Multi-aspect initiative to improve   
cross-border videoconferencing  
"Handshake"

Work-stream 2

D2.1 Overall Test Report

Too often getting connected is not as easy as it should be

|  |  |
| --- | --- |
| Deliverable Id : | D2.1 |
| Deliverable Name : | Overall Test Report |
| Status : | Final version 1\_0 |
| Dissemination Level : | EU Commission and Member States |
| Due date of deliverable : | November 2016 |
| Actual submission date : | 31 January 2017 |
| Work-stream : | WS2 – Practical Testing of VC-connections |
| Project coordinator: | Austrian Federal Ministry of Justice Johann Kickinger, Robert Behr, Thomas Gottwald |
| Organisation name of lead partner for this deliverable : | Netherlands Ministry of Security and Justice |
| Author(s): | Peter J.A. van Rotterdam (NL) |
| Partner(s) contributing : | AT, CZ, EE, HR, IT, LV, NL, PL, SE, SI, UK-E&W, UK-S and Eurojust. |

Abstract:

*The main test objective was to get findings to enhance the technical interoperability for cross-border videoconferencing in the judicial domain. It was found that videoconferencing is easy to use but too often getting connected is not so easy. This is because Member States implement videoconferencing technology in different ways and therefore legal professionals still need substantial technical support. Sharing among Member States the best practices for technological, ergonomic and organisational aspects of cross-border videoconferencing is expected to improve its usability for legal professionals.*

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

The overall objective of WS2 Practical Testing of cross-border videoconferencing connections was to enhance the technical interoperability for videoconferencing. This objective has been achieved by:

1. doing practical videoconferencing connection tests between the participating Member States;
2. documenting the test results, especially working parameters to make a successful videoconferencing connection between the user’s videoconferencing facilities and;
3. by documenting practical hints and tips to prevent failures and make the connection work.

Tests have been executed between multiple pairs of participating Member States in different configurations. With 12 participating organisations from 11 Member States the maximum total number of possible bilateral tests was 66. In addition a few multilateral tests were completed. For each test the detailed test results have been documented in a Test Log. From each Test Log the main findings have been abstracted and combined in order to derive a number of ‘overall key findings’ that impact on the ease of connection and interoperability of cross-border videoconferencing.

In half of the tests connecting one judicial videoconferencing facility cross-border to another one was easy. They worked as planned whether two end user facilities connected to a multipoint control unit or where they connected directly to each other. However, in the other half of the tests a connection was not so straightforward. This was due to configurations in the national judicial network infrastructures (firewalls and other protective measures such as not allowing dialling out), rather than by the videoconferencing equipment itself. In these cases, getting connected is not as easy as it should be and legal professionals need technical support to start a videoconferencing session.

Once a connection was established, in many tests the quality of both the image and sound was good and functions (like mute/unmute) worked well. If interoperability was not good the cause was either technical, such as not enough bandwidth, or ergonomic, i.e. room conditions (e.g. lighting, acoustics and camera position) were not to the required standard. Also, in many tests it was not clear whether the videoconferencing session was encrypted end-to-end. If the connection was not (end-to-end) encrypted this was caused by configurations in the control devices and sometimes also with the end user facilities in the national judicial network infrastructures.

In addition to this document, Work-stream 3 deliverable D3 "Recommendations on the practical application of technical standards for cross-border videoconferencing" provides the practical hints and tips to prevent failures and make the connection work.

In conclusion the overall objective of WS2 Practical Testing of cross-border videoconferencing connections has been achieved. In the judicial domain, cross-border videoconferencing is easy to use but not as yet as easy as telephony, as in many cases legal professionals still need technical support to connect a videoconferencing facility. In the short term it is recommended that:

* technicians check if and how two videoconferencing facilities work together before they are actually used for a cross-border judicial proceeding;
* the key findings of the tests are used to help develop best practices for technological, ergonomic and organisational aspects of cross-border videoconferencing to improve the ease to connect and use videoconferencing facilities, so that legal professionals need less technical support.

These will help Member States to take advantage of the great potential of videoconferencing and be beneficial to the growing number of cross-border judicial proceedings in the European Union.

