to preliminary proceedings only and not allowed for the main trial, where for reasons of immediacy the defendant has to stand physically in front of his judge or tribunal.

Typical VC use-cases in civil/commercial are quite similar (taking of evidence):

- Take witness testimony
- Hearing of expert / interpreter
- Hearing of party or representative of the party

In civil proceedings the "direct taking of evidence" is one of the most popular use-cases at national and cross-border level because the VC hearing is the responsibility of the requesting court and the assisting court must only provide a VC room and a person, who can start the VC, identify the witness, attend at and supervise the remote room. If the identity of the witness is to be established only by an authorized authority (judge) and how the oath is taken depends on the national procedural law of the assisting court.

Some MS (e.g. AT, LV) have even created national VC booking systems, where the judge can book both national VC rooms and the assisting person at the remote room is automatically informed to start and control the remote equipment and to guide the remote participants when the VC takes place.

VC technology supports the quality of justice:

- Future vision: VC is a step in the technological development within the lawsuit.
- VC recorded statements, audio and video, enable parties to further test the written interpretation of a judicial activity.
- This contributes to the quality of justice. In parallel, these changes in the method call for judges, court clerks, prosecutors and lawyers to get additional education and training.
- Because VC effortlessly bridges locations that are separated by great distances the prosecution is enabled to deal with those issues that otherwise due to high costs are not addressed. This supports the equality and legal certainty and stresses that VC is more than a cost effective tool.

1.4.1. Applying videoconferencing to simple and more complex judicial use-cases

VC can be applied to simple and more complex use-cases (e.g. multi-point VC with high bandwidth requirements), which might also require higher security levels.

The following are examples of reaching from simple to complex VC use-cases:

- Hearing of a single remote person (point-to-point VC)
- Hearing of a single remote person with consecutive interpretation
    - Note: a robust simple setup, which works well in practice is the following:
        - The judge sits the interpreter (whom they trust) beside themself in the same VC room.
        - The interpreter does consecutive translation of the questions from the judge and the answers of the remote single person (e.g. witness, expert, party, victim, suspected person).
    - Note: doing simultaneous interpretation will be (much) more difficult! Consult the results of the "AVIDICUS" projects for guidance, before trying to use VC with simultaneous interpretation.
- Multi-point VC: e.g. coordination meeting between EUROJUST and MS fighting serious crime
    - Note: This type of use-case will require high security, consult the chapter about security considerations in this document.
- Main tribunal with “true-to-live” VC environment
    - Note: the Netherlands are experienced with this type of setup.

1.5. Additional complexity of cross-border videoconferencing

Most Member States with VC installed for national use do also cross-border VC. But feedback from MS highlights that a cross-border videoconferencing adds additional levels of complexity which must be overcome:

- **Organisational**
  - Finding the right contact-point or contact-person in the foreign country to organize, setup and start the cross-border videoconference.

- **Language**
  - When organising the videoconference the contact-person in the foreign country might not understand your language or English.
  - The need for translation during a videoconference hearing – with the interpreter either physically present near the judge, physically present at the site of the foreign witness/party, or by connecting the interpreter over an additional videoconferencing link by doing a "multipoint videoconference".

- **Technical**
  - You must follow the **recommended technical standards** to enable cross-border VC (see chapter about recommended technical standards or the e-Justice Portal information pages on videoconferencing).
  - The partner-network will be protected by firewalls and you need to use gateway solutions or "virtual rooms".
  - You must exchange the technical parameters for starting the videoconference, e.g.: Type of connection (IP or ISDN, ISDN-Number or IP-Address, parameters for bandwidth to be used, parameters for quality of video- and audio, passwords for gateway-solutions).
  - You need to have some flexibility on the technical level and a good national technical support to achieve fitting technical parameter allowing to start the cross-border video-conference with sufficient video and audio quality. Video and audio.
    - Doing a test one week or some days before the actual VC hearing is highly recommended to avoid surprises!

- **Legal framework**
    - The formal process for cross-border mutual legal assistance, which have to be done in order to get permission for VC in the specific case, can take too long (can be up to several months!)
    - National laws can forbid or limit the use of VC for specific proceeding types or for specific use-cases.

This was the main reason, that the Council Working Party e-Law (e-Justice) decided to found the "**Informal Working Group on Cross-border Videoconferencing**", which started its work in January 2014.

1.6. Working method of the IWG on Cross-border Videoconferencing

Initially, the IWG issued a questionnaire to all interested Member States and organisations (e.g. EUROJUST) to get an overview on the real practical problems and issues with cross-border VC.

The completed questionnaires helped to detect the **typical problem areas** and displayed the majority of problems in the **organisational** and **technical** category:

- **Organising a videoconference, e.g.:**
    - **Contact person** in the other MS cannot be found
    - Contact person is unable to understand me – **language problem**
    - Wrong start-time because of different time-zones
- **Organisational (Legal), e.g.:**
    - **Formal process for mutual assistance** to get permission for VC takes too long (can be months!)
- **Technical problems - unable to start VC, e.g.:**
    - Wrong ISDN Number / wrong IP address / behind firewall / incompatible standards / insufficient bandwidth / parameters for optimizing quality of video and audio

In addition, by using different topics within the same questionnaire, suggestions for improvement were received in form of best practices, solutions, useful materials, suggestions for short-time actions and suggestions for projects.

After evaluating the completed questionnaires, the Informal Working Group on Cross-border Videoconferencing decided to **concentrate work on the critical aspects**, which are the

- **technical** and
- **organisational**

problems to deal with.

Since the procedures for "cross-border mutual legal assistance" in criminal or civil/commercial are currently a too formal and time-consuming prerequisite before doing a videoconference, it was decided that the

- **legal** aspects

of the surrounding legal framework have to be considered as well.

Therefore the IWG decided to organise its work – according to the major problem areas detected – within 3 sub-groups:

- **Legal sub-group**, led by the Ministries of Justice of Spain and France and supported by EUROJUST and EJN
- **Technical sub-group**, led by the Ministry of Justice of The Netherlands and supported by Sweden and UK (England and Wales, Scotland)
- **Organisational sub-group**, led by the Ministry of Justice of Austria and supported by Netherlands, Sweden and UK.

Thanks are due to all participants for their valuable contributions during the meetings and to this final report!

2. REPORT OF THE LEGAL SUB-GROUP

Videoconferencing in cross-border Criminal, civil and commercial proceedings Operational and legal problems

2.1. Context

In the course of an investigation or in further steps of a criminal procedure, the undertaking of some measures in another Member State of the EU or in a third country might be necessary. Among such measures, the judicial authorities might need the gathering of a witness testimony, the collection of a forensic expert opinion, or the hearing of a suspected or accused person who is residing in another Member State´s territory.

It is common practice for judicial authorities to issue letters of request summoning the witness or expert concerned to appear in its territory at the time agreed for a hearing. For the purposes of conducting a criminal prosecution, the judicial authorities tend to request temporary surrender, arrest and surrender through an European Arrest Warrant or, if the individual concerned is residing in a third State, their extradition.

Also in the course of a civil or commercial procedure, the undertaking of some measures in another Member State of the EU or in a third country might be proposed by one of the parties of the proceedings. Among such measures, the judicial authorities might need the gathering of a witness testimony or the collection of an expert opinion from someone who is residing in another Member State's territory.

As a general rule in the civil or commercial proceedings a party proposes witnesses or experts to be heard. If the proposed person to be heard resides in another EU Member State or a third country, the costs of travelling and being present at the court can represent a heavy financial burden for the proposing party to cover This is because in civil and commercial matters the proposing party is the one who covers the expenses. Although the expenses of the party's proposal can be recovered in damages from the other party, they sometimes cannot afford to cover the initial up-front costs.

The development of new technologies and the progressive improvement of videoconference systems in the Judiciary has created new possibilities in order to ensure the hearing of witnesses, experts and accused persons without the need to compel them to travel to the Member State where the investigation or the trial is being conducted.

The increasing use of videoconference in cross-border criminal, civil and commercial proceedings is however subject to certain limitations and conditions of a technical, organisational, and legal nature.

This report focuses on the limitations and conditions of a legal nature for the use of videoconference in cross-border criminal proceedings, and proposes best practices and recommendations to overcome them. It has been drafted by Eurojust, the European Judicial Network, the Spanish Ministry of Justice, and the French Ministry of Justice in the framework of the Informal Working Group (IWG) on videoconference set up within the Working Party of the Council on e-Law (e-Justice).

The report also mentions the civil and commercial proceedings with cross border elements where proceedings between different Member States are becoming more common. The use of videoconferencing systems provides a higher level of legal certainty in a global community.

2.2. Legal framework

The legal framework governing the use of videoconferencing in cross-border cases is mainly composed of two sets of rules: the European and international legal instruments, and the national Codes of Criminal and Civil Procedures.

As regards the European legal instruments, the *Council of Europe Convention of 20 April 1959 on Mutual Assistance in Criminal Matters* (1959 Convention) includes several legal provisions on the summoning of witnesses, experts and prosecuted persons and their further participation in hearings in the requesting Party territory. However, it does not make any reference to the hearings by videoconference: at the time the 1959 Convention was adopted, the relevant technology were barely developed and did not allow for a hearing by videoconference between two Contracting Parties.

The *Second Additional Protocol to the 1959 Convention, dated 8 November 2001*, devotes Art. 9 to the hearing by videoconference[1]. It is an extensive legal provision that reproduces almost entirely Art. 10 of the *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union* (2000 Convention)[2].

A large number of EU Member States[3], other European countries[4] and third States[5] have ratified this Protocol. Austria, Cyprus, Germany, Greece, Hungary, Ireland, Italy, Luxembourg signed the Protocol but have not ratified it yet. Spain is not a signatory Part to the Protocol.

In the European Union, the above mentioned 2000 Convention lays down provisions for the use of videoconference in cross-border cases in Art. 10. This Convention has been ratified by the majority of the EU Member States, with the exception of Croatia, Greece, Ireland and Italy.

The *Agreement between the EU and Iceland and Norway on the application of certain provisions of the 2000 Convention and its Protocol*[6] expressly includes hearing by videoconference using Art. 10 of 2000 Convention within its scope.

Clearly inspired by the above mentioned legal provisions, *Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order (EIO) in criminal matters*[7] has laid down in Article 24 the hearing by videoconference or other audiovisual transmission:

---

1 See status as of 18 September 2014 at http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=182&CM=8&DF=18/09/2014&CL=ENG

2 OJ C 197, 12.7.2000, p. 3.

3 Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, Ireland, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Sweden and United Kingdom.

4 Albania, Armenia, Bosnia and Herzegovina, Georgia, Ukraine, Moldova, Montenegro, Norway, Serbia, Switzerland.

5 Chile and Israel.

6 Art. 1(1) of the Agreement, second paragraph. OJ L 2, 29.1.2004, p. 3.

7 OJ L 130, 1.5.2014, p. 1.

"*1.Where a person is in the territory of the executing State and has to be heard as a witness or expert by the competent authorities of the issuing State, the issuing authority may issue an EIO in order to hear the witness or expert by videoconference or other audiovisual transmission in accordance with paragraphs 5 to 7. The issuing authority may also issue an EIO for the purpose of hearing a suspected or accused person by videoconference or other audiovisual transmission.*

2 In addition to the grounds for non-recognition or non-execution referred to in Article 11, execution of an EIO may be refused if either:

(a) ***the suspected or accused person does not consent****; or*

(b) the execution of such an investigative measure in a particular case would be contrary to the fundamental principles of the law of the executing State.

3.The issuing authority and the executing authority shall agree the practical arrangements. When agreeing such arrangements, the executing authority shall undertake to:

(a) summon the witness or expert concerned, indicating the time and the venue of the hearing;

(b) summon the suspected or accused persons to appear for the hearing in accordance with the detailed rules laid down in the law of the executing State and inform such persons about their rights under the law of the issuing State, in such a time as to allow them to exercise their rights of defence effectively;

(c) ensure the identity of the person to be heard.

4.If in circumstances of a particular case the executing authority has no access to technical means for a hearing held by videoconference, such means may be made available to it by the issuing State by mutual agreement.

5.Where a hearing is held by videoconference or other audiovisual transmission, the following rules shall apply:

(a) the competent authority of the executing State shall be present during the hearing, where necessary assisted by an interpreter, and shall also be responsible for ensuring both the identity of the person to be heard and respect for the fundamental principles of the law of the executing State. If the executing authority is of the view that during the hearing the fundamental principles of the law of the executing State are being infringed, it shall immediately take the necessary measures to ensure that the hearing continues in accordance with those principles;

(b) measures for the protection of the person to be heard shall be agreed, where necessary, between the competent authorities of the issuing State and the executing State;

(c) the hearing shall be conducted directly by, or under the direction of, the competent authority of the issuing State in accordance with its own laws;

(d) at the request of the issuing State or the person to be heard, the executing State shall ensure that the person to be heard is assisted by an interpreter, if necessary;

(e) suspected or accused persons shall be informed in advance of the hearing of the procedural rights which would accrue to them, including the right not to testify, under the law of the executing State and the issuing State. Witnesses and experts may claim the right not to testify which would accrue to them under the law of either the executing or the issuing State and shall be informed about this right in advance of the hearing.

6.Without prejudice to any measures agreed for the protection of persons, on the conclusion of the hearing, the executing authority shall draw up minutes indicating the date and place of the hearing, the identity of the person heard, the identities and functions of all other persons in the executing State participating in the hearing, any oaths taken and the technical conditions under which the hearing took place. The document shall be forwarded by the executing authority to the issuing authority.

7.Each Member State shall take the necessary measures to ensure that, where the person is being heard within its territory in accordance with this Article and refuses to testify when under an obligation to testify or does not testify the truth, its national law applies in the same way as if the hearing took place in a national procedure."

The United Kingdom has notified its wish to take part in the adoption and application of this Directive[1]. Ireland is not taking part in the adoption of this Directive and is not bound by it or subject to its adoption[2]. Denmark is not taking part in the adoption of the Directive and is not bound or subject to its application[3].

Most of the international Agreements on mutual legal assistance signed between the European Union and third States also include a legal provision related to hearings by videoconference. For example the *Agreement between the EU and Japan on mutual legal assistance in criminal matters* (Art. 16)[4] and the *Agreement on mutual legal assistance between the EU and United States of America* (Art. 6)[5].

---

1 Recital (43) Directive on EIO.
2 Recital (44) Directive on EIO.
3 Recital (45) Directive on EIO.
4 OJ L 39, 12.2.2010, p. 20
5 OJ L 181, 19.7.2003, p. 34.

In the area of international cooperation, the *United Nations Convention against Transnational Organised Crime* contains two legal provisions regulating the use of videoconference (Arts. 18(8) and 24).

Spain has a convention (The Convenio Iberoamericano sobre el uso de la videoconferencia en la Cooperación Internacional entre Sistemas de Justicia, Mar de Plata 3.12.2010, (BOE 13.8.14)) with other iberoamerican countries regarding the use of videoconferencing between them (Spain, México, Ecuador, Panamá and Dominican Republic), and it could be a referent in some parts.

The object of the convention (first article) is to promote the use of videoconferencing between the competent authorities of the parties and to have an easier and stronger cooperation in civil, commercial and criminal matters.
Obviously, for this type of activity to work it is necessary to regulate the relationship with national law and the international law (art 3).

In absence of an applicable European or international legal instrument, some Member States (e.g. Spain) will agree on a particular hearing to be held by videoconference in accordance with the general principles of judicial cooperation in criminal matters, or in application of the principle of reciprocity.

