Multi-aspect initiative to improve   
cross-border videoconferencing

"Handshake"

Work-stream 3

D3 Recommendations on the practical application of technical standards for cross-border videoconferencing

|  |  |
| --- | --- |
|  |  |
| Deliverable Id : | D3 |
| Deliverable Name : | Recommendations on the practical application of technical standards for cross-border videoconferencing |
| Status : | Final version 1\_0 |
| Dissemination Level : | EU Commission and Member States |
| Due date of deliverable : | December 2016 |
| Actual submission date : | 31 January 2017 |
| Work-stream : | WS3 – Summarise recommended technical standards  from a practical perspective |
| Project coordinator: | Austrian Federal Ministry of Justice Johann Kickinger, Robert Behr, Thomas Gottwald |
| Organisation name of lead partner for this deliverable : | Swedish National Court Administration |
| Author(s): | Ulf Berggren, Anna Nerhammar and Adnan Duzel |
| Partner(s) contributing : | AT, CZ, EE, HR, IT, LV, NL, PL, SE, SI, UK-E&W, UK-S and Eurojust. |

Abstract:   
*The aim of this document is to raise the quality of videoconferencing between judicial authorities within the European Union, and to make it easier to use cross-border videoconferencing between Member States. Work-stream 3 of this Project has collected and used the valuable findings and experiences from the practical testing done in Work-stream 2. We found that videoconferencing is fairly easy to use, but establishing the communication between Member States to arrange the videoconferencing session is not as simple as required in regard to finding the correct contact information and guidance on how to make the call. It is therefore recommended that each Member State has support available to help with these issues. The testing in Work-stream 2 and the exchange of previous experiences between Member States has greatly benefitted the development of this document. An important aim of this Project, besides facilitating the use of videoconference, is to prevent future misunderstandings and errors. It is therefore essential to establish channels of contact to enable the sharing of information and best practice for video conferencing, both now and in the future.*

Disclaimer:

This publication has been produced with the financial support of the Justice Programme of the European Union. The contents of this publication are the sole responsibility of the partners of the Handshake project and can in no way be taken to reflect the views of the European Commission.

Executive Summary

This report describes, in a comprehensive way, the components and systems which are usually used in a network with videoconferencing technology. This document provides recommendations on how to avoid some of the problems and shortcomings which have been detected during our systematic tests carried out by work-stream 2 (WS2).

The results of the practical tests in WS2 have shown that there are some common faults or defects which make it difficult to establish a cross-border videoconferencing connection. This report provides suggestions on appropriate actions to take to help overcome these issues in the future. This will improve the success-rate for cross-border videoconferences and will lead to an increased use of the technology by applying safer and simpler techniques.

The recommendations are based on the results of the tests carried out in WS2. For example, the users shouldn’t need to be concerned about the type of manufacturer or brand of the equipment when making videoconferencing calls. Also the recommendations include the need to consider the different types of dial sequences when configuring the videoconferencing infrastructure. The infrastructure shall handle all or at least the most common manufacturer’s and brands dial sequences, automatically. To minimize problems when dialling out there is a need to consider prefixes, so that they do not conflict with the dialling out sequence.

Another recommendation is to allow video conference systems to dial out directly from the national courtroom. Therefore the infrastructure should be configured in a way which allows outgoing calls directly from an endpoint to an external party in a secure manner. National endpoints should be able to call an external endpoint or an external multipoint control unit (MCU) directly, without having to go through an additional national MCU. The tests have shown that there are different policies how to secure the video infrastructure and how to keep the control over incoming calls and how to allow outgoing calls directly from the endpoints installed in court rooms.

Videoconferencing calls that are conducted between member states over public networks and public environments have to be secure. Videoconferences behind firewalls or over ISDN based networks reduce the potential risk for call wiretapping, although there is still a risk. Use of encryption enables call privacy, when cross border calls are made over the public Internet and most of the available VC endpoints can be configured to use encryption. The recommendation is that endpoints should be set to “best effort” in regards to encryption to enable the highest probability to establish a successful videoconferencing session, even if that means that no encryption is used. If the sensitivity of the hearing requires encryption then at least one side of the connection must enforce encryption to be absolutely sure that encryption is used.

When it comes to the design of video conferencing room then good acoustic and lighting conditions are the basis for good sound and picture quality. A modern court room equipped for videoconferencing has special requirements for the technology to function well so the best acoustics and lighting that can be provided is a really important factor.

It is recommended that the court room has the right acoustic properties. To achieve a good quality of sound the reverberation time has to be considered. It is recommended that this is relatively short to create the best sound, though this can create issues with participants who are speaking quietly and therefore they may need to be provided with some speech amplification. A courtroom should have a reverberation time of about 0.4 to 0.5 seconds. The reverberation time is strongly linked to the room volume, smaller rooms can be allowed to have a shorter reverberation time and the larger rooms a somewhat longer reverberation.

Chapter 5 “Practical application of technical standards for cross-border VC” in this document describes this and the other technical recommendations in greater detail. Chapter 6 “Other practical recommendations” contains some practical recommendations.

History

|  |  |  |  |
| --- | --- | --- | --- |
| *Version* | *Date* | *Changes made* | *Modified by* |
| 0.1 | 2016-08-29 | Early draft | Ulf Berggren |
| 0.2 | 2016-09-22 | Draft | Ulf Berggren |
| 0.3 | 2016-10-06 | Draft – New structure | Ulf Berggren |
| 0.4 | 2016-10-13 | New comments | Ulf Berggren |
| 0.5 | 2016-11-07 | New structure | Ulf Berggren |
| 0.6 | 2016-11-21 | Grammatical adjustments | Ulf Berggren |
| 0.7 | 2016-12-05 | Abstracts, executive summery and text about ISDN, changed | Ulf Berggren |
| 0.9 | 2017-01-12 | Abstract, executive summary, text on firewall traversal and SIP | Johann Kickinger based on review input from Hugo Fillet, Ulf Berggren and Alan Hutchings |
| 1.0 | 2017-01-27 | Final changes for submission to EC | Johann Kickinger |

Table of contents

[Executive Summary 2](#_Toc473302006)

[History 3](#_Toc473302007)

[Table of contents 4](#_Toc473302008)

[List of Abbreviations 6](#_Toc473302009)

[1. Project goals 10](#_Toc473302010)

[1.1. Objectives 10](#_Toc473302011)

[1.2. Work-streams 10](#_Toc473302012)

[1.3. User groups who will benefit from this project 10](#_Toc473302013)

[1.4. Alignment with the European e-Justice Action Plan 11](#_Toc473302014)

[2. Document structure and interrelation 12](#_Toc473302015)

[3. The purpose of this document 14](#_Toc473302016)

[3.1. Purpose 14](#_Toc473302017)

[3.2. Work approach 14](#_Toc473302018)

[3.3. Results 14](#_Toc473302019)

[4. Technical and Organisational aspects 15](#_Toc473302020)

[4.1. Introduction 15](#_Toc473302021)

[4.2. Test report 15](#_Toc473302022)

[4.3. Technical aspects 15](#_Toc473302023)

[4.4. Organisational aspects 15](#_Toc473302024)

[4.5. Technical standards 15](#_Toc473302025)

[4.6. Other external factors 16](#_Toc473302026)

[5. Practical application of technical standards for cross-border VC 17](#_Toc473302027)

[5.1. Different Brands and differences in call parameter sequences 17](#_Toc473302028)