History

|  |  |  |  |
| --- | --- | --- | --- |
| *Version* | *Date* | *Changes made* | *Modified by* |
| A(1) | 31/05/2016 | very initial; discussed in Jönköping | Author |
| A(2) | 24/08/2016 | 1st draft; to be reviewed by partners | Author |
| A(3) | 19/10/2016 | 2nd draft; to be reviewed by partners | Author |
| A(4) | 27/10/2016 | 3rd draft; to be reviewed by partners | Author |
| A(5) | 04/11/2016 | 1st final draft; to be approved | Author |
| A(6) | 21/12/2016 | 2nd final draft; to be approved | Author |
| A | 30/12/2016 | final; to be submitted to EC | Author |
| B | 23/01/2017 | final; to be submitted to EC | Author |
| 1\_0 | 27/01/2017 | Final changes for submission to EC | Johann Kickinger |

Table of contents

[Executive Summary 2](#_Toc473302356)

[History 3](#_Toc473302357)

[Table of contents 4](#_Toc473302358)

[On this Document 5](#_Toc473302359)

[Multi-Aspect Initiative to Improve Cross-Border Videoconferencing 6](#_Toc473302360)

[Objectives 6](#_Toc473302361)

[Work-streams 6](#_Toc473302362)

[Document structure and interrelation 6](#_Toc473302363)

[User groups who will benefit from this project 8](#_Toc473302364)

[Alignment with the European e-Justice Action Plan 8](#_Toc473302365)

[Test Overview 9](#_Toc473302366)

[Context of the Tests 9](#_Toc473302367)

[Test Objectives 9](#_Toc473302368)

[Objects to be Tested 9](#_Toc473302369)

[Features to be Tested 9](#_Toc473302370)

[Participants 10](#_Toc473302371)

[Doing Practical VC Connection Tests 11](#_Toc473302372)

[Bilateral Tests 11](#_Toc473302373)

[Multilateral and Multi MCU Tests 13](#_Toc473302374)

[Documenting Test Results 14](#_Toc473302375)

[Test Documentation 14](#_Toc473302376)

[Conclusions from Tests 18](#_Toc473302377)

[Different Brands mean different Call Parameter Sequences 18](#_Toc473302378)

[Zero, one or even two MCUs between user’s videoconferencing facilities 18](#_Toc473302379)

[IP is default, ISDN is fall-back, Private Network Stability is essential 19](#_Toc473302380)

[High Video Resolution and Good Frame Rate are needed 19](#_Toc473302381)

[Bandwidth of 2 Mbit/s works well, Quality of Service is essential 19](#_Toc473302382)

[Encryption is default, but how to be sure that it is end-to-end? 20](#_Toc473302383)

[Videoconferencing integrated in the Court Room 20](#_Toc473302384)

[Room Conditions make or break the Quality of Image and Sound 20](#_Toc473302385)

[Organizational Issues to do Videoconferencing still exist 21](#_Toc473302386)

[Other technologies for Videoconferencing might also be considered 21](#_Toc473302387)

[List of Abbreviations 22](#_Toc473302388)

[List of References 26](#_Toc473302389)

[I. Appendix I - Template for Connectivity Details of VC Facility 27](#_Toc473302390)

[II. Appendix II - Test Procedure and Test Log 28](#_Toc473302391)

[III. Appendix III - Template for the Test Result and Relevant Events 29](#_Toc473302392)

[End of Document 31](#_Toc473302393)

# On this Document

This document is the Overall Test Report that summarizes the set of all results of all test sessions that have been executed according to the Test Plan[[1]](#footnote-1) for ‘Practical Testing of VC-connections’, being the 2nd work-stream (WS2) of the action ‘Multi-Aspect Initiative to Improve Cross-Border Videoconferencing’ (short name ‘Handshake’) as described in the Grant Agreement with number JUST/2014/JACC/AG/E-JU/6961.

The final version of this Overall Test Report is the main deliverable from WS2 ‘Practical Testing of VC-connections’. It is, like all deliverables of the action, to be submitted by the Federal Ministry of Justice of the Republic of Austria (the action’s applicant) to the European Commission, DG Justice, Directorate B: Criminal Justice.



# Multi-Aspect Initiative to Improve Cross-Border Videoconferencing

This section is an overview of the project "Multi-aspect initiative to improve cross-border videoconferencing" and provides the context in which this Overall Test Report was being produced.

## 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.

## 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 documents 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.  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. |

## 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 also the external VC partners of the courts and prosecution offices e.g. **witnesses, external experts, (vulnerable) victims, police, penitentiaries, lawyers, defense 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.