The national Codes of Criminal Procedure of the EU Member States include some legal provisions on the use of videoconference. Although such legal provisions are related to national criminal proceedings, they have also to be taken into consideration in cross-border cases. In the case of Spain, the hearings by videoconference are mainly regulated in Art. 731bis of the *Ley de Enjuiciamiento Criminal*[1] (ES LECrim) and in Art. 229(3) of the *Ley Orgánica 6/1985, de 1 de Julio, del Poder Judicial*[2] (ES LOPJ). *Spain also has numerous bilateral mutual legal assistance conventions.*

1 Published at "Boletin Oficial del Estado" (BOE) n. 260, 17.9.1882.
2 BOE n. 157, 2.7.1985.

As regards the European legal instruments, the Council Regulation (EC) No. 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters [1], with the exception of Denmark, includes provisions for two ways of taking evidence in civil matters in cross border cases. These are direct transmission of requests between the courts and the direct taking of evidence by the requesting court. The Regulation provides for easier communication between the competent courts with the help of a designated central authority whose main role is to communicate and help the requesting court in another Member State take all the steps to provide for a fair trial for everyone and Art. 17 (4) shall encourage the use of communications technology, such as videoconferences and teleconferences.

Between Denmark and the other Member States the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters of 1970[2] applies. A large number of third countries have ratified the Haag evidence convention [3].

In addition to the European and international legal instruments applicable, and the national rules of criminal and civil proceedings, another relevant set of rules are the practical arrangements agreed between the issuing and the executing authority involved in a particular hearing by videoconference.

The practical arrangements are a precondition for the organisation of hearings concerning suspected and accused persons. They must cover the decision to hold the videoconference and the manner in which the videoconference will be carried out[4], and pay special attention to the gathering of the suspected or accused person´s consent.

The practical agreements are also necessary in other situations, for instance, in cases when the requested Member State does not have the technical means for a videoconference and the requesting Party wishes to ensure availability of such means[5].

The practical agreements will be also extremely useful when a hearing by videoconference is intended to collect testimonies of victims at risk of intimidation or in need of protection. In these situations, the competent authorities of the requesting and requested States must consider carefully

1 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001R1206

2 http://www.hcch.net/index_en.php?act=conventions.text&cid=82

3 http://www.hcch.net/upload/overview20e.pdf

4 Art. 10(9) 2000 Convention.

5 See for instance Art. 9(2) Second Protocol of 1959 Convention; Art. 10(2) 2000 Convention.

the measures to be adopted for the protection of the person concerned[1].

2.3. Guiding principles

2.3.1. Limitations of hearings by videoconference

The principles of immediacy and equality of arms

Some of the fundamental rights and principles of the criminal procedure enshrined in the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (EU Charter) could potentially be compromised during a hearing by videoconference in a cross-border case.

In particular, the right to a "fair" hearing proclaimed in Art. 6(1) ECHR, and the rights of the suspected and accused person to defend themself in person, through legal assistance of his/her own choosing or to be given it free (Art. 6(3)(c)), the right to examine witnesses against him/her (Art. (3)(d)), and the right to have the free assistance of an interpreter (Art. 6(3)(d)) may be affected.

The above mentioned rights are not absolute and may admit certain limitations, provided that such limitations are prescribed by the law, pursue a legitimate aim, are necessary in a democratic society and proportionate. The principle of proportionality entails that there is a reasonable relationship between a particular objective to be achieved and the means used to achieve that objective[2].

In the course of a hearing by videoconference, the limitations to the right of a fair trial or hearing[3] are due to the fact that the actors involved (e.g. the judicial authorities, the suspected or accused person, his lawyer, the interpreter, the victims, the experts, the translators) are located in different Member States and do not have the same opportunity to interact among each other as if they were in the same room or court. These limitations are certainly aggravated if the quality of the videoconference system does not meet the necessary standards.

---

1 Art. 23 Second Protocol of 1959 Convention. See this legal provision in relation to Art. 9(5)(b) of the same Protocol.

2 Delcourt c. Belgium, Judgment 17 January 1970.

3 The limitations to the rights mentioned in Art. 6(3) ECHR are analysed in Sections 4.2 and 4.3 to this Report.

It is generally acknowledged that the use of videoconference implies certain limitations of the principle of immediacy, as the judicial authority of the requesting Member State does not have the same proximity with the suspects, the witness and the experts as if they were in his presence, and therefore will not be able to appreciate so closely their statements and explanations, their movements and body language, and the nuance of their voices. The judicial authority of the requesting and requested Member State, when assessing the possibility to replace the physical presence of a witness, expert, suspected or accused person by a videoconference, must consider carefully whether the limitations of the principle of immediacy are proportionate to the aim pursued in that particular case. In jurisdictions where the principle of immediacy is a cornerstone of the criminal procedural law, this will be one of the greatest hindrances for the use of videoconferencing (E.g. in Austria, the Higher Regional Court of Vienna recently issued a verdict which clearly forbids the use of videoconferencing in criminal trials).

Another principle that might be compromised is the right to an equitable process and two other principles intrinsically linked to it: the contradictory principle, and the equality of arms. According to the right of an equitable process, both parties should have the same probabilities of defending their own interests and expose them in hearings and trials in conditions that are not disadvantageous vis-à-vis the counterpart[1]. Equality of arms may be breached, for instance, if the accused person has some difficulties to liaise and communicate fluently with this lawyer, or to understand clearly a witness or an expert who is giving testimony in a different room.

2.3.2. Added value of hearings by videoconference

Less intrusive measures than European Arrest Warrants and temporary surrenders.
Access to Justice of remote victims.
Costs-effectiveness

In some situations a hearing by videoconference may constitute an effective, proportionate and less intrusive measure than the arrest and surrender of an individual for the purposes of executing a European Arrest Warrant (EAW). This will be the case when the presence of the suspect before the judicial authority is not absolutely necessary, for instance, if such presence is required for the sole purpose of informing the suspect about his rights and charges.

---

1 Foucher v. France; Buruh v. Austria; Bobek v. Poland; Klimentyev v. Russia.

The Directive on the European Investigation Order promotes the issuing of EIOs for the hearing of suspects by videoconference as an alternative to the EAW, as follows[1]:

> *"With a view to the proportionate use of an EAW, the issuing authority should consider whether an EIO would be an effective and proportionate means of pursuing criminal proceedings. The issuing authority should consider, in particular, whether the issuing of an EIO for the hearing of a suspected or accused person by a videoconference could serve as an effective alternative".*

On the other hand, under certain conditions the use of videoconference or other technical means might ensure access to Justice for witnesses and victims of criminal offences that are in the territory of remote third States. This is the case of the victims of genocide, crimes against humanity or war crimes that do not have the possibility to report to the International Criminal Court or other competent authorities about the crimes committed in their territory. To enable them to report on such crimes and therefore ensure their access to Justice, Rule 122 of the Statute of the International Criminal Court states:

" *Lastly, a hearing by videoconference may also be convened for security reasons (e.g. suspected members of serious criminal organisations), in order to accelerate the investigation, or with the purposes of saving costs. The appropriateness of the use of videoconference in these cases must be examined carefully. In most of them, the convenience of accelerating the investigation or saving costs will not be reasons enough to justify the use of videoconference.* "

---

1 Recital (26) Dir on EIO. However, the Directive on EIO clearly states that "where that person is to be transferred to another Member State for the purposes of prosecution, including bringing that person before a court for the purpose of the standing trial, a European Arrest Warrant (EAW) should be issued in accordance with Council Framework Decision 2002/584/JHA".

2.4. Actors

2.4.1. Witnesses, victims and experts

The starting point of the European and international instruments mentioned in Section (2) is the situation wherein a judicial authority that is in a State´s territory needs to hear, as a witness or as an expert, a person who is in another State´s territory. When the appearance in person of the witness or the victim is not possible or not desirable, the judicial authority may request a hearing by videoconference instead[1].

Article 17 on the Rights of victims resident in another Member State of Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime, is noteworthy in this respect:

" *1. Member States shall ensure that their competent authorities can take appropriate measures to minimise the difficulties faced where the victim is a resident of a Member State other than that where the criminal offence was committed, particularly with regard to the organisation of the proceedings. For this purpose, the authorities of the Member State where the criminal offence was committed shall, in particular, be in a position:*

(a) to take a statement from the victim immediately after the complaint with regard to the criminal offence is made to the competent authority;

(b) to have recourse to the extent possible to the provisions on video conferencing and telephone conference calls laid down in the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 (1) for the purpose of hearing victims who are resident abroad."

Article 23(3) also requests to have certain measures available for victims with specific protection needs identified in accordance with Article 22(1) during court proceedings, such as:

(a) measures to avoid visual contact between victims and offenders including during the giving of evidence, by appropriate means including the use of communication technology;

(b) measures to ensure that the victim may be heard in the courtroom without being present, in particular through the use of appropriate communication technology;"

---

1 See Art. 9(1) of Second Protocol to 1959 Convention; Art. 10(1) of 2000 Convention.

Their appearance will not be "desirable", among other situations, where the witness is very young, very old or in bad health[1]. It will not be "possible", for instance, where the witness would be exposed to serious danger if appearing in the requesting State[2]. The rogatory letter should indicate the reason why it is not desirable or possible for the witness or the expert to appear in person before the court[3].

The hearing by videoconference of witnesses and victims is specially advisable where they are vulnerable and their appearance before the competent authority in another State´s territory may cause a second victimisation, as well as in cases of witnesses at risk of intimidation or in need of special protection, as evidenced by Rule 87 of the Rules of Procedure and Evidence in front of the International Criminal Court.

Some of the European and international Conventions on mutual legal assistance take special consideration of the situation of vulnerable victims and introduce specific rules to enable them to give testimony through videoconference[4].

On the other hand, the European and international legal instruments recognise the right of the witness not to testify in accordance with the law of either the requesting or requested State[5].

If however the witness has the obligation to testify and refuse it, or does not testify according to the truth, the law of the executing State should be applicable in the same way as if the hearing took place in a national procedure[6].

The hearing by videoconference may also be useful for persons in custody in a Member State whose personal appearance as a witness or for the purposes of confrontation is applied for by another Member State. In these situations, a hearing by videoconference may constitute an alternative and less intrusive measure than the temporary transfer of the person in custody to the territory of the requesting Member State.

---

1 Explanatory report to the Second Additional Protocol of 1959 Convention, parr. (74).
2 Explanatory report to the Second Additional Protocol of 1959 Convention, parr. (74).
3 Art. 9(3) Second Protocol of 1959 Convention; Art. 10(3) of 2000 Convention.
4 See also Art. 9(5)(b) in relation to Art. 23 Second Protocol of 1959 Convention.
5 Art. 9(5)(e) Second Protocol of 1959 Convention.
6 Art. 9(7) Second Protocol of 1959 Convention; Art. 10(8) of 2000 Convention.

Germany has submitted a declaration to Art. 10(1) of the 2000 Convention, according to which "*pursuant to the national law of the Federal Republic of Germany, no costs may be imposed or regulatory measures laid down against a witness or expert (Art. 10(1)) who fails to respond to an invitation to a hearing by videoconference to be conducted by a foreign judicial authority*".

As regards the experts, the provision of his opinion by videoconference may save time and expenses, without jeopardising the rights of the defence as soon as the suspected or accused person and his lawyers are given the opportunity to cross-examine the expert opinion in same hearing.

2.4.2. Suspected and accused persons. The assistance of a lawyer

In most of the European and international Conventions, including rules on hearing by videoconference of witnesses and experts, such rules may be extended to suspected or accused persons[1]. This extension is however subject to several limitations or conditions.

The first limitation is that the decision to extend the rules on hearing by videoconference to suspected and accused persons is at the discretion of the signatory States. The Second Additional Protocol to the 1959 Convention states that:

> "*Any Contracting State may, at any time, by means of a declaration addressed to the Secretary General of the Council of Europe, declare that it will not avail itself of the possibility provided in paragraph 8 above of also applying the provisions of this article to hearings by videoconference involving the accused person or the suspect*"[2].

A wide range of States signatory to this Protocol have declared that they will not allow the hearing of videoconference of suspected or accused persons. In particular, this declaration has been made by Croatia, Denmark, France, Malta and Poland. The Netherlands has declared that "*it wishes to avail itself of the possibility of excluding the use of hearings by videoconference involving suspects*". The United Kingdom has declared that "*it will not allow videoconferencing to be used where the witness in question is the accused person or the suspect*". The same declaration has been made by Norway and, among the third States signatories of this Protocol, by Chile.

---

1 See Art. 9(8) Second Protocol of 1959 Convention.

2 Art. 9(9) Second Protocol of 1959 Convention.

The 2000 Convention also enables the Member States to declare that they will not extend the rules on hearing by videoconference to suspects and accused persons[1]. This declaration has been made by Denmark, The Netherlands and the United Kingdom. France has declared that the hearing by videoconference is not possible in respect to "*accused persons when appearing before the trial court*". Germany has declared that the hearing of an accused person by videoconference is not excluded in principle, "*however, such hearings can be conducted only on a voluntary basis*". Hungary has stated that "*the hearing of an accused person may be conducted by videoconference only if consent is given in writing*". Article 6 of the aforementioned Convenio Iberoamericano sobre el uso de la videoconferencia en la Cooperación Internacional entre Sistemas de Justicia, Mar de Plata 3.12.2010, regulates that for defendants is possible to apply the general rules on the development of videoconferencing, but is necessary to take account the national law of each party and all rights must be respected. A Party may declare that will not apply the agreement in this part

The second limitation is that the hearing by videoconference of suspected and accused persons is possible "*where appropriate and with the agreement of their competent judicial authorities*".

The third important condition is that the suspected or accused person must give his consent. In words of Art. 10(9) last paragraph of 2000 Convention,

> "*Hearings shall only be carried out with the consent of the accused person*".

The use of videoconference is intended to ensure that the suspected or accused person who is in another State´s territory may be informed of his rights and the charges against him, being subject to certain questions by the prosecutor or the court, or have the possibility to exercise his right to defence during an investigation or a trial.

---

1 Art. 10(9), second paragraph.

The right to defence of suspects and accused persons requires, in most of cases, the assistance of a lawyer. With this assistance, the possible scenarios for a hearing by videoconference might be as follows:

(a) the requesting judicial authority is located in a Member State, whilst the requested judicial authority, the suspected or accused person and his lawyer are in another Member State;
(b) the requesting judicial authority and the suspected or accused person are located in a Member State, whilst the requested judicial authority and the lawyer are located in another Member State. The CCBE wonders whether this covers scenarios where the victim to be heard by videoconferencing is in location B, but the detained person is in location A – in which case it would be important to differentiate between cases where the lawyer is defending the rights of the victim or the witness who is in location B, or where there is a lawyer in location B, but he/she is there to protect the interests of the accused/suspect person who is in location A. ;
(c) the requesting judicial authority and the lawyer are located in a Member State, whilst the requested judicial authority and the suspected or accused person are in another Member State.
(d) An additional scenario, where the suspected/accused person is having a lawyer each in two places at the same time (both where the judges are and where the client is located) is identified by the CCBE.

Each scenario presents its own complexity. Scenario (a) seems to be the most protective of the rights of the defence, as it ensures direct communication between the lawyer and its client. Scenarios (b) and (c) would be also compatible with the rights to defence as soon as a direct line of communication (e.g. by phone, by a parallel videoconference system) is at the disposal of the lawyer and his client.