[5.1.1. Example of dial sequences 17](#_Toc473302029)

[5.1.2. Using MCU and multisite end-points 17](#_Toc473302030)

[5.2. IP, ISDN and the local area network 18](#_Toc473302031)

[5.2.1. IP or ISDN 18](#_Toc473302032)

[5.3. Video resolution, frame rate and bandwidth 19](#_Toc473302033)

[5.3.1. Bandwidth and quality of service 19](#_Toc473302034)

[5.4. Encryption 19](#_Toc473302035)

[5.4.1. Encryption endpoint to endpoint 19](#_Toc473302036)

[5.4.2. Encryption when using MCU 20](#_Toc473302037)

[5.5. Videoconferencing in courtrooms 20](#_Toc473302038)

[5.5.1. Presentation Layout – picture in picture 20](#_Toc473302039)

[5.6. Feeling of presence 20](#_Toc473302040)

[5.7. The design of the room is the basis of the videoconference quality 21](#_Toc473302041)

[5.7.1. Acoustic 21](#_Toc473302042)

[5.7.2. Acoustics in court rooms 22](#_Toc473302043)

[5.8. Lighting environment 22](#_Toc473302044)

[6. Other practical recommendations 23](#_Toc473302045)

[6.1. Organizational Videoconferencing 23](#_Toc473302046)

[6.2. Description of the national organisation in regards to videoconference 23](#_Toc473302047)

[6.3. Infrastructure 24](#_Toc473302048)

[6.4. Firewall traversal and Session Border Control 24](#_Toc473302049)

[6.4.1. ISDN Gateway 25](#_Toc473302050)

[6.4.2. Gatekeeper 25](#_Toc473302051)

[6.4.3. SIP Server 25](#_Toc473302052)

[6.5. Management System 26](#_Toc473302053)

[6.6. New Technologies 26](#_Toc473302054)

[7. Appendix I 28](#_Toc473302055)

[7.1. Picture 1 28](#_Toc473302056)

[7.2. Picture 2 29](#_Toc473302057)

[7.3. Picture 3 30](#_Toc473302058)

[7.4. Picture 4 31](#_Toc473302059)

[7.5. Picture 5 32](#_Toc473302060)

[7.6. Picture 6 33](#_Toc473302061)

[7.7. Picture 7 34](#_Toc473302062)

[I. References 35](#_Toc473302063)

List of Abbreviations

| *Acronym* | *Explanation* |
| --- | --- |
| AVIDICUS | AVIDICUS 3 is an EU funded project running from 2013 to 2015, focussing on the use of videoconferencing in bilingual legal proceedings that involve an interpreter |
| bit/s | Bit rate of the transmission in bit per second:   |  |  |  |  | | --- | --- | --- | --- | | **Symbol** | **Name** | **Multiplier**  (base 10) | **Multiplier**  (base 1000) | | bit/s | bit per second | 1 | 1 | | kbit/s | kilobit per second | 103 | 10001 | | Mbit/s | megabit per second | 106 | 10002 | | Gbit/s | gigabit per second | 109 | 10003 | | Tbit/s | terabit per second | 1012 | 10004 |   See: <https://en.wikipedia.org/wiki/Bit_rate>  See: <https://en.wikipedia.org/wiki/ISO/IEC_80000#Information_science_and_technology> |
| CCBE | Council of Bars and Law Societies of Europe (CCBE) |
| CODEC | A codec is a device or computer program for encoding or decoding a digital data stream or signal.  A codec encodes a data stream or a signal for transmission and storage, possibly in encrypted form, and the decoder function reverses the encoding for playback or editing. Codecs are used in videoconferencing, streaming media, and video editing applications. (Source: Wikipedia) |
| Defence agent | Defence agents are external VC users in UK Scotland with responsibilities, similar to a lawyer |
| DMZ | Demilitarized Zone |
| EAW | European Arrest Warrant |
| EIO | European Investigation Order |
| EU | European Union |
| Eurojust, | Eurojust is the European Union's judicial cooperation unit. It is a body of the European Union with its own legal personality and has its seat in The Hague (for details see: <http://www.eurojust.europa.eu> ).  Eurojust’s core business is to assist the competent authorities of Member States, when they deal with serious cross-border and organised crime, such as:   * Terrorism * Trafficking in human beings * Illegal immigrant smuggling * Drugs and arms * The sexual exploitation of women and children * Cybercrime * Online child abuse * Various kinds of fraud and money laundering * Counterfeiting * Environmental crime   Eurojust can also assist in such cases where a Member State and a non-Member State are involved. It can also help a Member State and the Commission when offences affect the European Union’s financial interests.  Eurojust’s goals are: first, to stimulate and improve the coordination between the national authorities, and to this end it works closely with EU partners such as the European Judicial Network (EJN), Europol, and OLAF where appropriate; second, to improve cooperation between the competent authorities, in particular by facilitating mutual legal assistance and the execution of mutual recognition instruments such as the European Arrest Warrant; and third, to support competent authorities in improving the effectiveness of their investigations and prosecutions, for example, by seeking solutions to recurring problems in judicial cooperation. In non-operational strategic matters, Eurojust works closely with EU and Member State institutions such as the European Parliament, national parliaments, the Council and the Commission.  Because crimes threatening European citizens are often global in nature, Eurojust has worked with various partners to help meet this threat. It has negotiated cooperation agreements for the exchange of judicial information and personal data outside the EU. Agreements have been concluded with Norway, Iceland, the USA, Switzerland, and the former Yugoslav Republic of Macedonia. Liaison prosecutors from Norway, Switzerland and the USA are based at Eurojust. In addition to cooperation agreements, Eurojust maintains a network of contact points outside the EU, and has memoranda of understanding with bodies such as the United Nations Office on Drugs and Crime and IberRed.  Eurojust supports this project in its normal role as EU body supporting the judiciary of the Member States in order that our project can benefit from Eurojust's experiences in videoconferencing and security and make best use of videoconferencing equipment at the European level, e.g. multi-point control units and their ability to create "virtual videoconferencing rooms". |
| 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.263 | H.263 is a video compression standard originally designed as a low-bit-rate compressed format for videoconferencing. It was developed by the ITU-T Video Coding Experts Group (VCEG). (Source Wikipedia) |
| H.264 | H.264 or MPEG-4 Part 10, Advanced Video Coding (MPEG-4 AVC) is a block-oriented motion-compensation-based video compression standard.  The intent of the H.264/AVC project was to create a standard capable of providing good video quality at substantially lower bit rates than previous standards (i.e., half or less the bit rate of MPEG-2, H.263, or MPEG-4 Part 2), without increasing the complexity of design so much that it would be impractical or excessively expensive to implement. An additional goal was to provide enough flexibility to allow the standard to be applied to a wide variety of applications on a wide variety of networks and systems, including low and high bit rates, low and high resolution video, broadcast, DVD storage, RTP/IP packet networks, and ITU-T multimedia telephony systems. The H.264 standard can be viewed as a "family of standards" composed of a number of different profiles. The decoder specification describes which profiles can be decoded. H.264 is typically used for lossy compression, although it is also possible to create truly lossless-coded regions within lossy-coded pictures or to support rare use cases for which the entire encoding is lossless.  H.264 was developed by the ITU-T Video Coding Experts Group (VCEG) together with the ISO/IEC JTC1 Moving Picture Experts Group (MPEG). The project partnership effort is known as the Joint Video Team (JVT). The ITU-T H.264 standard and the ISO/IEC MPEG-4 AVC standard (formally, ISO/IEC 14496-10 – MPEG-4 Part 10, Advanced Video Coding) are jointly maintained so that they have identical technical content. The final drafting work on the first version of the standard was completed in May 2003, and various extensions of its capabilities have been added in subsequent editions.  High Efficiency Video Coding (HEVC), a.k.a. H.265 and MPEG-H Part 2 is a successor to H.264/MPEG-4 AVC developed by the same organizations, while earlier standards are still in common use.  H.264 is perhaps best known as being one of the video encoding standards for Blu-ray Discs; all Blu-ray Disc players must be able to decode H.264. It is also widely used by streaming internet sources, such as videos from Vimeo, YouTube, and the iTunes Store, web software such as the Adobe Flash Player and Microsoft Silverlight, and also various HDTV broadcasts over terrestrial (Advanced Television Systems Committee standards, ISDB-T, DVB-T or DVB-T2), cable (DVB-C), and satellite (DVB-S and DVB-S2).  H.264 is protected by patents owned by various parties. A license covering most (but not all) patents essential to H.264 is administered by patent pool MPEG LA.[2] Commercial use of patented H.264 technologies requires the payment of royalties to MPEG LA and other patent owners. MPEG LA has allowed the free use of H.264 technologies for streaming internet video that is free to end users, and Cisco Systems pays royalties to MPEG LA on behalf of the users of binaries for its open source H.264 encoder.  (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) |
| IPv6 | Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.  Every device on the Internet is assigned a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available. By 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol. IPv6 uses a 128-bit address, theoretically allowing 2128, or approximately 3.4×1038 addresses. The actual number is slightly smaller, as multiple ranges are reserved for special use or completely excluded from use. The total number of possible IPv6 addresses is more than 7.9×1028 times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses. The two protocols are not designed to be interoperable, complicating the transition to IPv6. However, several IPv6 transition mechanisms have been devised to permit communication between IPv4 and IPv6 hosts.  IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol.  IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334, but methods to abbreviate this full notation exist.  (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) |
| MCU | Multipoint Control Unit |
| MS | Member State |
| NAT | Network Address Translation |
| PC | Personal Computer |
| QoS | Quality of Service |
| SBC | Session Border Control |
| 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) |
| VC | Videoconferencing (videoconference) |
| VTC | Video teleconference |
| WS | Work-stream (a subproject of this project) |