## 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 and 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.

# Test Overview

This section is derived from the Test Plan and summarizes the context, objectives and participants of WS2 ‘Practical Testing of VC-connections’ and specifies all test sessions that have been executed.

## Context of the Tests

The context of all test sessions is the action ‘Multi-Aspect Initiative to Improve Cross-Border Videoconferencing’ (Handshake); in this action all test activities are organized in the so-called 2nd work-stream: WS2 - ‘Practical Testing of VC-connections’.

## Test Objectives

The overall objective of WS2 ‘Practical Testing of Cross-border VC-connections' is to ’enhance the technical interoperability for videoconferencing’; this objective has been achieved by (1) doing practical VC connection tests between the participating Member States and (2) documenting the test-results, especially working parameters[[2]](#footnote-2) to make a successful VC-connection between the VC end points and (3) by documenting practical hints and tips to prevent failures and make the connection work.

## Objects to be Tested

Objects that have been tested are rooms where (1) judicial activities can take place and where (2) videoconferencing equipment is available; examples are court rooms, prosecutor hearing rooms and prison studios; some tests used regular meeting rooms.

## Features to be Tested

Features that have been tested are:

* Connectivity (here: ability to make a connection between two or more videoconferencing facilities in a network);
* Interoperability (here: capability of a videoconferencing facility to interact and function with other videoconferencing facilities reciprocally).

Features that also have been tested, but NOT in detail, are:

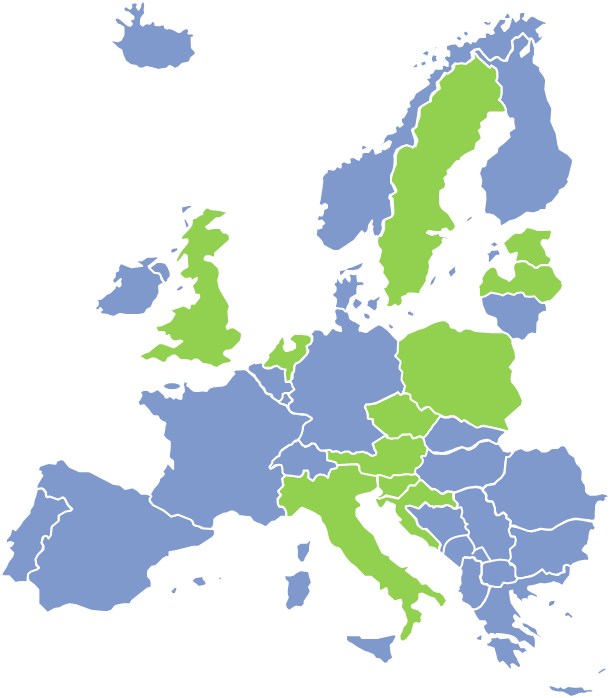
* Quality of Image;
* Quality of Sound.

The tests have been executed in different configurations depending on the technical capabilities of the objects that have been tested, e.g. IP or ISDN, bilateral (point-to-point) and multilateral (multipoint). Further details have been specified in the Test Logs.

## Participants

The participants of the test sessions are judicial authorities and/or technical staff from (and physically located in)

1. AT Austria Ministry of Justice;
2. CZ Czech Republic Ministry of Justice;
3. EE Estonia Centre of Registers and Information Systems;
4. HR Croatia Ministry of Justice;
5. IT Italy Ministry of Justice;
6. LV Latvia Court Administration;
7. NL Netherlands Ministry of Security and Justice;
8. PL Poland Ministry of Justice;
9. SE Sweden National Courts Administration;
10. SI Slovenia Ministry of Justice;
11. UK-E&W England & Wales Ministry of Justice;
12. UK-S Scotland Scottish Government;
13. Eurojust The European Union's Judicial Cooperation Unit.



# Doing Practical VC Connection Tests

This section summarizes the test sessions that have been executed.

## Bilateral Tests

Tests have been executed between multiple pairs of participating Member States in different configurations; with 12 participating organisations from 11 Member States the maximum total number of bilateral (point-to-point) tests is 66[[3]](#footnote-3) (see table below). In advance of its execution each test was planned, i.e. a date/time was agreed and the connectivity details of both videoconferencing facilities (see appendix I for the template) were exchanged between staff of both Member States.