Lastly, the scenarios described above may become more complex when an interpreter is also necessary. The matter is analysed in the next section.

There is a fairly widespread international recognition of the right of the defendant to be present at all critical stages of their criminal proceedings. Nevertheless, there are important State to State variations depending on the legal system type, the seriousness of the offence and on how critical a certain stage the proceedings is deemed.

Most importantly for the purpose of this paper, there is ground for interpretation about what being present really means. As technology allows an increasingly blurred distinction between physical and virtual presence, the right to be present is to be reconsidered. Then again, this reinterpretation differs from one system to another, therefore affecting judicial international cooperation.

2.4.3. Interpreters

A hearing by videoconference may become quite complex when interpretation services are needed. The Second Additional Protocol of the 1959 Convention and the 2000 Convention refers to the assistance of an interpreter in two different occasions. First, they mention that the judicial authority of the requested Member State shall be present during the hearing "*where necessary assisted by an interpreter*". The possibility to provide interpretation services in situations other than the hearings of suspects and accused persons must therefore be taken into consideration. Such interpretation services might be quite frequent in cross-border cases, as in many of them the judicial authorities involved will speak different languages.

The second occasion refers to the interpretation services provided to the suspect or accused persons: "*at the request of the requesting Member State of the person to be heard the requested Member State shall ensure that the person to be heard is assisted by an interpreter, if necessary*"[1]. In this situation, *Directive 2010/64/EU of 20 October 2010 on the right to interpretation and translation in criminal proceedings*[2] applies.

As anticipated in Section 4.2 of this Report, with the assistance of a lawyer and an interpreter the scenarios of the hearing by videoconference become quite complex:

(a) the requesting judicial authority is located in a Member State, whilst the requested judicial authority, the suspected or accused person, his lawyer and the interpreter are in another Member State;
(b) the requesting judicial authority and the interpreter is located in a Member State, whilst the requested judicial authority, the suspected or accused person and his lawyer is located in another Member State;
(c) the requesting judicial authority, the suspected or accused person and the translator are located in a Member State, whilst the requested judicial authority and the lawyer are located in another Member State;

---

1 Art. 10(5)(d) 2000 Convention.
2 OJ L 280, 26.10.2010, p. 1.

(d) the requesting judicial authority and the suspected and accused person are located in a Member State, whilst the requested judicial authority, the lawyer and the interpreter are located in another Member State;
(e) the requesting judicial authority, the lawyer and the translator are located in a Member State, whilst the requested judicial authority and the suspected or accused person are in another Member State.
(f) Regardless the location of the suspect and his lawyer, the judicial authorities involved in the hearing may decide to make use of remote interpretation.

2.4.4. Direct contacts and negotiation of arrangements between the issuing and the executing Member State

The principle of mutual recognition in criminal matters enables the judicial authorities of the issuing and executing Member State to establish direct contacts in order to clarify any European order or request for execution. In complex cases, the use of videoconference may facilitate the discussions between the competent authorities.

2.4.5. The assistance and support of the European Judicial Network and Eurojust

Eurojust is the EU body created in 2002 and reinforced in 2009 in order to support and assist the judicial authorities of the Member States (prosecutors, investigation judges) during investigations, prosecutions, trials and further steps of criminal proceedings against serious cross-border crime.

Eurojust facilitates the exchange of information between the judicial authorities concerned, accelerates the issuing, transmission and execution of the letters of request, and ensures coordination of ongoing investigations and prosecutions between several Member States.

Both Eurojust and the European Judicial Network (EJN) may develop a relevant role in the identification of the legal instrument applicable for the organisation of a particular videoconference. When the use of videoconference is requested to collect suspected and accused persons´ testimonies, Eurojust carefully analyses the legal systems of the requesting and requested Member State in order to ensure compatibility between the procedural rights and guarantees at stake.

As mentioned in a previous section, Eurojust and EJN may also assist the judicial authorities of the Member States in the issuing, transmission and execution of letters of request for a hearing by videoconference.

The assistance of Eurojust in the transmissions of rogatory letters issued in accordance with the 1959 Convention and its Protocols has been expressly recognised by France in a declaration contained in the instrument of ratification of the Second Protocol. In particular, France declared that

> "*Requests for mutual assistance requiring coordinated enforcement in several member States of the European Union may also, where requests addressed to France are concerned, be forwarded through the intermediary of the French national member of the Eurojust judicial cooperation unit*".

Eurojust also uses videoconference facilities for the adequate development of its tasks. In particular, Eurojust promotes the use of videoconference:

- As a relevant tool for the preparation of a coordination meeting. By using videoconferencing facilities, each National desk has the possibility to discuss with home authorities the details of the case and the best manner to present it during a coordination meeting;
- As an alternative to coordination meetings, where they do not seem to be feasible (e.g. difficulties to find an appropriate date for all the authorities involved) or cost-efficient;
- As a complementary tool to coordination meetings, where the judicial authorities of one of more Member States concerned are not able to attend it;
- As a follow-up to a coordination meeting, in order to monitor the execution of the rogatory letters and other requests for judicial cooperation and assist in case of difficulties
- Eurojust has also made use of videoconferencing facilitates during some coordination centres, thus enabling the monitoring in real time of the execution of letters of requests and EAWs, and the overcoming of obstacles raised during the action day(s).

Lastly, Eurojust makes use of videoconferencing facilities as an alternative to the physical attendance of non-operational meetings (for instance, preparatory meetings of the JHA Agencies´ network).

As result of the experience gained by Eurojust in the past years, the most relevant difficulties related to the use of videoconference in cross-border cases are as follows:

There is a certain reluctance of the judicial authorities to make use of videoconferencing facilities in cross-border cases involving serious crime, mainly due to

(1) difficulties in the identification of the requested competent authority;
(2) legal requirements derived from the existence of different procedural rules and guarantees applicable in the requesting and the requested Member State;
(3) lengthy execution of rogatory letters;
(4) different languages at stake and therefore need for interpretation, and
(5) special complexity of videoconferencing requests for taking suspects and accused person´s testimony (in some Member States it is simply not possible).

2.5. Issuing, transmission and execution of rogatory letters requesting a hearing by videoconference

In general terms the issuing, transmission and execution of rogatory letters requesting a hearing by videoconference is as follows:

2.5.1. Issuing

The rogatory letter is issued by the judicial authority of the State´s territory wherein the witness, expert or accused person has to be heard, in accordance with the general rules of mutual legal assistance laid down in the Convention applicable. Either such Convention or a separate/complementary legal instrument usually contains specific rules to be observed for the hearings by videoconference.

For instance, the signatory Parties of the 1959 Convention will issue rogatory letters in accordance with Art. 14 of such Convention and Art. 9(3) of 2001 Second Additional Protocol. According to the latter, the requests will contain:

> *"The reason why it is no desirable or possible for the witness or expert to attend in person, the name of the judicial authority and of the persons who will be conducting the hearing".*

2.5.2. Transmission

The letter of request may be transmitted directly between the judicial authorities of the requesting and requested Member States. EJN and Eurojust can assist them in speeding up the transmission and, if not known, in the identification of the competent judicial authority of the requested Member State.

2.5.3. Execution

2.5.3.1. Summoning of the person concerned

The judicial authority of the requested Member State is responsible for summoning the witness,

expert or suspected person who will be heard by videoconference, in accordance with the rules and formalities of his Member State. In the case of suspected persons, the service of a summon might inform him of his right to give or not his consent to the hearing by videoconference.

2.5.3.2. The hearing

The hearing is conducted directly by the issuing judicial authority in accordance with the rules and formalities of his Member State.

A judicial authority of the requested Member State must be present during the hearing. He/she is responsible for:

- Ensuring the identification of the person to be heard;
- Guaranteeing the respect of the fundamental rights and principles of the law of the requested State. If, in his/her view, such fundamental rights and principles are being infringed, the judicial authority of the requested Member State must immediately take the necessary measures to ensure that the hearing continues in accordance with the said principles and rights.
- Taking the minutes of the hearing[1].

In addition to these guarantees, both judicial authorities must ensure that the suspected or accused person has given his consent to the hearing by videoconference.

As mentioned, an interpreter may by present in order assist the judicial authorities involved in the hearing, the witness or victim, the expert, and/or the suspected or accused person.

2.5.4. Relevant changes introduced by the Directive on EIO

The Directive on EIO will introduce some relevant changes in the hearings by videoconference.

Firstly, the rogatory letters will be replaced by a new document, the European Investigation Order, in the form set out in Annex to Directive 2014/41/EU. The EIO contains a general part and some specific sections related to specific investigative measures, including hearings by videoconference.

[1] On this particular point see "Section 2.8. Documentation" of this Report.

The EIO is inspired by the principle of mutual recognition in criminal matters. In accordance with this principle, a European Investigation Order issued for the purposes of a hearing by videoconference must be executed by the judicial authority of the Member State where the witness, the expert, or the accused or suspected person is, "*without any further formality being required, and ensure its execution in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing State*"[1].

Among the conditions to be taken into consideration, the issuing judicial authority must assess whether the EIO is necessary and proportionate for the purpose of the proceedings, taking into account the rights of the suspects and accused person[2]. The principles and rights analysed in section (3) of this report must therefore analysed carefully before issuing a EIO for the purposes of a hearing by videoconference.

The Directive on EIO expressly refers to the possibility of transmitting EIOs "*via the telecommunications system of the European Judicial Network (EJN) set up by Council Joint Action 98/428/JHA*".

The Directive on EIO enables the executing judicial authority to resort to a different type of investigative measure "*where the investigative measure selected by the executing authority would achieve the same result by less intrusive means that the investigative measure indicated in the EIO*"[3]. The recourse to a different type of investigative measure might lead the executing judicial authority to convene a hearing by videoconference in cases when the temporary transfer, or the arrest and further surrender of the suspect has been requested.

---

1 Art. 9(1) Directive on EIO.
2 Art. 6(1)(a) Directive on EIO.
3 Art. 10(3) Directive on EIO.

As mentioned, the principle of mutual recognition entails that the executing judicial authority must execute the EIO in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing State, "*unless that authority decides to invoke one of the grounds for non-recognition or non-execution or one of the grounds for postponement provided for in this Directive*". In addition to the general grounds for non-recognition or non-execution, the Directive on EIO has introduced two particular grounds for refusal. Firstly, the EIO may not be executed if "*the suspected or accused person does not consent*". Secondly, if "*the execution of such an investigative measure in a particular case would be contrary to the fundamental principles of the law of the executing State*".

2.6. The use of videoconference at the different stages of a criminal procedure

A hearing by videoconference may be held in different steps of a criminal procedure, including the pre-trial stage, the trial stage, the execution of convictions, and the resolution of appeals. In this respect the rules of procedure at the ICC (International Criminal Court) provide for a person who is unable, due to a disability or illiteracy, to make a written request, application, observation or other communication to the Court, to make such request, application, observation or communication in audio, video or other electronic form.

In the pre-trial stage, the use of videoconference may ensure that the arrested person is informed about his rights and about his charges at the earliest possibility. In some Member States (the Netherlands, for instance), the prosecutor is normally at one police station and communicates with the defendant in custody in another police station. In this perspective videoconference might be used as an effective bridge between different procedural systems, granting the presence of the Investigating Judge when the requested State is unable to fit this into a system where Judges only intervene at the trial stage.

In cases where the language spoken by the arrested person is not well known or there is no interpreter available at short notice, the use of remote interpretation might ensure the prompt assistance of an interpreter and therefore the respect of the fundamental rights of the suspect[1].

---

1 See Recital (25) and Art. 3(2) of Directive 2012/13/EU (the right to information in criminal proceedings), in relation to Directive 2010/64/EU (the right to interpretation and translation in criminal proceedings).

The collection of witness' testimonies and the gathering of experts' testimonies may also take place at pre-trial stage.

The hearing of suspects and accused persons in the course of trials is especially controversial. As mentioned in Section (2) of this Report, some Parties to the Second Additional Protocol of 1959 Convention expressly excluded this possibility, and some EU Member States that ratified the 2000 Convention also made a reservation excluding the hearing by videoconference of suspects and accused persons.

During the execution of convictions, the hearings with the penitentiary centres may facilitate the communication between the convicted person and the court who is supervising the execution of their convictions. For some, videoconferencing could also be viewed as an alternative to in absentia trials, as evidenced by the rules of the ICC.

2.7. Additional use of videoconferencing - Using videoconferencing at hearings of children in criminal proceedings

A wide range of documents recommend the use of modern technologies in judicial proceedings where children are involved. The main objective which is to follow in this type of proceedings is **the best interest of a child (e.g. item 2 of paragraph b. of Article 6 of the European Convention on the Exercise of Children's Rights of 1996 and Article 40, paragraph 2, subparagraph (b), item (iii) of the United Nations Convention on the Rights of the Child of 1989)**.

The main legal instruments that specifically mention the use of technologies with respect to children are the **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention)** states especially in its Articles 35 and 36 that an interview with a child victim should be commenced with the use of modern technologies and recorded so the records could be used later in the proceeding if necessary due to avoiding the secondary victimization of a child. The same main propose is followed by the **Council of Europe Guidelines on Child Friendly Justice** adopted by the Committee of Ministers of the Council of Europe on 17 November 2010 the interviews with children, victims of crime, should be recorded and the children should be interviewed in a child friendly environment.

The "**Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA**" also promotes the use of videoconferencing in cases where the confrontation of a victim and/or his/her family with the perpetrator should be avoided or where they are in a different Member State.

A number of Member States uses modern technologies at interviews with children. In the Republic of Slovenia these provisions and recommendations were systematically implemented in 2010 with the implementation of videoconferencing systems at the courts. As the videoconferencing system can be widely used and the videoconferences can be recorded, they used the system for interviewing children. The child (it can also be used for other victims of e.g. domestic violence who do not want to confront their perpetrator) would normally be interviewed at a location of the Social Care Centers where he/she is staying in a child friendly room. There is the facility for a video connection to be established between the court and this room, whereby the court hears and sees everything from the child friendly room and in the child friendly room there are no screens or loudspeakers, just two cameras and a microphone. The court has the possibility during the interview to send additional questions to the expert commencing the interview. The interview is recorded, the suspected or the accused has its right to question the victim respected and there is a greater possibility that the secondary victimization of this child is avoided or prevented.

There is also a possibility in a pre-trial proceeding for Police to use the child friendly room with all of its videoconferencing equipment for commencing an interview with a child victim. Near the child friendly room there is another room in the same social care center equipped similarly as the court room with loudspeakers, screens and handheld communication devices. The Police can also order a recording of the interview with the objective to avoid the secondary victimization of the children in a way that the prosecutors use the recording in a following court proceeding.

2.8. Documentation

2.8.1. Documentation in accordance with European and international legal instruments

As a general rule[1], the judicial authority of the requested Member State is responsible for drawing up the minutes of the hearing by videoconference.

The minutes must indicate the date and place of the hearing, the identity of the person heard, the identities and functions of all other individuals participating in the videoconference, any oaths taken, and a description of the technical conditions under which the videoconference took place[2].

2.8.2. Documentation in accordance with national legal systems

When completed, the requested judicial authority must forward the minutes of the hearing by videoconference to the requesting Member State, for their insertion in the judicial file. In principle, this insertion will not be controversial, as the requesting judicial authority conducted directly the hearing "in accordance with its own laws"[3].