Table 1: Abbreviations

# Project goals

## 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.
* Enhancing 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.

## Work-streams

To achieve the above goals the project has been organised in the following **work-streams** (WS):

* WS0 – Management and coordination of the project.
* WS1a – Identify judicial use cases which would benefit most from increased and better use of cross border VC.
* WS1b – Develop a step-by-step protocol with instructions for typical cross-border VC use cases.
* WS2 – Perform practical testing of point to point and multi point VC between different Member States.
* WS3 – Summarise recommended technical standards from a practical perspective.
* WS4 – Develop an improved 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.

## User groups who will benefit from this project

**Judges, prosecutors and court clerks** 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** planning and supporting VC operations will benefit from the results of this project.

In addition, 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.

Several hundred thousands of VC’s 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.

## Alignment with the European e-Justice Action Plan

This project specifically supports the implementation of the e-Justice Action Plan project number 30 “Videoconference” (Category A).

By following the suggestions of the Council “Working Party on e-Law (e-Justice) – Expert Group on videoconferencing" and building on other work-results and experiences from the Member States, Eurojust and the Commission, this project aims to support and improve the following sub-goals of project nr. 30 “Videoconference” of the European e-Justice Action Plan 2014 - 2018:

* Organising and running cross-border videoconferences (in all MS)
* Enhancing Interoperability for videoconferencing
* Form for requesting/confirming a cross-border videoconference
* Exchange of experience and sharing best practice on videoconference – including materials (e.g. improved step-by-step “protocol” for VC in typical judicial use-cases), that can be re-used later (after translation and national customization) by the Member States for better training of their VC users.

The innovative aspect is to combine the organisational, legal and technical view in the same project in order to substantially improve the use of cross-border videoconferencing between the judiciaries of the Member states.

The results of this project will raise the probability for successful cross-border videoconferencing connections; this will help to increase the confidence of judges and prosecutors in using videoconferencing technology for their cross-border cases in both criminal and civil/commercial matters.

# Document structure and interrelation

This project produced the following delivery documents:

|  |  |
| --- | --- |
| **Work-stream** | **Deliverable** |
| WS1a | **D1a** **"Judicial use cases with high benefits from cross-border videoconferencing"**  This guideline document identifies typical judicial use cases which benefit most from (cross-border) videoconferencing – both in criminal and civil/commercial matters.  It is closely related with delivery document D1b, which contains the step-by-step instructions ("protocol") to plan, organise and run cross-border videoconferences. |
| WS1b | **D1b** "**Recommended step-by-step protocol for cross-border videoconferencing in judicial use-cases**":  This guideline document helps the requester of the videoconference with detailed step-by-step instructions on all legal, organisational and technical steps which are necessary to plan, organise and run a successful cross-border videoconference.  This document is closely related with document D1a – as D1b shall support the typical judicial use-cases identified in D1a. |
| WS2 | **D2.1 "Overall Test Report"**  This document summarises the findings from all individual test reports including the bilateral and multilateral cross-border VC connection tests done between the project partners.  This document concentrates on the facts gained from the tests by summarizing things which went well, and identifying the typical problems which occurred during the tests.  The recommendations to address the problems identified during the practical VC connection tests will be found in deliverable D3.  **D2.2 "Test Plan"**  The Test Plan was an important document to plan and organise the VC connection tests between the project partners. It describes the test procedure used and contains the template for the test logs (test reports) used to report the outcomes of each individual test.  As such tests can be done with and between additional Member States - this document was included as additional deliverable to allow reuse of our test procedure for cross-border VC connection tests by other Member States. |
| WS3 | **D3** **"Recommendations on the practical application of technical standards for cross-border VC"**  This guideline document gives the recommendations on the practical application of the technical standards. It specifically addresses the practical and technical problems identified in D2.1.  D3 is of utmost importance – as Member States following the recommendations of D3 will significantly increase the probability for establishing successful cross-border VC connections between their judicial authorities.  This document is closely related with D2.1 as D3 builds on the findings and experiences from the practical VC connection tests done. |
| WS4 | **D4 "Form for requesting/confirming a cross-border videoconference"**  This document describes an improved form which contains the relevant parameters for requesting/confirming a cross-border videoconference. This form is intended to be used as a supplement or appendix to the existing legal forms which have to be used as prerequisite to get legal permission to run a cross-border videoconference.  It includes recommendations which public and static VC parameters should be published on the European e-Justice Portal.  As an appendix it includes also the process documentation for the flow of the forms between the requesting and the assisting authority.  This document is closely related to D2.1 as the relevant technical parameters for a cross-border VC were identified when running the practical VC connection tests. |

# The purpose of this document

Recommended technical standards from a practical perspective

## Purpose

The purpose of this Work-stream 3 (WS3) has been to recommend practical application on technical standards for cross-border VC and to describe how to use the technical standard, from a practical perspective and to provide advice and recommendations on how to avoid problematic issues. It also proposes some best practice to facilitate cross-border videoconferencing by using experiences gathered in the practical tests made in Work-stream 2.