2.9. Conclusions and recommendations

Videoconferencing offers a convenient option to ensure the hearing of witnesses, experts and accused persons without the need to compel them to travel to the state where the investigation or the trial is being conducted. It has gained legal recognition through international conventions and more recently European Union law, with the European Investigation Order Directive.

While bringing added protection to witnesses and vulnerable persons, the use of videoconferencing also has the potential to be detrimental to defence's rights and as such contradictory to the overarching principles of European law. Special care must therefore be taken to ensure the principles of immediacy, equality of arms and contradiction are respected. This entails using equipment that is up-to-date and secure in proportion with the sensitivity of the case.

---

1 See Art. 9(6) Second Additional Protocol of 1959 Convention; Art. 10(6) 2000 Convention.
2 See for instance Art. 10(6) MLA Convention of 2000.
3 See for instance Art. 10(5)(c) MLA Convention 2000.

In order to guarantee defence's rights, a number of Member States have indicated they will not allow videoconferencing when the person heard is accused or suspected in the context of conventions. European Union law is however introducing videoconferencing for a suspected or accused person through the European Investigation Order Directive. The impact of this legislative evolution on the different procedural rules and guarantees applicable in the requesting and executing Member States will therefore have to be assessed. Other legal issues related to videoconferencing also include the identification of competent authorities.

The following further actions are therefore proposed:

- Assess the impact of the EIO in relation to current procedural rules;
- In line with the previous point, devise tools to help judicial authorities to identify the legal instrument applicable for the organisation of a particular videoconference;
- Devise tools to help judicial authorities to identify the competent authority for the organisation of a given videoconference;
- Ensure legal support for the proposed practical results of the working group, in line with the overarching principles of European law (contradictory principle, immediacy, equality of arms, proportionality) – see next section.
- Identify the arrangements that should be made to guarantee procedural safeguards in the exercise of the rights of the defence.

2.10. French experience on operational and technical aspects with videoconferencing

2.10.1. General Remarks

One needs to make a clear distinction between legal problems that occur only with digitisation and those that would occur under any circumstance. For instance, often the only protection that will be afforded to testifying witnesses is that granted by the rule of law.

Therefore, this section aims to shed some light on legal challenges linked to the implementation of electronic procedures.

A first requirement is of course that national law allow videoconferencing. In France for instance, videoconferencing is allowed for a number of criminal and administrative procedures, allowing for instance a videoconference between the police and a court. Its use for civil law procedures is much more restricted, as it needs to take place in a suitably equipped court, implying for instance that the testifying expert needs to travel to a court anyway. It can however be noted that currently negotiated European instruments may make videoconferencing possible for specific procedures.

The experience of large-scale digitisation projects in Europe points to two main axes that must be explored when implementing transnational electronic procedures and could also be applied to videoconferencing:

- The verification of the users' roles and identities,
- The security of the exchange to guarantee data integrity and the protection of transmitted data.

2.10.2. The verification of the users' roles and identities

In the context of videoconferencing, this entails making sure the person you are talking to is really the person you want to talk to. Of course, there are organisational procedures in place to ensure that users will recognise communications when they emanate from legitimate correspondents, but in the most sensitive cases it might be worth securing the booking of a videoconference with the help of an electronic signature (using at least the advanced level).

2.10.3. The security of the exchange to guarantee data integrity and the protection of transmitted data

As sensitive data may be exchanged via videoconferencing, it makes sense to ensure that it is secure. To this end, the community has already developed secure networks such as sTESTA.
The security of data is essential to abide by the key principles of data protection, one of which is also the idea of proportionality: the measures put in place must be proportional to the sensitivity of the data that is being handled. For instance, extra care should be applied when dealing with suspected persons (as opposed to sentenced persons). Consideration should therefore also be given to the data that is handled through booking forms, how it is handled and stored.

2.10.4. Suggested short-time actions

- Agree between participants on usages that could be promoted (e.g. specific instruments such as taking of evidence, or types of cases) through questionnaires
- Assess the security needs of these suggested usages while in parallel assessing current security measures
- Suggest potential improvements though e.g. implementation of Secure Trans European Services for Telematics between Administrations (sTESTA).

2.11. CCBE position regarding the use of videoconferencing in cross-border criminal proceedings

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 32 member countries and 13 further associate and observer countries, and through them more than 1 million European lawyers. With regard to the work that has been undertaken by the Informal Working Group (IWG) on Cross-border Videoconferencing set up within the Council Working Party on e-Law (e-Justice), the CCBE is very grateful for the fact that it has been invited to attend the meetings of the IWG as well as the possibility it has been given to provide feedback to the reports developed within this context.

The CCBE understands that the use of videoconferencing systems provides a number of advantages. However, there are potential risks and drawbacks that must be considered before there is a headlong rush to adopt videoconferencing in cross-border criminal procedures. In particular, its use should not undermine fundamental principles of a fair trial especially with respect to defence rights. The CCBE's main concerns are as follows:

- If there is a trend towards using videoconferencing for cost reasons, this could eventually result in it being the main or only form of access to a suspect held in custody in cross-border cases. The CCBE does not consider this acceptable and stresses that cost savings should never be at the expense of defence rights which in most cases can be better guaranteed in physical hearings. Therefore, the use of videoconferencing should remain the exception to the main hearing of the case on its merits.
- The CCBE considers that the use of videoconferencing must always be subject to the suspected or accused person´s consent. Care must be taken that the suspect or accused person is able to seek legal advice prior to consenting to the use of videoconferencing. Also, legal remedies should be readily available to challenge a decision on using videoconferencing.
- Experience shows that in case videoconferencing is used in prison, the suspected or accused person must be assisted by a lawyer in order to ensure that no intimidation takes place off screen.
- Some practitioners may be reluctant to rely on the confidentiality of communication with clients through video conferencing because of interception or surveillance risks. It is very important that, if there is videoconferencing, the necessary safeguards to protect confidentiality can be assured. Any breach of confidentiality, be it by a third party or agency, should be a criminal offence, and such information should not be able to be relied upon in the proceedings. The necessary safeguards across all the Member States which use videoconferencing should therefore be harmonised.

- It is essential that clients have ready access in person to their lawyers to build up the relationship of trust and confidence. This will be more difficult in cross-border cases using videoconferencing, also due to the frequent need for interpreters.
- The accused or suspected person has a right to ask for the personal appearance of a material witness in order to exercise his right under Article 6(3) (d) ECHR. Alternatively, the examination of the witness by the accused person and his/her counsel shall take place face to face in his/her (the witness') residence where the witness is prevented to appear in person before the court.
- In cross-border criminal cases, particularly where the defendant might not be a native speaker and will be subject to different cultural influences, it might be difficult for the judge to examine the nuances of the defendant's appearance and responses through a video-link.. Therefore, it is important that the EU develops mandatory minimum standards as to the technical arrangements that should be in place for the use of videoconferencing. Such technical arrangements should ensure as much as possible a true-to-life hearing experience including full communication/interaction of all the parties to the procedure with the examined person.
- In jurisdictions where the principle of immediacy is a cornerstone of the criminal procedural law, this will constitute one of the greatest hindrances for the use of videoconferencing; e.g. in Austria, the Higher Regional Court of Vienna recently issued a verdict which clearly forbids the use of videoconferencing in criminal trials. On the other hand, the use of videoconferencing could be more appropriate where there is no taking of evidence, and there can be a lawyer present at the site where the suspected or accused person is.
- In cases where documents have to be shown to the witness, that should be done via an independent person present with them (court clerk or similar) who can ensure (e.g. from the point of view of the prosecution) that they are looking at the right page and (from the defence point of view) also ensure they are not looking at other documents, particularly documents that have not been disclosed to the defence.
- The CCBE also encourages the EU to provide for sufficient training opportunities for both competent government authorities as well as legal practitioners in order to become acquainted with the use of videoconferencing technologies for cross-border criminal cases.

3. REPORT OF THE ORGANISATIONAL SUB-GROUP

3.1. Findings: Key problem areas identified

Evaluation of the VC questionnaires displayed clearly that the **majority of problems/issues** with cross-border videoconferencing fall into the **organisational** or **technical** category.

The completed questionnaires also contained a number of suggestions for best practices, solutions and actions for improvement which will help in addressing these problems.

3.2. Statistics on videoconferencing Questionnaires

The following table shows the number entries from all completed questionnaires per topic and category:

Table 1: Statistics on VC Questionnaires

Number of entries	Category					
Topic	Legal	Organisational	Psychological	Technical	Other	Total Number
Action recommended	3	12	2	10	3	30
Best practice recommended	2	12	4	9	3	30
Issue or problem	5	43	6	29	4	87
Other			1		2	3
Project suggested		5	2	3		10
Solution recommended	3	22	4	12	1	42
Synergy with other project		1		2		3
Useful material or document	2	14		1	3	20
Total Number	15	109	19	66	16	225

The detailed questionnaire results can be found in the appendices of this report.

Note: the combined results from the questionnaires in the form of a combined spreadsheet and as PDF-reports were already distributed to the participants and all Member States via the General Secretariat of the Council.

3.3. Typical organisational problems identified

- **VC contact person** of the competent court in other MS cannot be found
    - **Missing or outdated** VC contact information in e-Justice Portal Member States pages on videoconferencing, e.g. just general switch board number of court provided
    - **Unable to find the competent court** in the other MS, e.g. Court ATLAS data outdated

- **Language problem** with VC contact person
    - Translation, interpretation, or common language needed for organizing a VC

- **Duration (months!) and bureaucracy of the formal process** for mutual assistance to get permission for VC

- **Different time-zones** can cause troubles with wrong start-times

- **Exchange of technical VC parameters: via Contact-List and/or in Booking-Form**
    - Some are public and can be displayed in the e-Justice Portal MS pages on VC, e.g.:
        - Telephone-number of contact-point / contact-person
        - Type of connection - IP or ISDN
        - Room-number of the VC room
        - ISDN-number (in case of ISDN connection only)
    - Some are confidential and should be only be exchanged in a secure way using a "Booking form", e.g.:
        - Passwords for outside access via gateways or for accessing a "virtual room"
        - IP-address to be called (in case of IP connection only)
        - IP-address of the calling partner (in case of IP connection only)

- **Training of VC users** (e.g. judges, prosecutors) needed
    - Capabilities of local VC system should be known to users! Sometimes judges decline cross-border requests for using VC, because they don't know that their courts have VC equipment installed or don't know how to use it.

- **Step by step description ("Protocol") needed** for preparing, testing, starting and running the VC, e.g.:
    - who will start the VC, who will wait for an incoming call
    - how are witnesses identified,
    - handling of incidents, technical problems

- **Technical support for incidents during testing / starting / running a VC**

3.4. Specific short-time actions suggested

The Organisational sub-group identified several action for improving the current situation.

3.4.1. Organisational Action 1 – MS's overall position with videoconferencing

- **Action Org-1:** The e-Justice Portal VC MS pages on "national facilities" shall be improved by adding a "**Brief summary of the Member State's overall position with videoconferencing in the justice system"** (Idea from Scotland, promoted by Sweden), consisting of 2 sub-chapters:
    - **General description of the videoconferencing infrastructure** (mandatory)
    - **Description of the Member States videoconference organisation** (optional)
- **Example from Sweden:**
    - In total there are 373 video conferencing systems in court rooms and in small meeting rooms at the courts. At the prosecution authority there are 40 video conferencing systems, one at each office. The prison and probation service has 110 videoconference system.
    - SNCA (Swedish National Courts Administration) is an administrative organisation within the Swedish Courts System. The Swedish Courts are separate from the police, the prosecution authority, prison and probation service. SNCA has a central role in videoconferencing. SNCA installs, maintains and supports the videoconference infrastructure and videoconference end-points within the Swedish Courts System.
- **Outcome of discussion**:
    - The general description of the Member State's VC infrastructure is considered more important
    - The description of the Member State's VC organisation should be optional

3.4.2. Organisational Action 2 – Information on videoconferencing contact point / contact person/s

- **Action Org-2: Improve information on VC Contact point / contact person.**

  Optimal solution seems to be **a single contact point per MS**, which could help finding the right court (or other authority) and **in addition a contact point per court or other authority** (e.g. prosecution, prison, police, community-centre) **with VC-facilities.** It is noted that there may need to be different criminal and civil contact points in some Member States

  Note: The EJN-Website (see: http://www.ejn-crimjust.europa.eu or https://e-justice.europa.eu/content_ejn_in_civil_and_commercial_matters-21-en.do) contains a list of contact points EJN mutual legal assistance. The access is restricted to registered users.

  - **Establishment of a national contact point** at each MS for all incoming requests for cross-border VC is highly recommended
    - **With language skills, helps to find the competent judicial authority** and then forwards the valid request to the competent court or authority
    - **Note: This is already done by some MS**, e.g.: EE, IE (cross-border VC in criminal), UK (cross-border VC-requests in criminal cases)
    - **To be decided is: Who shall do this?** The same "Central authority", which is required by "direct taking of evidence" for civil? Or using the Eurojust or EJN contact point?
  - In addition a **contact point at each court** (judicial authority) is required
    - As most other MS do currently
  - Further details are to be decided:
    - **Recommended means of communication?**
      - Functional mailbox? Note: Only 13 Member States allow e-mail!
      - Fax? Letter? Telephone? Special tools?
    - **Use of English as common language?**

- **How the information on contact points is to be published on the e-Justice Portal:** PDF-File per Member State or additional fields in European Court Database?

- **Note on the situation in the Netherlands:**

  - In general, non EU-countries can send their requests to our Ministry of Security and Justice (central authority). When a non EU-country is party to the 'Second Additional Protocol to the 1959 Convention, dated 8 November 2001, on Mutual Legal Assistance in Criminal Matters', requests may be sent directly to the relevant Dutch judicial authorities. EU-countries and Schengen countries may send their requests directly to the competent Dutch judicial authorities.
  - The Netherlands has established a network of coordination centres (in short: IRC's) to ensure the quick handling of foreign requests. An 'IRC' is a cooperation structure between the police unit and the prosecution service of a particular region. It coordinates the execution of your request.
  - As explained above, you may send your request straight to the 'IRC' of the relevant region, that is competent for the execution of your request.
  - For example, if your request for interrogation of a suspect needs to be executed in Amsterdam: you may send the request to 'IRC Amsterdam'.
  - If you are uncertain which IRC is competent, the request can be sent to the 'LIRC' (SPOC).
  - If the foreign authority's request for VC is assessed suitable, then the actual VC connection will be established by the central service of the IT back office.
  - Both the Police and the Judiciary have a central authority for VC.
  - In urgent cases, INTERPOL services are also available.

3.4.3. Organisational Action 3 - Language

- Issue: **Language problem** with VC contact person

  - **VC contact person is unable to understand me**

  - Translation, interpretation, or technical skills in a common language are already needed for organizing a VC

- **Action Org-3:** A central national VC contact-point is recommended for each MS, and will probably understand English to help the requester to determine the right "assisting court" for doing the cross-border VC. But for communication with the local contact point at the "assisting court" most participants suggested the use of a multi-language booking-form for requesting/confirming a VC.