## Work approach

This project document gives some practical advice and experience on the basis of errors or differences in design and structure which have been found in our videoconferencing connection tests performed by Work-stream 2.

## Results

The result is a guideline document that can help Member States when planning their videoconferencing infrastructure and be a guide to the technical staff. It will recommend useful technical standards to follow when planning and setting up a cross-border videoconference.

The entire project results shall help to increase the total number of cross-border videoconferences and increase the percentage of successful cross-border videoconference calls.

Greater reliability of cross-border videoconference will motivate and encourage legal professionals from the courts and prosecution offices to apply this technology in more cross-border cases.

# Technical and Organisational aspects

## Introduction

This chapter describes shortly the test report and some general observations that affect the experience and the potential for a good experience when using video conferencing. In next chapter you will find recommendations and best practise described.

## Test report

Work-stream 2 has conducted a total of 56 bilateral tests involving 12 different organisations from 11 Member States. In addition a limited set of multilateral tests has been executed. The Work-stream 2 deliverable document **D2 "Overall Test Report"** summarises the results from all test sessions done.

The tests have been very useful and fruitful, and have shown that there quite a number of differences in the construction in the technical infrastructures and how the configurations has been set up. In some cases, these differences have been perceived as errors or defects, when in fact, the Member States have had different conditions and requirements.

The report from Work-stream 2 highlights problems that sometimes have appeared when trying to establish videoconference calls. The report also notes a variety of improvements and areas of development.

## Technical aspects

The goal of the Work-stream 3 has been to develop practical guidelines on the basis of the tests carried out in the Work Stream 2. These guidelines will be helpful for Member States in the planning and design of technical solutions for videoconference-infrastructure. The report can also be used as guidance when setting up cross-border videoconference calls. The ambition has been that these collected experiences can enhance the interoperability between the Member States videoconference infrastructure. This document shall contribute to a more reliable, simpler and more secure cross-border videoconferencing between different organisations within the Member States judicial systems. The technical standard, as described in the European e-Justice Portal, is the foundation for this document´s technical recommendations.

## Organisational aspects

The project and our tests have shown that there is a great need of information and experience exchange between the Member States. Not only when it comes to technical and practical experience, but there is also a need of understanding on how different the organisational structures and responsibilities are between the Member State´s judicial systems. The responsibility and the supporting organisations differ. In some cases is everything handled in-house by the own organisations staff, in some other parts, it´s handled by an external operator.

## Technical standards

The technical standard for videoconferencing described in the European e-Justice Portal is a recommended minimum technical standard. All Member States should be able to live up to the lowest level recommended in the e-Justice Portal.

The technical standard creates good technical basis and reduces the likelihood of problems; it also provides conditions for an acceptable level of image and sound quality.

## Other external factors

The report also contains a number of recommendations relating to the design of the rooms where videoconferencing technology is installed. Work stream 2 has shown that many rooms are not suitable for videoconferencing when it comes to lighting and acoustics.

# Practical application of technical standards for cross-border VC

The following recommendations have been made, based on the results of the tests carried out in WS2.

## Different Brands and differences in call parameter sequences

The sequence for entering the parameters when establishing a connection can be an issue when different brand combinations (equipment from different manufacturers) are involved. The users shouldn’t have to care about the type of manufacturer or brand when calling videoconference calls. Some problems encountered in the call setup have proven to be due to different technical solutions. Various technical solutions require different ways to connect calls

*Recommendations*:

* Consider the different types of dial sequences when configuring the videoconference infrastructure. The infrastructure shall handle all or at least the most common manufacture’s and brands dial sequences, automatically.
* To minimize problems when dialling out one has to consider prefixes, so that they do not conflict with the dialling out sequence.

*Benefits:*

* The users don’t have to care about the type of manufacturer or brand to which calling to or from. It should be as easy as making a phone call.

### Example of dial sequences

|  |  |  |
| --- | --- | --- |
| **Manufacturer** | **TCS4 delimiter** | **Example** |
| Aver | ## | 57.67.208.40##govvideoroom1 |
| Huawei | @ | Govvideoroom1@57.67.208.40 |
| Tely | @ | Govvideoroom1@57.67.208.40 |
| Polycom | ## | 57.67.208.40##govvideoroom1 |
| LifeSize | ## | 57.67.208.40##govvideoroom1 |
| TANDBERG/Cisco | @ | Govvideoroom1@57.67.208.40 |
| Sony | # | 57.67.208.40#govvideoroom1 |
| Codian | ! | 57.67.208.40!govvideoroom1 |
| Skype for Business | @ | Govvideoroom1@57.67.208.40 |

Table with example of different brands (manufacturers) in which sequence and with how many # (hashes) the call-in parameters must be entered in order to establish a successful connection.

### Using MCU and multisite end-points

Multipoint Control Unit (MCU), often called “video- or conference bridge“, enable multipoint or multiparty videoconferencing and enable connections between multiple videoconferencing endpoints. Tests showed that the configurations, when making a videoconferencing call between two member states, could contain none, one, or two MCU's.

When a MCU is integrated in the video conferencing infrastructure, it is important to consider how to handle and allow incoming- and dial out calls. If a dial out call passes an MCU then you have to be sure that the receiving part doesn´t utilise an MCU on its side. When more than one MCU is used for dial out calls, problems may occur, including the risk of that the call can start looping and ends the connection.

A MCU can handle multiple videoconferences calls simultaneously and the MCU operator can manage participants from individual conferences. It can block audio and video to or from any participant in any particular conference and it can merge conferences and much more. A central MCU often requires more frequent administration and management, which requires a bigger technical supporting organisation.

*Recommendations:*

* If it is possible, use endpoints with built in MCU function, also called a multisite function. This type of endpoint can usually connect 3-5 participants. An endpoint with multisite facility can handle participants in one virtual meeting room and easily add and drop participants.
* For authorities or organizations that have many videoconference systems and the need for several simultaneous meetings it is recommended to have a central MCU. A centrally located MCU can handle many participants in one or more virtual meeting rooms. The number of meeting rooms in an MCU can be a fixed number or a dynamic number of rooms. The rooms can be equipped with or without authorization. An MCU can be combined for a variety of options and combinations and this is one of many features.

*Benefits:*

* Endpoints with embedded MCUs (multisite) require less administration and management, it can be an advantage when it is common to have, two or more participants/endpoints. The judge can connect participants in a videoconference meeting itself. It will be a great advantage if it is possible to combine these two solutions, a central MCU and endpoints with multisite function, in the same videoconferencing infrastructure. In this way the court itself, in greater occurrence, can control the meeting, without a central operator involved. The choice and scalability becomes larger.

#### Dial-in/dial-out policies

Member States have different policies how to secure the video infrastructure and how to keep the control over incoming calls and how to allow dial out calls.

*Recommendations*:

* It is recommended to allow video conference endpoints to dial out directly. The infrastructure should be configured so that calls can be dialled directly from an endpoint to an external party on a secure way, without that the call goes through an MCU solution.

*Benefits:*

* It will be less administration and management if users can dial out by them self.

## IP, ISDN and the local area network

### IP or ISDN

Most of our Member States use IP to connect their videoconferencing sets. An IP solution typically provides higher bandwidth, which in turn gives a much better picture and sound quality.

*Recommendations*:

* It´s recommended that the Member State has a primarily focus on videoconferencing via IP. If one already has an ISDN gateway it should be kept as a backup channel. New investments in ISDN equipment’s should only be done as redundancy.

*Benefits:*

* Increased quality and availability of existing system.

## Video resolution, frame rate and bandwidth

The recommended frame-rate in the E-JUSTICE portal is 30 frames per second. Tests in WS2 showed that a good frame rate can be 25 frames/sec or 30 frames/sec. The resolution, 720p (HD), should in most cases be good enough.

*Recommendations*:

* Recommended video resolution is 720p (HD) with 1280 x 720 pixel, which allows excellent video quality (prerequisite for this of course that the required minimum bandwidth of 1.5 Mbit/s can be provided for an IP connection; with ISDN you have to use a much lower video resolution as the maximum bandwidth available for ISDN calls is typically only 384 kbit/s)
* The recommended minimum frame-rate is 25 fps, though the test in Work-stream 2 showed that the frame-rate usually is between 25 fps and 30 fps – depending on the used technology and available bandwidth.

*Benefits:*

* The recommended minimum frame-rate and the minimum resolution ensure, in most of the cases, a good quality for videoconference calls.

### Bandwidth and quality of service

In accordance with the E-justice portal the recommended minimum bandwidth for IP is 1.5 Mbps and for ISDN is it 384 kbps. Internet does not support Quality of service (QoS) but it can be a requirement in the own network (Local area Network or the own Wide area network (WAN)).

Once the number of participants in a conference call increases beyond a handful of people, having each of them keep a separate audio/video connection, participants will quickly overwhelm the local available bandwidth and processing capacity at the endpoint client.

In order to support a sufficient number of parallel videoconferences the Internet access point of the firewall traversal infrastructure must have enough bandwidth to support the required number of parallel cross-border VC sessions involved in (concurrent) videoconferences during peak-times.

*Recommendations*:

* In accordance with the e-Justice Portal the recommended minimum bandwidth for IP is 1.5 Mbit/s for each VC session plus 20%. For example, an IP call using 1.5 Mbit/s requires 1.8 Mbit/s of guaranteed priority bandwidth.
* The internal LAN and/or internal WAN of your organisation should have Quality of service (QoS) for videoconference calls.
* The Internet access point of your organisation needs to have sufficient bandwidth to support the required number of concurrent (cross-border) VC sessions during peak-times.

*Benefits:*

* QoS contributes the quality of the internal network traffic, though one should keep in mind that the Internet does not have QoS.
* The recommended minimum bandwidth ensures an excellent quality for videoconference calls.

## Encryption

Video conference calls that are conducted between member states over internet (public networks and public environments) need to be protected. Video conferences behind firewalls or over ISDN based networks reduce the potential risk for call wiretapping, although there is still a risk. Encryption solutions can assist call privacy, when cross border calls are made over the public internet.

### Encryption endpoint to endpoint

Most endpoints can be configured to use encryption.

*Recommendations*:

* In general, endpoints have a number of encryption settings. One can typically choose between “OFF”, “ON” and “AUTO” to indicate in which way the encryption capability should be utilised. Furthermore, there is also the choice to select which encryption mode should be used by selecting “AES”, “DES” or “AUTO”. To achieve the best compatibility with other systems it is recommended that endpoints are set to AUTO or “best effort” in regards to encryption.   
  This should normally provide an encrypted connection utilising the best common denominator, but in the event that one of the parties is unable to support a common encryption technique, the link can be unencrypted. If the hearing is especially sensitive case the Member States should make absolutely certain that the encryption is on. Encryption of the connection between the VC endpoints can be mandatory in a number of court cases.

*Benefits:*

* High security is important for the credibility of the technology and for protection of all participants in the videoconference.

### Encryption when using MCU

One has to consider that while the call from the endpoint to the MCU is encrypted, in the MCU itself it is normally not encrypted. This is important when outsourcing one’s MCU or infrastructure. It is a security issue. Therefore staff operating such devices should possess the relevant security clearances.

*Recommendations*:

* It is recommended to have the infrastructure and the MCU, in-house and to have in-house competence for the operation and maintenance of the videoconference infrastructure.

*Benefits:*

* The Member State with in-house equipment and competence will have a better control over the security and the infrastructure.

## Videoconferencing in courtrooms

Today's courts are modern and digital technologies are common. It is expected that one can connect their laptop or tablet to view and present images and documents in a case or negotiation, in both the courtroom and by the other party, participating by videoconference.

### Presentation Layout – picture in picture

Digital presentations like PowerPoint/Keynote or similar should be able to be send by the videoconference system, as picture in picture, in accordance with the de facto standard.

*Recommendations*:

* It is recommended that images can change the layout can be varied to not block or obstruct the presentation or image.

*Benefits:*

* Depending on what is most important to show there are options to display the most important thing as a larger image.

## Feeling of presence

It is important that participants in a videoconference can get a sense of presence and that the image is centred on the person or persons participating in the meeting and the image enables to observe the body language of the person speaking.

*Recommendations*:

* The camera should be placed as close as possible to the centre of the image on which the other party is presented. Sometimes it may be appropriate to use an additional camera to switch between if the room is large and there are many participants in the meeting.

*Benefits:*

* The advantage is that meeting participants have a greater sense of presence and the ambition is that the experience should be equivalent to a regular meeting as far as possible.

## The design of the room is the basis of the videoconference quality

In a modern court room equipped with videoconference there are special requirements for the technology to function at its best. Good acoustics is a very important part in a video conference call. Equally important is lighting.

### Acoustic

Good acoustics in a courtroom may be accomplished in a number of ways and should be studied on a case to case basis. A court room’s acoustics includes consideration of reverberation, sound absorption, sound diffusion and speech perception”

#### Reverberation time

Reverberation time means the time it takes for the sound pressure level, in a room, to drop to 60 dB after the source of the sound has become silent.

#### Sound Absorption

The sound absorption affects how sound behaves in a room. When a sound wave meets a room surface, the sound energy is reflected, absorbed or transmitted through the material. The sound quality in a room is determined by the sound absorption, room layout and the materials used in the room.

Sound absorption means a material's ability to absorb sound. With the help of sound absorption in different materials, the sound pressure level will be affected so that a comfortable sound environment is created. It creates the necessary prerequisites so that people and technology can work together. Correct amount and correctly distributed absorption, increases speech intelligibility, reduces reverberation (echo), and makes the electroacoustic installation easier.

This parameter is given in percent form or decimal format where 100% is the maximum practicable sound absorption and 0% is total reflection. All materials have some form of sound absorption.

#### Sound Diffusion

Sound diffusion means a surface's ability to break up the incident sound in different directions. In some cases, a surface that is perceived as plain has a function of diffusing for certain frequencies. Hard and plain material has generally very low diffusing characteristics in the frequency range of speech.

The diffusion is very important in rooms with short reverberation time. A diffuse sound field reduces the risk of flutter echoes and annoying reflections from the wall surfaces without absorbers.

#### Speech intelligibility – Speech Transmission Index

Speech Transmission Index (STI) is an objective measure of speech transmission quality. Speech intelligibility shouldn´t be mistaken with speech quality which is related to the quality of reproduced speech signals with respect to the amount of audible distortions.

Intelligibility of speech sound is a measure of how the spoken information is affected by interference from reflections in the room during the sound path from the speakers to the listener. The scale below is used to rate speech intelligibility and is abbreviated STI (Speech Transmission Index) and is given in % or in decimal form with the names of the intervals in the table below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STI (decimal)** | 0-0,3 | 0.3-0,45 | 0,45-0,6 | 0,6-0,75 | 0,75-1,0 |
| **STI (percent)** | 0-30% | 30-45% | 45-60% | 60-75% | 75-100% |
| **Term** | Bad | Poor | Fair | Good | Excellent |

### Acoustics in court rooms

A modern equipped court rooms should have some kind of special sound absorption material to get a higher quality of sound.