- Further details need to be clarified/decided:
    - Always use English for cross-border contacts or use of national contact point with language skills (who could also help finding the competent court / judicial authority)?
    - Translator / Interpreter must already be foreseen for organizing the VC?
    - "Multi-lingual Booking-Form" vs. "English Booking-Form" for requesting and confirming a VC

3.4.4. Organisational Action 4 – Formal process for mutual assistance

- Issue: Duration (Months!) and bureaucracy of the formal process for mutual assistance to get permission for VC
- **Action Org-4.1:** Recommendation: The legal framework for cross-border mutual legal assistance should be simplified for the requestor by always using a central VC-contact-point in the requested Member State country, who guides the requester to the most suitable "assisting court". In addition the new process should follow the simpler and more effective process model of "direct taking of evidence" (which also means less work for the "assisting court" / former "requested court")

3.4.5. Organisational Action 5 – Time-zones

- Issue: **Different time-zones** can cause troubles with wrong start-times
- **Action Org-A5:** Any Booking-Form must include time-zone information for start date and time!
- Outcome of discussion: This is considered to be a minor issue within Europe, but a major issue, if you do a VC with the far east or Latin America.

3.4.6. Organisational Action 6 – Exchange of technical videoconferencing parameters

- Issue: Exchange of technical VC parameters: via public Contact-List and/or in Booking-Form?
    - Some public: e.g. IP or ISDN (at e-Justice Portal Member States pages on VC), Room-number, ISDN-number
    - Some confidential: e.g. passwords for outside access via gateways; IP-address
- **Action Org-A6**: **Public static** VC parameters shall be published in **Contact-List** of each MS, other **variable or confidential** details shall be requested and confirmed with the **Booking-Form.**
    - Clarification required which concrete parameters are public and static (e.g. to avoid all hackers of the world are sitting on your IP ports for VC!)
- Outcome of discussion:

- To be clarified, which parameters are static and public and should therefore be in the public contact list in the MS pages on videoconference information on the e-Justice portal.
- As a general principle UK suggested, that also the booking form should contain only the high level request with the really needed parameters and that more detailed parameters should be "delegated", e.g. to the other end-point, who fills in details as the IP-address and suffix for his own VC-endpoint. For rarely used parameters there should be no fixed field on the booking-form, but just an optional field for further parameters, which could be required under special circumstances.

3.4.7. Organisational Action 7 – Training of videoconferencing users

- Issue: **Training of VC users** (e.g. judges, prosecutors) needed
  - Capabilities of local VC system should be known to all users!
- **Action Org-A7:** Establish a new "**European Network on Videoconferencing in the Judiciary**" for exchange of experience and sharing best practices on VC, including training!

- Outcome of discussion:
  - **Establishing a new network has challenges as it must have a legal personality.**
    - **==> This issue must be delegated back to the "Working Party e-Law (e-Justice)" because only a Council decision could create the necessary legal personality for such a network**
  - But training of the intended VC users is extremely important.
  - UK wants to raise their user's experience with VC. In addition UK also wants to connect external users such as their "defence agents", who will require some VC-training / VC-experience to incentivise them to use VC.
  - For lawyers the confidentiality of the communication of the lawyer with her/his client is a major issue.
  - The UK has the general principle not to exclude lawyers/defence-agents in order to realize the vision of a fully digital court with a virtual court-room.
    - They found solutions to enable the confidentiality of the lawyer/client communication:
      - Separate rooms for individual confidential conversations
      - Switch-off the microphone, so that other users can watch you without hearing the communication between lawyer/client
  - In the Dutch situation is plotting a microphone while non-verbal communication remains visible not acceptable.

- Prior to the first interrogation by the police, the suspect has the right, even in minor offenses, to consult with his counsel (Saldusz judgment). The suspect who wants to consult a legal counsellor prior to the interview is provided a tablet with a secure Jabber account. In a closed room he takes on contact through the tablet with the duty solicitor/ Lawyer .
- The Lawyer who is also in possession of a tablet can remotely serve his client with advice. This may result in his presence during the hearing. If so, the parties will have to wait for his arrival.
- The Netherlands is in the process of implementing this nation wide.

3.4.8. Organisational Action 8 – Step-by-step protocol for videoconferencing

- **Issue: Step by step description ("Protocol") is needed** (for the judge, prosecutor, other VC user) for preparing, testing, starting and running the VC, e.g.:
- who will start the VC, who will wait for an incoming call, how are witnesses identified, handling of incidents.
- Note: e-Justice Portal videoconferencing pages **"Manual"** (see: https://e-justice.europa.eu/content_manual-71-en.do) already includes a useful step by step description of the overall process in
  - "**6. ANNEX III - KEY STEPS FOR USING VIDEOCONFERENCING IN CROSS-BORDER PROCEEDINGS**" (see: https://e-justice.europa.eu/content_manual-71--maximize-en.do?idSubpage=19)
- **Action Org-A8: This "Annex III" needs to be further enhanced with additional detailed steps: testing, starting, what is to be done within the videoconference, and customized for specific judicial procedures**
- **Outcome of discussion:**
  - UK sees the "protocol" as a list of instructions of who does what and when for running through the steps of a judicial procedure using a videoconference.
  - UK wants to establish a standard "protocol" (or adapt the existing protocol) for the VC-situation by working through a series of test-cases, which simulate the running of a real court procedure under VC-conditions.
  - NL notes, that there is also an English version of the description of a "true-to-live" VC, which should be consulted as well.

3.4.9. Organisational Action 9 – Technical support

- Issue: **Technical support for incidents** during testing / starting / running a VC
- **Action Org-A9: Build a national technical support for VC in your Member State.** (E.g. by applying learning from experiences from Sweden and UK Scotland and other MS)
- Outcome of the discussion:
    - SE has centralized national support and uses the "train the trainers" concept.
    - UK has outsourced the technical support to a separate organisation.
    - SI has a national support. Judges can call and a single person has remote access to all VC-endpoints.
    - LV uses a 3-level support:
        - Level 1: Help-Desk
        - Level 2: Local Technician
        - Level 3: Central Administrator of all VC-endpoints
    - AT has a central Administrator/Technician with remote access to all VC-endpoints.

4. REPORT OF THE TECHNICAL SUB-GROUP

4.1. Using a questionnaire as starting point

Participating Member States and institutions filled out a questionnaire. The answers were consolidated within an Excel worksheet and a report was created, sorted by Topic / Category / Priority / User group plus some statistics on the answers received per Topic / Category and Member State. Please see the reports gained from the questionnaire results in the annexes to this document.

4.2. Findings of the Technical Sub-group

From the viewpoint of organisation and coordination of this partnership it was considered prudent to combine issues, problems and solutions raised. Those issues or problems were divided into several categories: legal, organisational and technical. Each category was then divided into sub-groups for each issue or problem.

As far as the technical issues are concerned the following problems were notified:

- Disruption of VC link due to technical problems. The picture might become unclear. Sound and/or quality issues.
- The line capacity is insufficient, video as well as audio signals cannot be transmitted together with adequate speed. Image as well as sound are of low quality.
- Safety measures like firewalls prevent contact.
- No document cameras available.
- Mobile cameras instead of fixed ones.
- The defendant needs to see the judge and the prosecutor simultaneously. She/he has to know who are standing in the trial room.
- The other court shows a frozen image because they do have not enough bandwidth when calling ISDN.
- An ISDN system contains a number of restrictions and causes higher costs to make a call compared to IP systems.
- The videoconferencing session cannot be established because of incompatible technical standards.
- Older videoconference models are not always compatible with newer brands/models.
- Technical support needed for e.g. defence agents to start and encourage their use of VC.
- Maintain security of the network whilst allowing links to outside organisations and individuals (e.g. when connecting defence agents).

In the technical category there were also questions raised highlighting a common need for tools to aid the process of cross-border videoconferencing between the judiciary in the various MS of the European Union.

- In principal it should be possible to use an Internet protocol video to access a secure VC point of entry of the Member State or the Judiciary or the Public Prosecutor.
- It has been suggested that the sTESTA network can potentially ensure that secure environment. However the sTESTA network is not designed to support any type of real-time traffic, which is needed for VC. As secure "virtual private network", which uses Internet links, sTESTA cannot guarantee any performance levels (e.g. for bandwidth). This question is to be re-evaluated when the new generation of the sTESTA network is available (e.g. video-bridge in TESTA-ng). Therefore currently the end-to-end encryption of the VC session between the VC end-points is the way to go.
- Several Member States have implemented a national booking system with very good success. But the booking system is easier within a MS, as users have both end-points under their control and can e.g. directly reserve both rooms required.
- The cross-border situation is different: one MS can request to carry out a video-conference, but needs a confirmation from the other MS that the VC room at the other end is reserved. This will require at least a 2-step process. The organisational sub-group has suggested a booking form for requesting and/or confirming a videoconference (see chapter 3.4.6 Organisational Action 6 – Exchange of technical videoconferencing parameters). Note: this booking form is not intended to replace the formal process for mutual assistance (see chapter 2.2 Legal framework), which has to be followed in any case as prerequisite for doing a cross-border videoconference!
- Some MS suggest the sharing of availability over the VC calendar of a MS could benefit the promotion of VC: the calendar of the planned timetable for videoconferences in different MS should be visible on the e-Portal – e.g. for registered VC contact persons, but not for public.
- The technical sub group of the IWG proposes to examine the possibilities for simplification of cross-border VC, e.g. using multi-point control units (MCU) at the European level (e.g. existing MCUs at Eurojust or at the Commission), where you could reserve a "virtual VC room". Both (or more) VC end-points could dial-in into this "virtual VC room" to establish the videoconference. Reservation of the "virtual room" could be done via the European e-Justice Portal, the national end-points need to be reserved by the participating Member States.

4.3. Security and data protection

A central theme in the creation of cross-border videoconferencing is the concern about security and data protection, e.g.:

- Security of the connection which has been established,
- and the security requirements and measures, which are required to ensure a secured videoconference.

Security measures should be agreed in advance. A protocol is needed in order to be able to work on a common basis to ensure the SECURITY of the connection with each other in the same way.

Part of that protocol should be a risk assessment. The way in which the security assessment is carried out and the security measures are communicated and agreed could be carried out in different ways:

- As a part of the check-list to be used when organizing and preparing for the videoconferencing session.
- As a memorandum of understanding between potential parties.
- Subject of the check list or a memorandum of understanding on the exchange of technical VC parameters:
    - Some of these parameters are public, e.g.: IP or ISDN; Room-number; ISDN-number (e.g. for a back-up scenario).
        - Note: The public parameters should be available for each Member State at the e-Justice Portal Member State's pages on videoconferencing.
    - Some of these parameters are confidential, e.g.: Passwords for outside access via gateways; IP-addresses for outside access (to avoid denial of service attacks)
- (Although it might be considered to be an organisation topic instead of technical one): A step-by-step description ("Protocol") is needed for preparing, testing, starting and running the videoconference, e.g.:
    - who will start the VC,
    - who will wait for an incoming call,
    - how are witnesses identified
    - handling of incidents?
- Please see also chapter **5 Security aspects**, which was provided by Eurojust!

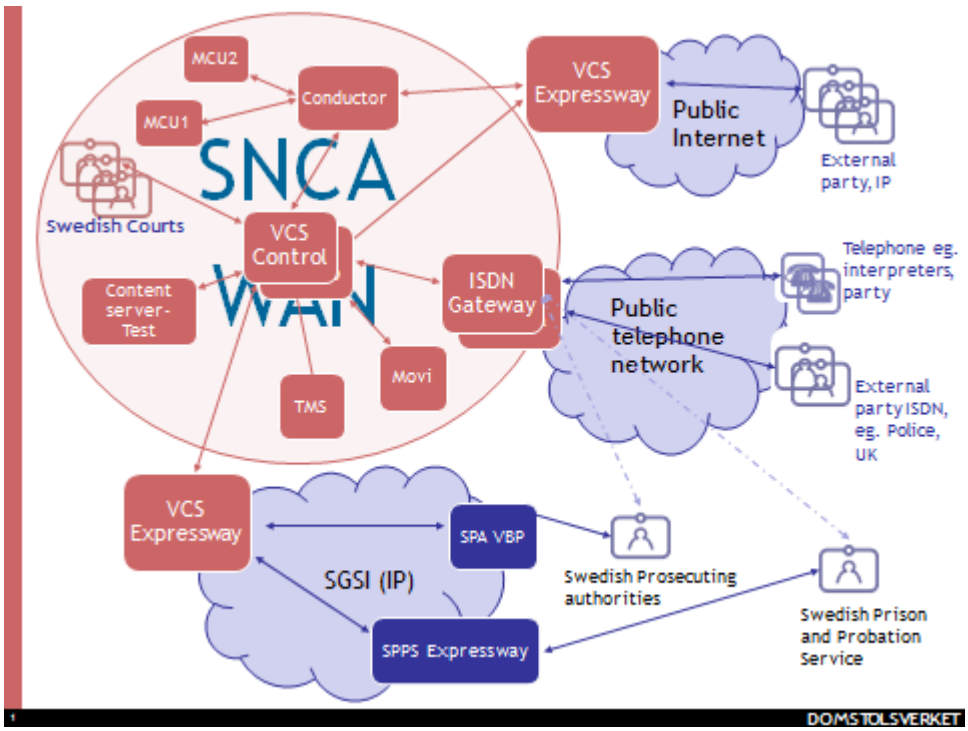
Several MS offered to share their expertise and knowledge. Best practice recommended during the meetings of the informal working group and the Member State's overall position with VC showed that technical standards between MS differ depending on the choices made by national back offices. Equally, there are also a number of Member States who implement the same architecture and international standards.

4.4. Comparable or similar setup of technical videoconferencing architecture

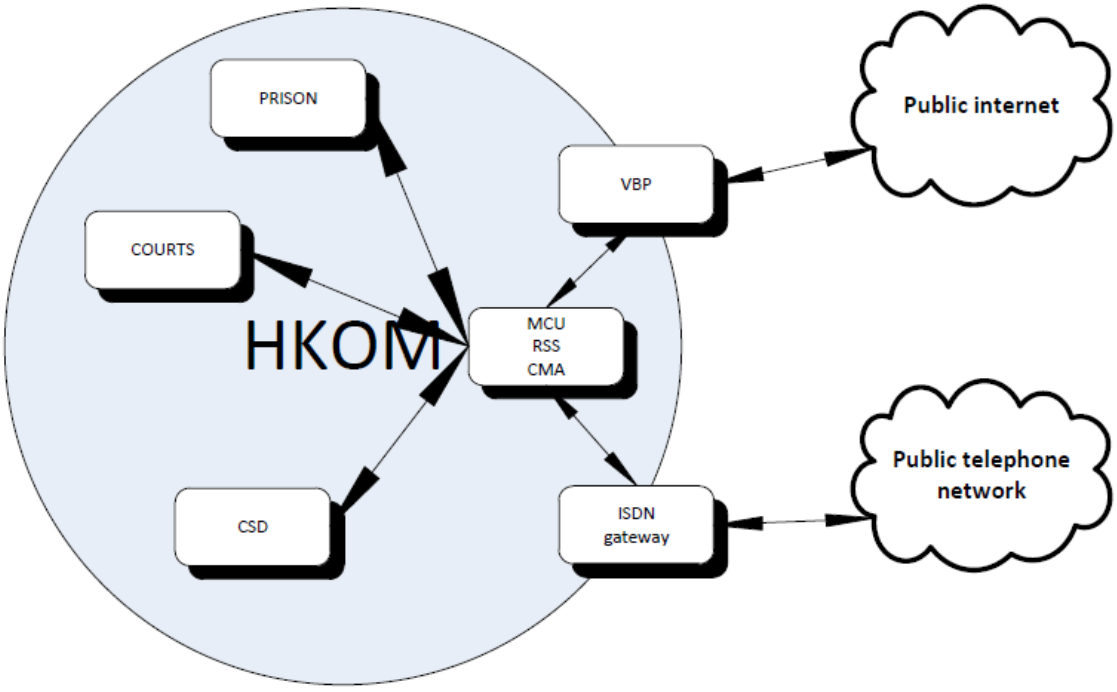
The diagrams below provide, by no means the only, examples of Member States that have opted for a similar technical setup:

The similar setup of technical videoconferencing architecture a does not imply that successful establishment of cross-border connections between those countries and their Judiciary will take place, since other factors play a decisive role. A test program should provide an overview of the possibilities.

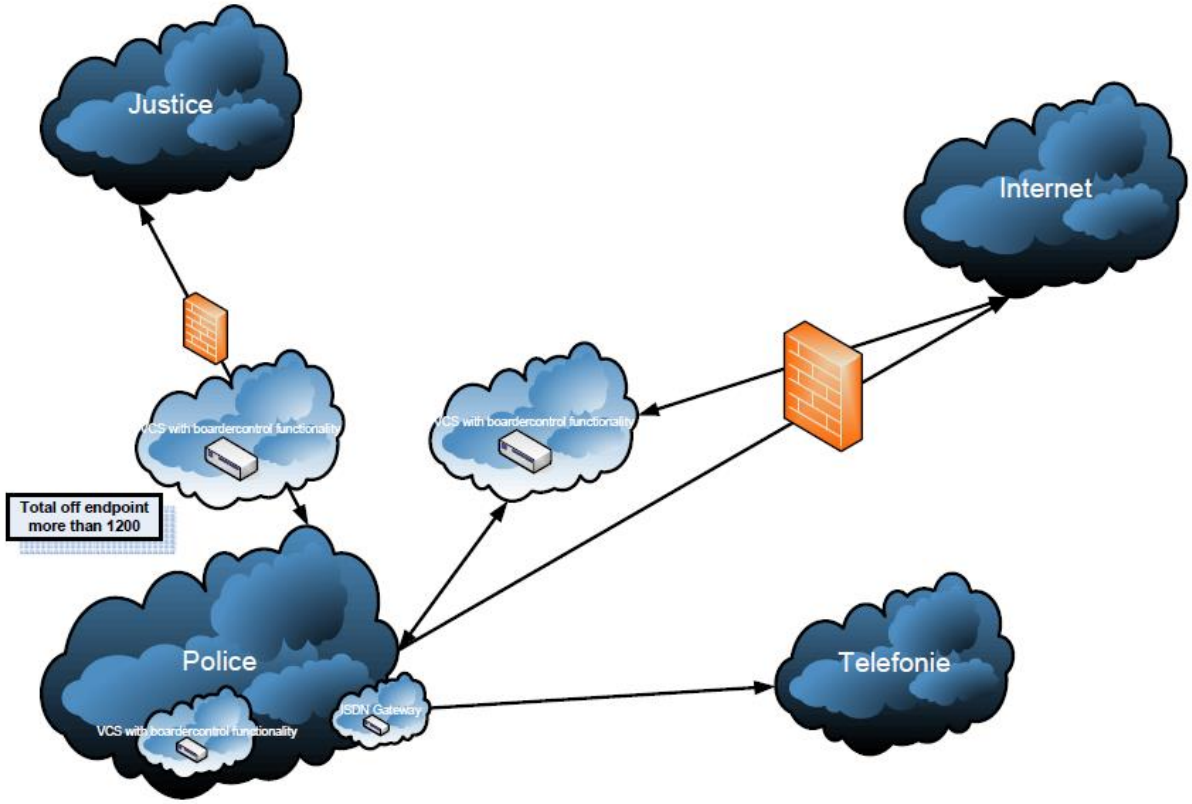
4.4.1. Sweden



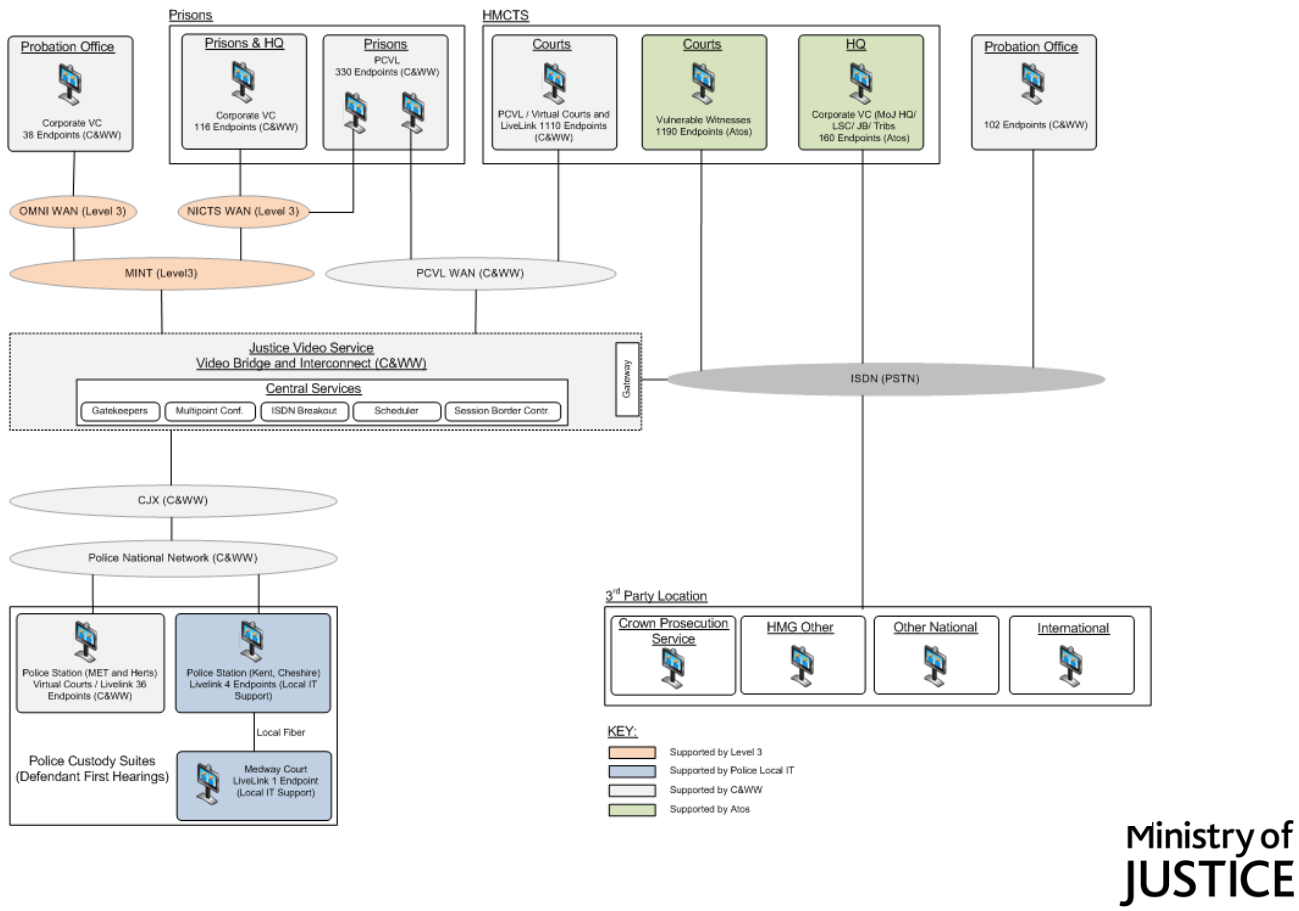
4.4.2. Slovenian video conferencing architecture



4.4.3. The Netherlands



4.4.4. United Kingdom – England and Wales



4.5. General advice: Implement the same international standards

This section further analyses the technical problems highlighted by the Member States in the questionnaire and recommends ways in which to find solutions or minimise their impact.

When it comes to the realization of a video link between the Judiciary in different Member States, the Technical Sub-group strongly recommends the need to establish applicable technical standards for videoconferencing endpoints.

This is the basic recommendation:

These technical standards are summarised on the "Videoconferencing information pages" on the e-Justice Portal.

- **Hardware-based video conferencing system (H.323/videoconference SIP)**
- **IP–based**
- **Firewall traversing infrastructure**
- **Encrypted communications (AES-128)**
- **Receive presentation as a duo video (H.239)**

See also paragraphs 71 to 92 in the "Technical Manual"

(see: https://e-justice.europa.eu/content_manual-71--maximize-en.do?idSubpage=18)

in the e-Justice Portal information pages on videoconferencing

(see: https://e-justice.europa.eu/content_videoconferencing-69-en.do).

Several Member States announced to post their technical standards on the e-justice portal and this will further improve the situation.

4.6. Mutual recognition of national laws

Within the European Union many different national legal systems exist. There are considerable differences between jurisdictions of Member States and even within a Member States (e.g. UK has 3 different national jurisdictions for England and Wales, Scotland and Northern Ireland). The Law of Member States is mutually recognised. If the technical restrictions are removed and a video link between the Judiciary in Member States is established, this would represent a huge step forward compared to the current practice.

However, one should realise while legal procedures differ between Member States this could also affect the technical requirements of (technical) support.

For a joint pilot project between several Member States and Institutions it cannot be ruled out that additional hardware components are required. Examples include the use of a multi-point control unit (MCU).

The use of such hardware allows authorities within the Judiciary or the Public Prosecution to meet in a "virtual meeting room" in a safe and secure way, without being provided with access to a MS network.

This type of solution is also feasible for the e-Justice Portal. Even without a video bridge (MCU) in the TESTA-ng network, it will be still possible to run videoconferencing traffic between two connected authorities within Europe if both authorities have an Expressway that is connected to TESTA-ng between judicial authorities (neighbouring zones). The Commission is not a collaborating partner in the IWG, but if this report will lead to a proposal for a project, this could be a consideration. This project could examine which opportunities and technical requirements are necessary to make such connections possible. MS would get access to a common videoconferencing network where security, reliability and performance would increase.

The Technical Sub-group recommends the involvement of the Commission in a joint project to examine whether a "virtual meeting room" is feasible and desirable in the e-Justice Portal.

Basic Functionality:

Judges, prosecutors, lawyers, persons to be heard, interpreters and clerks could interact the same way as doing face-to-face meetings via 2-way simultaneous video/audio transmission links.

4.7. Projects suggested during the meetings.

During the meetings several Member states emphasized that a joint project between the participants of this informal Council Working Group is the only viable way to achieve a working network for cross-border VC. Two concrete proposals were made in the early stages of the working group meetings:

1. "the adoption of the communication standards through VC and the establishing as well as implementation of the VC system within the judiciary institutions on the whole state territory that includes audio-visual equipment, communications equipment / network / infrastructure and setting up of the portal for practical users and citizens."
2. "A form should be created with the necessary technical information for each videoconference session (local technical contact (phone and e-mail), the videoconference system model, the bandwidth, type of connection (IP(H.323) and ISDN(H.320) and the supported protocols). We propose a shared calendar between EU courts equipped with videoconferencing equipment so that the schedule may make aligning the availability of the requesting court with the requested court. It is important to get feedback about real practical problems from judges, prosecutors and other professionals involved in videoconferencing."

4.8. Specific (funding) projects suggested.

Exchanges of views and discussions between the experts during the meetings of the Informal Working Group on Cross-border video conferencing, as well as informal contacts during conferences and other meetings, led to the realization that a joint project is highly desirable. Mutual trust has increased partly due to the understanding of each other's limitations and possibilities. Suggested content for different projects was logically combined into one combined project with different workflows. The approach of the project and its ambitions are realistic and have a step by step approach.

1. Research and identify per Member State which type of business is best suited to cross border Videoconferencing
2. Start with the testing and realization of a video connection between pairs of Member States and, adjust, if necessary, a protocol between Member States.
3. Summarize recommended technical standards from practical perspective.
4. Develop a step-by-step protocol for the processes and the cases that are going to be used.
5. Improve the Videoconferencing request in such a way that it reaches the right people within the Member States and that it become clear when and between whom the video conference will take place.
6. Develop training courses for potential VC users.

Notes:

- **Not all the points listed above are only technical issues but they do contribute to the flawless video session between Judicial authorities**
- **The technical sub group strongly recommends such a joint project to subscribe at the call for proposals**

The project ideas suggested were subsequently consolidated and circulated to the whole group, please see chapter **7.1 Content items for projects** for a more detailed description of the content-items for possible (funding) projects.

5. SECURITY ASPECTS

The protection of information and data processed in relation to the Videoconferencing sessions is a vital element of the overall juridical process facilitated by the use of modern IT and communication technology. To prevent information being compromised before, during and after the Videoconferencing session appropriate measures should be taken. The level of protection and controls should be driven by the sensitivity and confidentiality of the juridical case. As the implementation and maintenance of measures are related to certain costs the appropriate balance between the cost and the security level should be reached and only the relevant measures should be taken. Therefore there is no uniform solution for security measures that fit all kinds of cases.
In the paragraphs below the basic principles of protecting information and deployed ICT assets are addressed. These principles could be used as a guideline when assessing risks and identifying mitigating measures for specific cases, which could differ from the measures applicable for other cases.

5.1. Basic ICT security principles

In general, the basic security principles address the confidentiality, availability, integrity and accountability of the information.

5.1.1. Confidentiality

The IT and communication systems have to preserve the confidentiality of all sensitive information that is stored, processed, transmitted, received and presented. This means limiting access to the systems and information to only those who are authorized to enter, edit and view the information. Assets that must be protected include network configuration settings, administrative settings, security settings, user credentials, data and voice including audio and video stream.
Secure measures should consider not only devices within the environment, but the users as well. This means that organisations have to implement measures preventing data from both intentional and inadvertent security leaks. The measures include the following activities:

- Tight control over the issuing of user accounts
- Prompt removal / disabling of unused or stale accounts.
- Enforcement of strict password guidelines (password length, content, expiration)
- Use of additional identification techniques (e.g. biometrics, digital authenticators)
- Environment-wide policy of granting user privileges on a “must have” basis
- Blocking of inappropriate or unauthorized communications or applications

In addition, information that is transferred between devices and systems must be properly protected using the appropriate forms of encryption and cryptography. This includes information payload (meaning the data being sent such as the audio / video traffic itself) and the signalling information in use as part of the data transport / transfer and all control / device management information. The implemented controls must meet relevant EU and international standards and must be compliant with relevant National and EU regulations.

5.1.2. Integrity

Information and data integrity measures ensure the quality of correctness, completeness, wholeness, soundness and compliance with the intention of the information / data originator.

When necessary an originator of the information, data, video or audio recording might request a control which would prevent any unauthorised persons (accidentally or deliberately) altering of the information.

Nowadays, digital certificates are the most common means of data integrity validation. In addition to digital certificates, many organisations use digital signatures to verify the identity of the person creating, signing, or sending a document. The proper use of digital signatures provides data recipients with a degree of confidence that the information they received was provided by the proper source and has not been inappropriately altered.

Alternatively organisations might use special equipment to ensure integrity. These types of systems are often used for information archiving.

5.1.3. Availability

In some cases the availability of the videoconferencing service might be one of the top priorities as the failure of the VC session could have severe consequences.