*Recommendations*:

* It is recommended that the court room with videoconference system have the right acoustic properties. To achieve a good quality of sound the reverberation time has to be considered. It is recommended that it is relatively short to create the best sound. Which can create issues with participants who are speaking quietly and therefore might require speech amplification. Speech amplification often involves an electro acoustic amplification with microphones and speakers.
* As a guideline, a courtroom should have a reverberation time of about 0.4 to 0.5 seconds. The reverberation time is strongly linked to the room volume. Smaller rooms can be allowed to have a shorter reverberation time and the larger rooms a somewhat longer reverberation.

*Benefits:*

* Good speech intelligibility is the key during video conference meetings, and will give more presence and hopefully good videoconference meetings.

## Lighting environment

It is important that the videoconference participants have correct lighting and from the right direction. One should also consider how well the participants face is shown compared to the background.

*Recommendations*:

* The light should be a combination of both diffuse light and directional light to create the best conditions. The surface behind the participant should have a contrast corresponding to a reflectance value that gives a clear image of the person. The background should be evenly illuminated.
* To create optimal conditions for the camera, the surfaces should not be completely white, red or yellowish and shadows and glare should be avoided.

*Benefits:*

* The right lighting and the right background gives more natural experience.

# Other practical recommendations

Under this heading are collected other practical experiences and recommendations noted during the project work but not directly linked to the tests.

## Organizational Videoconferencing

When organisation a cross-border videoconference session it can be hard to find the right person to set and planning, finding an agreed date/time, reserving the videoconferencing facilities and if appropriate, arranging technical staff. It often can take much more time than the call or proceeding itself.

*Recommendations*:

* Each Member State should have a general document, with an overall level schematically illustrates and describes the national videoconferencing network for the legal system. It is important that each Member State have a general knowledge of their existing infrastructure. It makes it easier for the Member States to create a long-term plan for future investments and improvements.
* The structure and the organisation of the operation and maintenance of the infrastructure are a very important and will affect, service, maintenance, development and costs. Technological development occurs quickly and it is important to follow the developments in order to provide and maintain a high security and high availability to the infrastructure for videoconferences.

*Benefits:*

* An overall description of the infrastructure can facilitate the understanding of the technology if there are problems with the connection of videoconferencing calls between member states. It is also beneficial if there is a broad comprehension and knowledge within the own organisation, i.e. how the infrastructure is constructed and how it all works together.

## Description of the national organisation in regards to videoconference

The judicial system is organized in different ways throughout the member states which means it is a challenge to find the right contact channels. This has been evident in the testing phase of Work-stream 2. It is difficult to find the right contact channels and make an appointment and to get the booking confirmed.

*Recommendations*:

* Each Member State should have an overall description of their organisation, published on the European e-Justice Portal. It should describe the overall structure and which organization is responsible for the technical infrastructure. For example, does the Member State have a national technical support that can be contacted in case of technical issues?
* Contact information between the Member States technical organisations should be up to date. The technological development is fast and it is very important that there is continuity regarding the exchange of technical know-how and practical information, between the Member States. Each Member State should have a support organisation to turn to when technical issues occur. If there are one or several support organizations, it should describe how to contact these. Exchange contact information with technical staff in other Member States.

*Benefits:*

* A description of the organization and who is responsible for the different parts of videoconferencing technology, and contact information to technical staff will promote contact and exchange of information.

## Infrastructure

Networks to which the videoconference systems are connected may consist of a national judicial network or several autonomous networks for each authority and organisation.

Regardless if the network is an individual network or consists of a large number of connected organisations, the way of connecting to the Internet is important for the videoconference function and for the security of the network.

When it comes to videoconferencing technology as the link between different networks and the Internet, should the infrastructure consist of a technical solution with a high level of security. The network should also have a high availability of the service to videoconference.

The network should have a firewall to be able to communicate with the outside world in a secure manner, and the infrastructure should include firewall traversal equipment, gatekeeper (for H.323), management system, SIP server, etc.

Firewalls will, amongst other things, actively monitor incoming packets, traffic and application data entering a private network and it will block incoming network transmissions that violate the network policies.

*Recommendations*:

* It is recommended to have a redundant technical solution. ISDN connections can in some cases provide redundancy for IP.
* Coupling between different networks should be built with firewall traversal equipment and software, suitable for videoconferencing.

## Firewall traversal and Session Border Control

The Session border controller handles firewall traversal and IP address translation (when NAT is used). A Session Border Controller (SBC) will be placed at both sides of the firewall. The SBC that is placed at the internal network side of the firewall can then be accessed by a Gatekeeper. A network administrator has to implement a methodology suited to the firewall and to decide which types of traffic (protocols) are allowed.

Connectivity between the Internet and the internal videoconferencing (VC) infrastructure should be via firewall traversal equipment. The traversing equipment should be configured to handle incoming and outgoing calls.

For your VC endpoints direct outgoing calls over the Internet **must** be allowed to enable the following cross-border calls:

1. Your VC endpoints can call-in into a virtual VC room created by a multipoint control unit (MCU) of another Member State (or organisation). **This policy is required.** The reason is: if both Member States (both organisations) forbid the direct dial-out for their VC endpoints then they will end-up either with no connection possibility at all or with a non-working configuration involving two MCUs.
2. Your VC endpoints can call-in directly to a VC endpoint of the other Member State (or organisation) – if the other Member State (or organisation) allows this.

If a Member State or organisation allows or forbids incoming calls over the Internet directly to their VC endpoints is of course a decision of each MS or organisation.  Incoming calls directly to your VC endpoints **should** be allowed in order to enable a cross-border point-to-point connection directly between two VC endpoints.  If a Member State (or organisation) does not allow this – then the most secure cross-border connection – a point-to-point connection between two VC endpoints with true end-to-end encryption – is not possible any more.

Incoming calls that are not addressed to a specific virtual VC room or VC endpoint should be routed to a generic virtual room or lobby on the MCU.

*Recommendations*:

* It is recommended that the Member State should incorporate actual firewall traversal equipment into their infrastructure instead of primarily using an MCU as firewall traversal equipment. The primary role of an MCU is to host a videoconference, not to act as a firewall. Videoconferences with multiple partners do normally not require more than 1 MCU.  
  If MCU’s are used at both sides of the link it is most likely that video looping will occur   
  (Droste effect, see <https://en.wikipedia.org/wiki/Droste_effect> ). The reason for this effect is: both MCUs try to produce a combined picture from all input video-streams and send this combined output video-stream back to the other. This will result in an always deeper nested picture or black picture and might even overload or crash the MCU.

*Benefits:*

* The use of a firewall traversing solution minimizes problems when connecting to external videoconference systems. The tests made in Work-stream 2 have shown that where a real firewall traversing solution is available and where it takes place according to the SBC it has worked out well in most of the cases. See also the findings in the report of Work-stream 2.

### ISDN Gateway

Gateways can allow videoconferencing devices on ISDN to participate in conferences with devices on an IP network.

*Recommendations*:

* ISDN is used by some Member States, but also occurs outside the EU. ISDN should be part of a redundant solution of the videoconference infrastructure.

*Benefits:*

* An ISDN gateway creates the opportunity to work as a backup solution when there is problem with the Internet and it can be the only solution to connect other countries that do not allow or don’t yet have an IP solution in its infrastructure.

### Gatekeeper

Gatekeepers regulate addressing schemes, internal prefixes and dialling plans and traverse the firewall. Gatekeepers can also allow endpoints and MCUs behind a firewall to receive inbound calls.

*Recommendations*:

* It is recommended that Member States incorporate a gatekeeper in their videoconference infrastructure.

*Benefits:*

* When a gatekeeper is used in concert with firewall traversing equipment, the gatekeeper can be used to traverse firewalls. It also gives a greater control of all videoconference systems and their calls.

### SIP Server

A SIP server handles call setup and call tear down of all SIP calls in the network. A SIP server can also referred to as a SIP Proxy. As such, a SIP proxy server primarily has the role of call routing. Proxies are also useful for enforcing policies, such as for determining whether a user is allowed to make a call.

A SIP server can also have the role of a registrar and accepts register requests, recording the address and other parameters from the user agent, and that provides a location service for subsequent requests. The location service links one or more IP addresses to the SIP URI of the registering agent. SIP registrars are logical elements, and are commonly co-located with SIP proxies.

Note:

* For a detailed description of the Session Initiation Protocol (SIP) – RFC 3261 of the Internet Engineering Task Force (IETF) – see: <https://www.ietf.org/rfc/rfc3261.txt>
* SIP functionality (SIP proxy server, SIP registrar) can be integrated in Gatekeepers and can be hardware devices or software applications – depending on the types of devices deployed

*Recommendations*:

* It is recommended that Member States incorporate a SIP server in their videoconference infrastructure.

*Benefits:*

* SIP is considered to be a modern successor of the H.323 protocol suite. More specific, the call setup handling within SIP is less complex than in H.323.
* SIP also uses a Uniform Resource Identifier ([URI](http://www.ietf.org/rfc/rfc2396.txt)) – see <https://www.ietf.org/rfc/rfc2396.txt> – to uniquely address a resource over an IP network.
* URI’s can be registered within the [DNS system](https://tools.ietf.org/html/rfc7553) as a Uniform Resource Identifier (URI) DNS record – see: <https://www.ietf.org/rfc/rfc7553.txt>

## Management System

Management solutions can be deployed as software or hardware system and the functions are integrated with the videoconferencing infrastructure.

A management system can help configuring software options, provisioning, and prepare video conferencing devices to meet requirements on networks and the conferencing manager’s needs. It can update and apply software to devices and monitoring endpoints to ensuring that they are on line and operational.

A management solution can give scalability and automation and let administrators to manage all these meetings from a single interface.

Conferences can be created directly or scheduled so that the management solution will direct the MCU to dial out to the correct endpoints at the right time using the correct settings. Conference management can include conference templates, or saved meetings, for a quick meeting creation.

*Recommendations*:

* Member State that has enough endpoints to motivate an infrastructure is recommended to have a specific management system for administration, monitoring end points, provisioning and to handle software upgrades and much more.

*Benefits:*

* A management system provides benefits as minimizing the administration tasks and creates possibility to device monitoring, provisioning and software management. It is often possible to get statistics and diagnostic information when troubleshooting videoconference calls.
* It will also provide a good overview of connected systems as well as a snapshot of the status of all connected and active systems.

## New Technologies

The Member State should construct a videoconference infrastructure that in the near future is capable of handling external parties calling videoconference via non-traditional videoconference ways, such as using a normal PC, laptop or Android device with a browser which supports the **WebRTC** standard (Web Real-Time Communication – standardized by the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF)). A browser with WebRTC support allows the user to connect to a videoconference directly by clicking on a Link in his Internet browser.

In addition also **standalone software** (e.g. Jitsi or similar vendor-specific implementations) can be used to enable a PC, laptop, tablet or even a mobile phone to be used as VC endpoint.

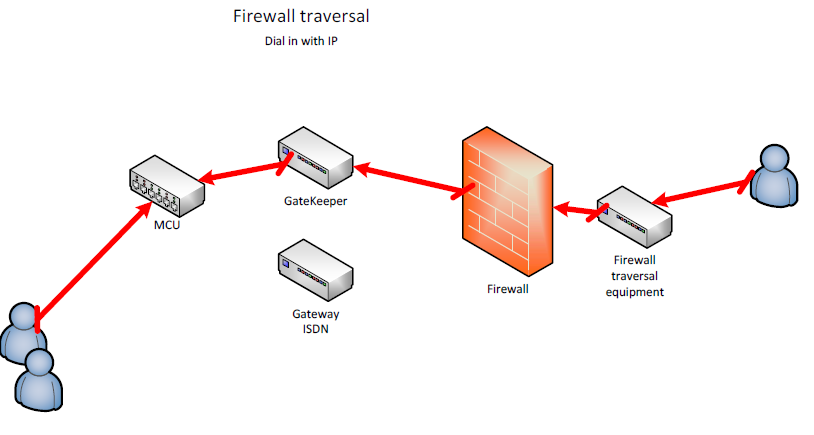
Organisations need to be aware that the migration from IPv4 to **IPv6** will also affect their videoconferencing infrastructure.

New upcoming standards like **High Efficiency Video Coding** (**HEVC**), also known as **H.265** and **MPEG-H Part 2**, will support higher video resolutions up to 8192×4320 pixel, including **8K UHD.** Even if such new standards use more efficient data compression technologies to support higher video quality at the same bit rate, they will require much more bandwidth for transporting – e.g. when using 4K UHD video with 3840x2160 pixels per picture – than the bandwidth we use today to transport a 720p HD video with just 1280x720 pixels per picture. So network planners must be aware that they will need to provide more bandwidth in the future to support higher video resolutions.

# Appendix I

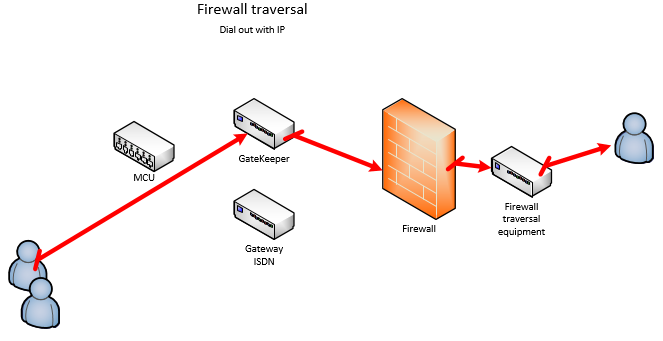
## Picture 1

The picture shows a schematic structure of firewall traversal solution, where the meeting participant have agreed to meet in a virtual meeting room. The external meeting participants dials in to a MCU.



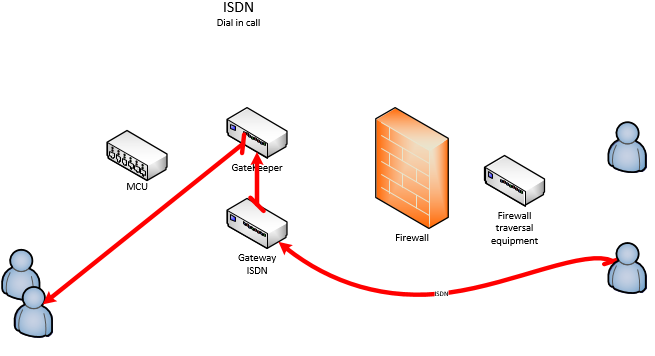
## Picture 2

The picture shows a schematic structure of a firewall traversal solution, where a meeting participant dials out to an external meeting participant, by using IP. The external person receives the call directly without MCU.