Availability threats can be categorized into several categories:

- Deliberate threats including hacking, spoofing, and denial-of-service attacks
- Inadvertent threats including configuration changes / environmental modifications
- Device failures and malfunctions
- Issues caused by / related to third party services and systems

To maximize availability organisations should:

- Deploy high performance firewalls with strict access control lists / rule sets
- Limit the number of people able to modify / update system settings
- Define and follow strict backup procedures – including environmental settings
- Implement redundant, distributed, and self-healing architectures

- Deploy products that include …
    - inherent intrusion detection and auditing capabilities
    - the ability to disable unnecessary functions, and services
- Minimize 3rd party / external dependencies to the lowest degree possible

Maximizing availability means balancing cost, convenience, and risk.

5.1.4. Accountability / non repudiation

An important part of maximizing security is instilling an element of accountability within the environment. This requires proactive tracking and logging of communication sessions and managerial tasks. Key items that should be tracked include:

- User activities (logins, application usage, file transfers, etc.)
- Communication session information (call detail records, etc.)
- Security violations (unauthorized access, repetitive access failures, etc.)

Ideally, the tracking function should provide a) real-time information to allow security personnel to address certain concerns immediately, and b) archived and searchable information to enable the identification and resolution of longstanding or complex issues.

The concepts outlined above are intended to provide an overview of basic security concepts and not an all-encompassing view of all potential security risks and recommended preventative measures. However, readers should note that devices intended for use on secure Government networks must address a wide range of security guidelines and recommendations.

5.2. Some practical guidelines

5.2.1. Risk assessment

It is important that security measures are identified and agreed upon in advance. The most efficient way to determine security measures is to carry out a risk assessment based on the business needs and level of information, confidentiality and sensitivity.

During the risk assessment process an organisation analyses the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organisation. It is important that organisations seek to incorporate emerging risks and threats and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

The outcomes of a risk assessment could be laid down in:

- Memorandum of Understanding (MoU) signed by all partied involved in Videoconferencing
- As a part of a check-list to be used when organisations are preparing for a Videoconferencing session

A risk assessment should take into consideration:

- Security of an ICT environment hosting the Video Conferencing systems (servers, desktops, firewalls, routers, portable devices, etc.)
- A need to carry out security screening of stake-holders (participants, interpreters, supporting staff, etc.)
- A need for technical support before/during the video conference
- A need for specific security measures, such as secure exchange of authentication credentials, additional encryption of the communication channel, deploying trustful certificates
- A need for ensuring audit trance for future needs
- A need for ensuring the confidentiality of the session and potential recording
- A need to provide stakeholders with security awareness

5.2.2. The risk management framework

The Framework is composed of three parts:

- Framework Core
- Framework Implementation Tiers
- Framework Profiles.

Each Framework component reinforces the connection between business drivers and cybersecurity activities. These components are explained below:

- The Framework Core is a set of measures, desired outcomes and applicable references that are common across critical infrastructures. The Core presents industry standards, guidelines and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organisation from executive to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover.
- Framework Implementation provides context on how an organisation views cybersecurity risks and the processes in place to manage that risk.
- A Framework Profile (“Profile”) represents the outcomes based on the organisations business needs. The Profile can be characterized as the alignment of standards, guidelines and practices to the Framework Core in a particular implementation scenario.

5.2.3. Potential measures as a part of profiles

Security measures could include technical measures such as:

- Change default passwords
- Apply best password security practices
- Enable encryption for the VTC sessions
- Disable broadcast streaming
- Disable the far-end camera control feature
- Disable insecure IP services (e.g., Telnet, HTTP)
- Perform initial VTC settings locally using the craft port or the menu on the system
- Regularly update firmware and apply patches
- Practice good physical security (i.e., restrict access, turn off the device, and cover the camera lens when not in use)
- Disable any auto answering feature
- Disable wireless capabilities
- Separate VTCs logically from the rest of the IP network using Virtual Local Area Networks
- When remote access is absolutely required, institute strict access controls (e.g. router access control lists, firewalls rules) to limit privileged access to administrators only

5.2.4. Elements of the request for important for security

The following questions would have to be assessed when defining security requirements and measures:

- Who will attend / chair the video conference?
- What will the sensitivity levels be of the information discussed during the video conference (including the need for classifying the content)?
- Will there be a use of interpreters?
- Will the video conference be recorded?
- Is there is need for compiling evidence?
- Is compliance with National / European regulations needed, applicable MoU or Checklist?
- Need for exchange information prior the videoconference session?

5.3. Conclusion

The fundamental principles of data security (confidentiality, integrity, availability, and accountability) applicable to a videoconferencing session are similar to the sets of principles organisations are implementing in general when protecting their ICT infrastructure. Organisations should recognize that proper data security involves the protection of more than just the obvious pieces of information exchanged during videoconferencing sessions. For example, in the videoconferencing world, one must protect not only the media streams, but also the information stored within the video endpoints, video bridges, management systems, and other devices within the visual collaboration environment. For that reason it is important to address security matters before the actual start of the session.

6. VIDEOCONFERENCING WITH AN INTERPRETER (OUTCOMES OF THE AVIDICUS PROJECTS)

Sabine Braun, University of Surrey

6.1. Main configurations of bilingual videoconferencing with an interpreter

The increased use of videoconferencing in legal proceedings also concerns bilingual national and cross-border proceedings that involve the services of an interpreter. The videoconference configurations become more complex when interpreter is involved.

National proceedings: National legislative frameworks differ what is permissible, but in principle the following three configurations can be distinguished:

1. The judicial authority and the person to be heard (who does not speak the official language) are in different locations. This is used especially for video links between courts and prisons but also between courts and police stations (e.g. for first hearings in England and Wales) or hearings of remotely located witnesses. The interpreter is at one of these locations.
2. The judicial authority and the person to be heard are in the same location, and the interpreter is linked in from another location ('remote interpreting'). This is still infrequent in Europe, but common in the United States.
3. The main parties and the interpreter are all in different locations (combination of 1 and 2). This is also still infrequent, and in most cases the interpreter is just brought in via telephone. However, it is conceivable and preferable that a multipoint videoconference is used in such cases.

Cross-border proceedings: As outlined in chapter **2.2 Legal framework** of this report, cross-border videoconferencing has a legislative basis in the Second Additional Protocol of the 1959 Convention and the 2000 Convention. The legislation distinguishes between interpreting support for the judicial authority of the requested Member State, who is normally present during the proceedings (at least in criminal cases), and interpreting support for the person to be heard. A distinction therefore needs to be made between the following situations:

A. The person to be heard speaks the language of the requesting authority. The interpretation is provided to enable the requested authority to follow the communication between the requesting authority and the person to be heard. For example, if a Dutch court requests to hear a Dutch citizen who lives in Germany, the communication would normally be in Dutch, and the interpreter would interpret from Dutch into German for the benefit of the German judge.

B. The person to be heard speaks the language of the requested authority. The interpretation is provided to facilitate the communication between the requesting authority and the person to be heard. For example, if a Dutch court requests to hear German citizen who lives in Germany, the interpreter would interpret between Dutch and German, which could be a minority language) for the benefit of all parties involved.

Other, more complex situations arise when the person to be heard is a minority-language speaker (e.g. if the German citizen who lives in Germany does not speak sufficient German). Furthermore, due to the presence of both the requesting and the requested judicial authority, cross-border proceedings also lead to a more complex array of possible participant distributions than national proceedings. The options have been outlined in chapter **2.4.3 Interpreters** of this report. Essentially the interpreter can be co-located with either authority, or s/he can be in a third location. However, it is also important to take into account whether the parties speaking the same language are all in one location (as in case A above) or not (as in case B above).

Notwithstanding the many different configurations, all forms of videoconference-based interpreting share many characteristics of communication, and it is these characteristics that will be outlined in the remaining part of this Chapter. This is based on the research conducted in the European AVIDICUS projects.

6.2. Videoconferencing and interpreting: communicative aspects

The use of videoconferencing in legal proceedings has many benefits such as speeding up the proceedings, saving travel costs and avoiding prisoner transport to courts. At the same time, videoconference (VC) communication can be challenging. Research suggests that technical (video and audio) channels are less effective in transmitting a communicative message than the channels used in face-to-face communication and that it is more difficult to gauge what 'the other side' does and means. The involvement of an interpreter in the VC creates additional challenges. The feasibility of interpreting in a VC depends on a number of factors, including especially:

- The location of the interpreter in relation to the other participants, i.e. whether the interpreter is integrated into a video link between two (or more) sides, or whether the video link is used to gain access to an interpreter;
- The purpose, complexity and duration of the communication, i.e. whether the video link is used for a short exchange between a small number of participant or for a lengthy court trial or similar, involving various layers of communication;
- The mode of interpreting used, i.e. consecutive interpreting, whereby speakers say a few sentences and then pause for the interpreter to deliver his/her rendition, or simultaneous interpreting, whereby the interpretation is delivered while the speaker is speaking, either by whispering or with specific equipment (interpreting booth or portable equipment).

Several studies have focused on the use of VC in simultaneous conference interpreting in international institutions such as the EU and the UN. These institutions mainly have a need for 'remote interpreting', whereby the interpreters work from a different location, e.g. due to a shortfall of interpreting booths in meeting rooms. Although these settings are different from the requirements for interpreting in legal proceedings, some of the findings are noteworthy. All of these studies have, for example, highlighted the importance of sound and image quality and lip synchronisation as a prerequisite for good interpreting quality. The AVIDICUS projects have provided an assessment of the viability of videoconference-based in interpreting in legal proceedings (with a focus on criminal proceedings).

6.2.1. The AVIDICUS projects

The **AVIDICUS 1 project (2008-11)** provided an initial assessment of the viability and quality of videoconference-based interpreting in legal proceedings, and especially criminal proceedings. The focus was on consecutive interpreting as the most common mode of interpreting in criminal proceedings. Based on the outcomes of a survey among 200 legal interpreters in Europe, designed to identify the most pressing problems and the most likely settings for videoconference-based interpreting, the project conducted a series of experimental studies to compare the interpreting quality in traditional interpreting and in video links for some of the settings identified in the survey. The analysis of the data showed a number of differences between the two conditions, especially listening and comprehension problems, a higher number of interpreting problems (e.g. inaccuracy), difficulties with communication management, problems with rapport-building with the other interlocutors, and a faster decline of interpreting performance over time in video links, suggesting greater difficulties for interpreters and a faster onset of fatigue, and ultimately a higher cognitive load for the interpreters. The analysis also revealed that many of the problems arising were related. For example, overlapping speech was often followed by omissions. Another observation was that traditional interpreting strategies, such as visual signals, were less effective, e.g. in allowing the interpreter to take the floor and interpret, whilst other strategies, such as oral intervention to take the floor or resolve a problem, tended to feel more disruptive.

The findings of AVIDICUS 1 suggested that videoconference-based interpreting magnifies known problems of (legal) interpreting to a certain extent but that improvements may be achieved through training (e.g. to avoid overlapping speech), and the use of high-quality equipment (e.g. to ensure that voices can be heard clearly even in situations of overlapping speech). However, the data also suggested that there are also deeper-rooted behavioural and communication problems which may change the dynamic of legal communication and which warranted further research. To follow up further on the potential impact of training and equipment and on the potentially changing communicative dynamics in videoconference-based interpreting, the **AVIDICUS 2 project (2011-13)** was designed to address two strands of research. The first strand replicated the AVIDICUS 1 comparative studies, involving the same interpreters but providing them with short-term training in videoconference-based interpreting before they participated again. Moreover, better equipment was used. The second strand of the AVIDICUS 2 research focussed on the analysis of the communicative dynamic in video-mediated legal proceedings.

AVIDICUS 3 (2014-16) is currently assessing the implementation of videoconferencing facilities in legal institutions across Europe in terms of their fitness for the purposes of bilingual proceedings and interpreter integration.

The projects have also developed guidelines of good practice for videoconference-based interpreting in criminal proceedings (see e-Justice Portal: https://e-justice.europa.eu/content_manual-71-en.do), and designed and piloted training modules for interpreters and legal practitioners (see www.videoconference-interpreting.net).

6.2.2. Main outcomes of the AVIDICUS projects

Findings of the comparative studies: As mentioned above, the initial comparative study in AVIDICUS 1 revealed a higher number of interpreting problems, which led to the design of a follow-up study in AVIDICUS 2. The findings of this follow-up research create a complex picture, making it impossible to say without reservation that training, familiarization and the use of better equipment resulted in a clear improvement of the quality of interpreting. On the positive side, an improvement was observed in relation to some of the parameters that were analysed in the comparative studies. Moreover, the general impression of the observers and the participating interpreters was that under the influence of training and familiarisation, the experience of interpreter-mediated videoconferencing became less stressful for the interpreters, and there are indicators for improved confidence in approaching videoconference-based interpreting.

Adaptive behaviour: Subtle differences in the distribution of interpreting strategies, especially problem-resolution strategies, between traditional and videoconference-based interpreting support the conclusion drawn from the comparative studies that videoconference-based interpreting is, on the whole, more challenging than traditional interpreting. This is particularly apparent in the interpreters' more frequent use of passive and inefficient strategies in the videoconference settings. Given the fact that the participating interpreters were experienced interpreters, this may suggest that the interpreters' resources were too strained to apply more efficient strategies. At the same time, the data include a number of successful examples of strategy deployment and adaptive behaviour, and strengthen the assumption made in AVIDICUS 2 that training in videoconference-based interpreting particular emphasis on a detailed reflection upon the effectiveness of different strategies, including problem resolution strategies and pre-emptive strategies.

Communicative dynamics: Another strand of the AVIDICUS 2 research focussed on the analysis of the communicative dynamic in bilingual video-mediated legal proceedings. The analysis of (simulated) investigative interviews suggests that the interviewing officers spent more time developing and unfolding their interview strategy in the face-to-face setting than in video-mediated settings. These results could indicate that the interviewers had better contact with the interviewee during a face-to-face interview and that the interaction was better because the interviewers built up the interview more slowly and with a better foundation. The analysis of the (real-life) court hearings suggests that the use of VC in the court entails a reduction in the rapport between the participants.

The participants develop communication strategies that are aimed at restoring the rapport, although in the instances that were analysed some of these strategies led to a fragmentation of the communication and reinforced the changes in the communicative dynamics rather than reducing them. In part, the fragmentation was linked to the use of consecutive interpreting in situations in which traditionally whispered simultaneous interpreting would be used.

Physical location of the interpreter and the parties: The observations in relation to communicative dynamics led to more in-depth considerations of the interpreter's physical location in videoconference situations. In principle, the interpreter can be co-located either with the judicial authority or with the person to be heard (other-language speaker). In cross-border proceedings, where both the requesting and the requested judicial authorities are present in addition to the person to be heard (and other parties such as lawyers), the situation is even more complex. The AVIDICUS comparative studies suggest that there is no 'best' place for the interpreter and that different participants have different preferences. Many interpreters feel that they would like to be co-located with the other-language speaker. Where there is a choice for participant locations, strong asymmetries in the participant distribution should be avoided. If possible, the other-language speaker should not be separated from all other parties and the interpreter. It also needs to be borne in mind that the interpreter needs to be an impartial participant, focused on mediating the communication between the parties. Due care must be taken that the interpreter's physical location (i.e. side by side with one of the parties) does not undermine the required impartiality or the perception of impartiality. In complex participant configurations, this may be resolved by using a three-way or multipoint videoconference, where the interpreter is in his/her own location, but conclusive evidence is not available and further research is required into multipoint conference with interpreters. A further important point is that the interpreter's location has an impact on the mode of interpreting (see below).

Seating arrangements and spatial organisation: In addition to the interpreter's and other parties location, the seating arrangements in relation to cameras and screens are an important factor in the communication. In all data sets that were analysed in AVIDICUS 1 and 2, the seating arrangements and the spatial organisation led to interactional difficulties and changes in the communicative dynamics, and created a need for cooperative adjustments. One common problem was that due to being shown on a large screen or being placed in the centre of the video screen some participants were given an unjustified level of prominence or 'visibility'. A related problem was that seating arrangements gave the impression that the participants on one side of the video link spoke 'as one' or could be perceived 'as one' whilst in fact their roles need to be clearly distinguished – especially in order to maintain the interpreter's partiality.

View of participants: As a basic principle, every participant in a VC **including the interpreter** should a) be able to see the participants at their respective locations, b) be seen by the other parties, and c) see his/her own image. This will support the participants in constructing the situation at the other side(s) and in gauging the reactions of remote participants. Mutual visibility of all participants including the interpreter is best suited to overcome potential communication challenges in the videoconference. There should not be a situation where any of the parties or the interpreters are left guessing whether or not they are visible to the others. Furthermore, it is important that the interpreter can see the participants' facial expressions and possibly lip movements to aid comprehension of what is being said, and sometimes to resolve potential ambiguities. At the same time, the interpreter should not become the centre of attention simply by appearing on a video screen. The screen(s) showing the interpreter should therefore have an appropriate size (not too large), and the position of the screen(s) should not create a situation in which the parties have to turn away from each other in order to see the interpreter.

Mode (method) of interpreting: So far, consecutive interpreting is normally used in bilingual videoconferences in legal proceedings. This mode allows more easily than simultaneous interpreting for clarifications and interventions that may be necessary to ensure that the interpretation is accurate. Whispered interpreting (chuchautge), which is traditionally used in court proceedings in many Member States to interpret from the court's official language into the language of e.g. the defendant, is possible in videoconferences when the interpreter is co-located with the defendant (or other person to be heard). Whispered interpreting is also an option in cross-border proceedings when the interpreter interprets for the benefit of the requested judicial authority and is co-located with this authority. Limited tests with this mode of interpreting in the AVIDICUS projects shows, however, that it has its own dynamics; its feasibility would need to be investigated further. Simultaneous interpreting with specific equipment is theoretically possible in videoconferences as long as additional sound channels are made available, but there is very little experience with this mode in legal settings in Europe. A move to simultaneous interpreting would constitute a change from existing traditions in many national courts. A prerequisite would be a trained workforce of interpreters able to interpret simultaneously in both language directions but the systematic use of simultaneous interpreting in national courts and cross-border proceedings would require thorough testing and analysis of the interpreting quality and other factors. In the US, the Florida circuit courts use a combination of consecutive and simultaneous interpreting. Whilst this simulates the situation in traditional court proceedings (i.e. the combination between consecutive and whispered interpreting), it would still require an additional investment in suitable technology, testing and training.

Interpreters' working conditions: The introduction of video-mediated interpreting also raises important issues for the working environment of the interpreters. Given the cognitively demanding nature of interpreting, the duration of an interpreter's turn in a video link will require attention. Research shows a decline in the interpreting quality after approximately 15 to 20 minutes, suggesting that interpreters may not be able to work for an extended period of time in a video link. Given the high cognitive load of interpreting it also needs to be borne in mind that any additional distraction e.g. from technical parameters, unsuitable positioning and other factors are likely to have negative consequences for the interpreting quality. This is exacerbated by the fact that because of the novelty of many videoconferencing situations, interpreters are less likely to have coping strategies available when a processing overload occurs in a videoconference (e.g. when a speaker speaks too fast) than in traditional situations.

Some caveats are in order. Current research findings are derived from short-term studies. Given the generally low level of experience with bilingual videoconferencing, it is highly likely that some adaptation and familiarisation is yet to take place. However, given the challenges identified, interpretation in videoconferences should currently be applied with caution. Although some configurations are fairly well established, e.g. the user of interpreters in video links between courts and prisons, there are still no protocols, and many participants' experience with (professional) videoconferencing is still limited.

6.2.3. Implications

The outcomes of the AVIDICUS 1 and 2 projects have the following main implications:

- *Training*: The results of AVIDICUS support the need for training of the legal practitioners in interpreted video-mediated proceedings, in spite of some concerns about the effectiveness of short-term training. An effective type of training can be joined training sessions, with legal practitioners and professional interpreters. Although there are clearly different issues to be tackled for each group, ultimately they should come together in training, as indeed they will in practice. This is corroborated by the outcomes of various training sessions (for each group and join sessions) held in AVIDICUS.
- *Mutual trust*: The findings from the AVIDICUS studies make it clear that training and familiarisation cannot resolve all problems. Remaining problems can only be overcome in an atmosphere of openness and mutual trust between the parties, which, in turn, is only possible when the potential challenges of the VC setting are clear to all and when legal interpreters can be confident that their requests for clarification, for example, are not attributed to a lack of competence. Awareness-raising and the promotion of mutual trust therefore need to be included in all inductions to video-mediated and interpreter-mediated proceedings.
- *Interpreters' working conditions and interpreting quality*: Equally important, the quality of interpreting also depends on the quality of the interpreter. Given the current situation in Europe, where there is still insufficient provision of training and education in legal interpreting and where current trends of outsourcing as a way of cost-saving have led to a decline in the interpreters' overall working conditions, there is a high risk that qualified interpreters, who are able to cope with the challenges of VC-based interpreting, are not available for working in legal proceedings in sufficient numbers, because they choose more attractive interpreting jobs in other segments of the interpreting market. It is therefore necessary to consider not only the impact of VC-based interpreting on the interpreters' working conditions, but also the impact of the current working conditions of legal interpreters on the quality and viability of VC-based interpreting. Current trends in the procurement of legal interpreting seem to work against achieving minimum quality standards and mutual trust, i.e. are not conducive to using the benefits of VC-based interpreting.

- *System design*: Efficiency and quality in bilingual videoconferences are influenced by a range of factors which should not be considered in isolation. The use of high-quality technology – especially with regard to sound and image quality, lip synchronicity and stability of the connection – is one important parameter for enabling successful communication, but it needs to be complemented by other parameters. These include, at least, a suitable audiovisual environment in terms of lighting, visibility, sight lines etc.; careful and appropriate positioning of all participants; and effective communication management. All of these parameters are closely interconnected and build on each other. Minimum standards need to be specified not only for the main technical parameters, but also for the other parameters.

6.3. Conclusions

Appropriate solutions for bilingual videoconferencing will be beneficial for European cross-border proceedings and national proceedings alike and will make the use of videoconferencing in legal proceedings more attractive for all European Member States. They will contribute to the dematerialisation of legal proceedings and to simplifying and encouraging judicial communication between Member States, which are important aims of European e-Justice. Further research into the effectiveness of bilingual videoconferencing therefore constitutes an important horizontal measure for European e-Justice, serving the needs of both civil and criminal justice.

This research needs to be driven by the most recent emerging trends in relation to the use of videoconferencing and interpreting in legal proceedings which include:

- A potentially more diversified participant distribution leading to three-way videoconferences and new configurations of video-mediated interpreting;
- The extension of the use of videoconferencing and interpreting beyond its current uses mainly in pre-trial stages;
- The use of both consecutive and simultaneous modes of interpreting in videoconferences, and the associated questions of feasibility and appropriateness.

The questions about the appropriateness of the different modes of interpreting in videoconference-based proceedings is indicative of the more comprehensive question of whether video-mediated and interpreter-mediated proceedings will work best when they replicate as closely as possible the traditional face-to-face settings, e.g. by transferring known communication strategies and the spatial organisation of face-to-face settings to the videoconference settings, or whether justice is better served when design solutions start from the main requirements for all legal communication—i.e. fairness and efficiency of justice—and when systems are designed such that this is possible. Some of the AVIDICUS may suggest that a replication of all aspects of face-to-face interpreting is not the most efficient solution for video-mediated proceedings. Future research should therefore focus on video-mediated communication and video-mediated interpreting as modes of communication in their own right and address the question of where replicating face-to-face communication makes sense and/or is necessary to achieve appropriate communication and interpreting quality, and where adaptation will lead to better solutions for the fairness and efficiency of justice.

7. PROJECTS SUGGESTED

7.1. Content items for projects

The suggested project-ideas from all sub-groups were further refined and discussed with the whole group. The results are summarized in the following table.

Possible content for (funding) project(s)	Deliverable
1.) Identify use cases with high benefit from cross-border VC, e.g. Criminal: coordination meetings, … Civil: direct taking of evidence, … (Goal: get the overall picture)	• Guideline-Document
2.) Practical technical tests of cross-border VC connections between pairs of MS, e.g. point-to-point and multipoint incl. EUROJUST	• Technical Tests • Documentation of results (working parameters, failures, recommendations) • Know-how transfer
3.) Perfecting VC between a pair of MS (as separate or follow-on project)	• Standard procedure • Documentation • Re-usable parts?
4.) Develop step-by-step "protocol" with instructions for doing certain use-cases and processes with cross-border VC	• Practical tests including judges and court clerks; • Guideline-Document;
5.) Summarize recommended technical standards from practical perspective (belongs to 2, 3 and 5)	• Guideline-Document • Practical tips to make VC work
6.) Training and motivating potential VC users: e.g. via a series of demo VC-sessions, e.g. simulating a witness or expert hearing (postponed to a later follow-on project)	• Demo VC sessions for specific user groups • E.g. record some of these sessions for re-use
7.) Improve Form for requesting/confirming a VC (and public parameters to be published)	• Improved Form • Recommendations for parameter split
8.) Implement electronic sending of forms for "Direct Taking of Evidence" via e-Justice Portal and e-CODEX (should be an e-CODEX project)	• Implementation of e-CODEX use-case "Direct Taking of Evidence"

A large sub-set of the Member States participating in the Informal Working Group on Cross-border Videoconferencing submitted a funding proposal under the Justice Programme (CALL FOR PROPOSALS **JUST/2014/JACC/AG/E-JU**, application number **4000006961**) named "**Multi-aspect Initiative to Improve Cross-border Videoconferencing**" to address several of the above content-items for projects. The funding proposal aims to implement content-items 1, 2, 4, 5 and 7 of the above table:

- identify which use cases would benefit most from increased and better use of cross border VC;
- develop a step-by-step protocol with instructions for specific cross border VC use cases;
- perform practical testing of point to point and multi point VC between different Member States;
- summarise recommended technical standards from a practical perspective; and
- develop a form to request and/or confirm a cross-border VC between Member States.

The following suggestions should be implemented by further (follow-on) projects:

- support for the training and motivation of cross-border VC users through demonstration of typical VC use cases;
- perfecting VC between pairs of Member States; and

  Implement electronic sending of forms for cross-border mutual legal assistance, e.g. starting with forms for "direct taking of evidence" using the European e-Justice Portal and e-CODEX.

7.2. Summary of the project "Multi-aspect Initiative to Improve Cross-border Videoconferencing"

7.2.1. Objectives

Objective of the project "Multi-aspect initiative to improve cross-border videoconferencing" is to promote the practical use of and to share best practice and expertise on the organisational, technical and legal aspects of cross-border videoconferencing (VC) in order to help improving the overall functioning of e-Justice systems in Member States and at European level. The sub-goals are:

- Improve organising and running cross-border videoconferences between the EU Member States by providing VC users enhanced guidelines and step-by-step protocol for typical cross-border VC use-cases.
- Enhance the technical interoperability for videoconferencing by doing practical VC connection tests between the participating MS.
- Create an improved version of a form for requesting / confirming a videoconference together with static public information to be published on the European e-Justice Portal.

7.2.2. Activities

- Identify judicial use cases- which would benefit most from increased and better use of cross border VC;
- Develop a step-by-step protocol with instructions for typical cross-border VC use cases;
- Perform practical testing of point to point and multi point VC between different Member States;
- Summarise recommended technical standards from a practical perspective;
- Develop a form to request and/or confirm a cross-border VC between Member States in conjunction with public and static parameters to be published on the European e-Justice Portal.

7.2.3. Type and number of persons benefiting from the project

Judges and prosecutors from the judiciaries of the Member States, who are involved in cross-border cases with remote hearings via VC, as well as the technical staff supporting VC operations will benefit from the results of this project.

In addition also the external VC partners of the courts and prosecution offices e.g. witnesses, external experts, (vulnerable) victims, police, penitentiaries, lawyers, defence agents and community centres will benefit from smoother videoconferencing.

Since several hundred thousands of VC are already done by the European judiciaries per year and around 15% of them are cross-border, several tens of thousands of European citizens will benefit from the project results in addition to judges, prosecutors, legal professionals and external partners engaged in cross-border VC.

7.2.4. Expected results

- Guideline document on civil and criminal use-cases which can achieve high benefit from cross-border VC
- Guideline document with improved step-by-step instructions ("protocol") for typical VC use-cases, which combines technical (e.g. starting, accepting a call) and judicial (e.g. identify witnesses, experts, suspected and accused persons) and organisational elements (e.g. requesting/confirming the detail parameters for the VC)
- Practical technical VC connection tests between the participating MS
- Documentation on test results (working parameters, failures, recommendations)
- Guideline document summarizing the recommended technical standards from a practical perspective and with practical tips to make VC work
- Improved form for requesting/confirming a VC containing the variable and/or confidential parameters for the videoconference and recommendations for the public and static VC parameters to be published on the European e-Justice Portal.

7.2.5. Type and number of outputs to be produced

All above documents describing the project results will be produced in electronic format (Microsoft word or in PDF format) and are intended to be shared via the EU COM CIRCABC repository and re-used by the Member States and the Commission.

7.3. Project Partners

The project – if awarded – will be implemented by **12 partners** (including the applicant) and **3 associate partners** giving the **total of 15 organisations involved** in the project from **11 different Member States**.

Applicant:

Austria – Federal Ministry of Justice

Partners:

CCBE – Council of Bars and Law Societies of Europe
CZ – Ministry of Justice
EE – Centre of Registers and Information Systems
HR – Ministry of Justice
IT IRSIG – Research Institute on Judicial Systems
IT MoJ – Ministry of Justice
NL – Ministry of Security and Justice
PL – Ministry of Justice
SE – National Courts Administration
SI – District Court in Kranj
SI – Ministry of Justice

Associate partners:

LV – The Court Administration
UK (England and Wales) – Ministry of Justice
UK (Scotland) – Scottish Government

In addition the project will be **supported by Eurojust** in its normal role as EU institution supporting the judiciaries of the Member States.

The partners and associate partners of this project have already worked together in the Informal Working Group on cross-border videoconferencing and share the strong view that this project is useful and necessary to improve the use of cross-border VC.

8. APPENDICES

To keep the size of the final report as small as possible all appendices were moved to separate files!

Please see the following **annexes to see e.g. the detailed reports** gained from results of the "**Questionnaire on videoconferencing**":

VC-ANNEX - 8364/15 ADD 1: All completed videoconferencing Questionnaires sorted by Member State and ID

VC-ANNEX - 8364/15 ADD 2: Sorted report on all completed videoconferencing Questionnaires sorted by Topic, Category, Priority and Usergroup

VC-ANNEX - 8364/15 ADD 3: Statistics on all completed videoconferencing Questionnaires

VC-ANNEX - 8364/15 ADD 4: Project description "Multi-aspect initiative to improve cross-border videoconferencing"

_____