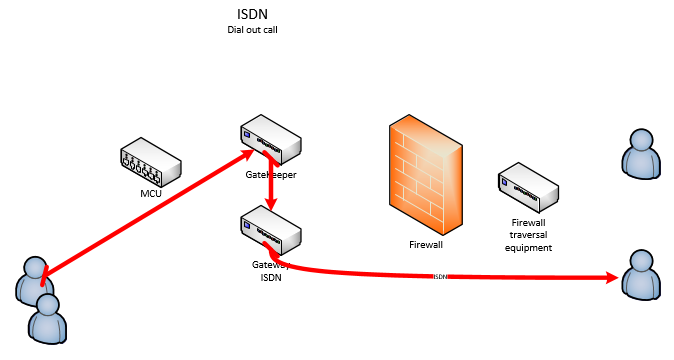
## Picture 3

The picture shows a schematic structure of an ISDN solution, where the external meeting participants dials in to another meeting participant, using an ISDN gateway.



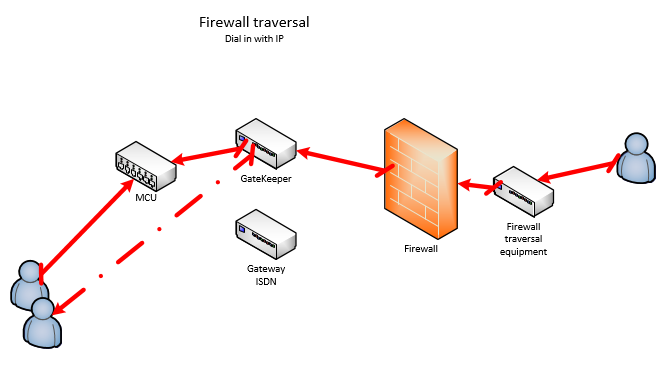
## Picture 4

The picture shows a schematic structure of an ISDN solution, where a meeting participants dials out, to another external meeting participant, using ISDN and a gateway.

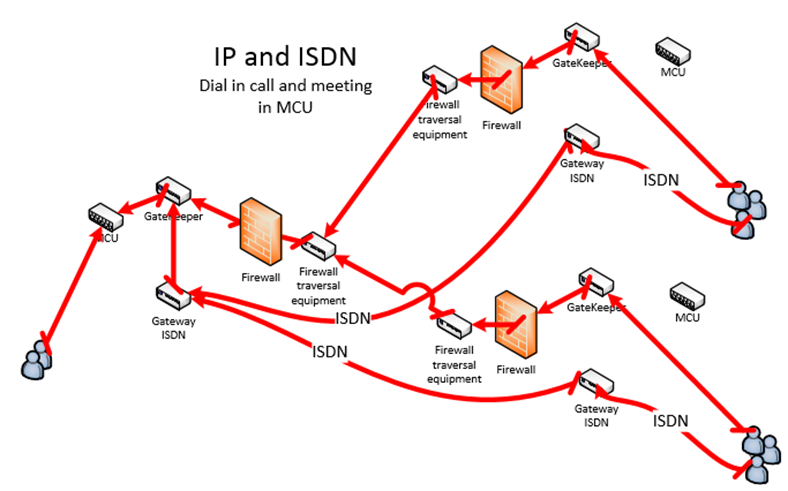


## Picture 5

The picture shows same schematic structure of firewall traversal solution as picture 1, where the meeting participants have agreed to meet in a virtual meeting room. In this case it is possible to dial directly in to the meeting participant. If the VC endpoint are placed in a court room this is not recommended. The presiding judge decides when the external meeting participant shall be connected to the courtroom, from a security point of view.

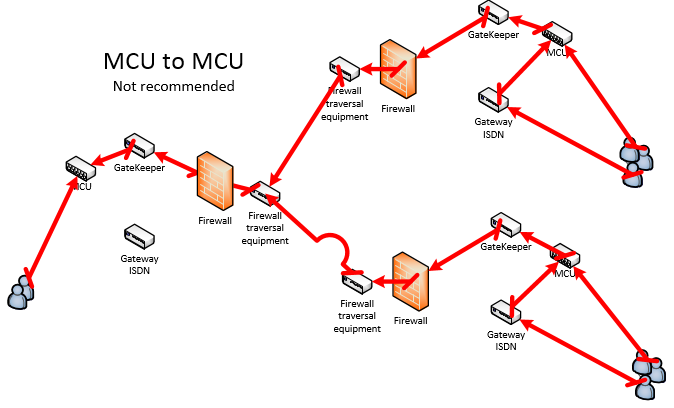


## Picture 6

The picture describes schematically how a solution might look like when several organizations meet in a virtual meeting room, in an MCU. All VC endpoint are dialling the meeting room. The room should be locked and a pin code must be entered in order to enter the meeting.

## Picture 7

Some Member States have set up their infrastructure in such a way that they are always dialling out through the MCU. Tests in WS2 have shown that this is often a problem when the dialled participant has a similar solution, with a MCU for incoming calls. We recommend that the MCU shouldn´t be used for outgoing calls, when dialling directly from a VC endpoint.



1. References

**Council of the European Union. 2015.** *Council Recommendations ‘Promoting the use of and sharing of best practices on cross-border videoconferencing in the area of justice in the Member States and at EU level’.* 31 July 2015. Official Journal of the European Union (2015/C 250/01).

**Council of the European Union: Working Party e-Law (e-Justice) - Expert Group on videoconferencing. 2015.** *Final Report - Informal Working Group on Cross-border Videoconferencing (plus appendices).* 02 March 2015. The "Informal Working Group on cross-boder videoconferencing" was the predecessor of the official "Working Party e-Law (e-Justice) - Expert Group on videoconferencing". Council document 8364/15.

**Council of the European Union: Working Party e-Law (e-Justice). 2016.** *Suggestions for best practices concerning videoconferencing with third countries.* 27 May 2016. Council document 9337/16.

**e-Justice Portal.** European e-Justice Portal. *Tools for courts and practitioners - Videoconferencing.* [Online] https://e-justice.europa.eu/content\_videoconferencing-69-en.do.

**ICAB – Barcelona Bar Association. 2016.** *Videoconferencing between inmates and lawyers (sheets presented in Tallinn).* 16 June 2016.

**Multi-aspect initiative to improve cross border videoconferencing - Work-stream 2 - D2.1. 2016.** *Overall Test Report.* November 2016.

**NL Ministry of Security and Justice. 2012.** *Implementing Transnational Use of Videoconferencing – True-to-Life Implementation – True-to-Life and Other Requirements.* 31 August 2012.

**Scottish Government. 2014.** *Video Conferencing Standards for the Scottish Public Sector.* June 2014.

**SNCA - Swedish National Court Administration. 2016.** *Room Function Programs (RFP) – Technical Requirements Court Rooms, Rumsfunktionsprogram Bygg/teknik Domstolsverket. Utgåva 3, 2013-11-13\_Rev D 2015-09-10. (sheets presented in Jönköping, June 2016).* Jönköping, Sweden : s.n., 06 2016.

**University of Western Sydney. 2013.** *Gateways to Justice: design and operational guidelines for remote participation in court proceedings.* 2013.

\*\*\* End of document \*\*\*