**Table - Bilateral Tests planned and executed[[4]](#footnote-4)**

## Multilateral and Multi MCU Tests

A limited set of multilateral tests and so-called multi MCU[[5]](#footnote-5) tests (see the table below) has been executed:

* a test, where multiple Member States connected with one MCU provided by Eurojust;
* a test, where multiple Member States connected with one MCU provided by Austria;
* a test, where Austria and Eurojust connected (there multiple end points) via their two MCU’s;
* a test, where Sweden and Eurojust connected (there multiple end points) via their two MCU’s.



**Table - Multilateral and Multi MCU Tests planned and executed**

# Documenting Test Results

This section summarizes how the test sessions have been documented.

## Test Documentation

For each test:

* the date and time were agreed and the test was prepared by exchanging the Test Connectivity Details of the two (or more) VC facilities involved according to the template in appendix I;
* the Test Procedure (test script) was distributed to the two (or more) VC facilities involved according to the template in appendix II;
* the test results were documented directly after the test in a Test Log according to the template in appendix II and the template in appendix III; this Test Log was later agreed and finalized by the two (or more) VC facilities involved;
* from each Test Log findings have been abstracted and combined (see table below) such that key findings (see next chapter) have been derived that impact the ease of connection[[6]](#footnote-6) and interoperability of cross-border videoconferencing;









**Table – Findings abstracted from Test Logs**

# Conclusions from Tests

This section summarizes the conclusions or key findings based on all tests. Due to the focus on connectivity and interoperability most key findings are of a technical nature.

## Different Brands mean different Call Parameter Sequences

In order to connect a videoconferencing set to some other device the videoconferencing set has to call the other device. The other device has a ‘number’, usually consisting of a first part and a second part (‘extension number’) separated by a delimiter. Tests showed that it depends on the brands of both videoconferencing sets involved how to call the other device, i.e. whether to start the number with the first or second part and which delimiter (e.g. @ or # or ##) to use. In addition tests showed that some numbers could not be called because within the national videoconferencing infrastructure these (prefix-) numbers have been reserved for special purposes.

In addition: in order to connect a videoconferencing set to some other device the videoconferencing set internally uses a communication protocol, like H.323[[7]](#footnote-7) or SIP[[8]](#footnote-8). Tests showed that most videoconferencing devices support these state-of-the-art protocols. Whether a videoconferencing device supports a protocol is usually checked in the stage of acquiring videoconferencing devices and should never be a reason for not being able to connect.

## Zero, one or even two MCUs between user’s videoconferencing facilities

Tests showed that configurations with zero, one or even two MCUs were used to connect a videoconferencing facility in one MS to a videoconferencing facility in another MS:

1. connecting two videoconferencing facilities directly to each other, i.e. without an MCU in between is an option that is only possible if at least one of the videoconferencing facilities is allowed to accept incoming calls and the other is allowed to dial out. Tests showed this is not always the case, because one or even both MSs require the call to go via its MCU.
2. Connecting two videoconferencing facilities to an MCU, provided by one of the MSs, in between is an option that is only possible if both videoconferencing facilities are allowed to dial out. Tests showed that many MSs require inbound calls to go via their national MCU rather than directly to a videoconferencing facility to be accepted or not; this is perfectly OK. Tests also showed that some MSs do not allow videoconferencing facilities to dial out; this leads to ‘one-way-only’ connections, that is the connection can only be established by the MS that allows to dial out.
3. Test showed that connecting each videoconferencing facility to its national MCU and then connect both MCUs to each other gives undetermined results; this can only be avoided if both MCUs are carefully reconfigured, just for this one and only video session. So, using two MCUs leads at best to the need for work arounds and in worst cases to ‘no connection possible’.

Reasons for using MCUs in the ‘set up of national videoconferencing infrastructure’ as mentioned by MSs are (1) need for (perception of) security, (2) management control of call statistics, (3) set up was delivered as such by the provider and (4) no problems encountered insofar.

Tests showed that, besides impact on the ‘ease to connect’, the use of MCUs also has impact on the ability to interact with the other videoconferencing facility, such as the possibility to (cross-border) control cameras and mute microphones of the other facility, the use of encryption et cetera.

## IP is default, ISDN is fall-back, Private Network Stability is essential

Tests showed that most Member States use IP to connect their videoconferencing sets; some Member States are migrating from ISDN to IP; some Member States will keep ISDN alive as a fallback for IP. Note that ISDN is of much lower bandwidth than IP and therefore usually provides less quality of image and sound or even a lack of synchronization between image and sound (lack of lip-sync). Also ISDN has higher costs than IP.

When operating via IP, videoconferencing sets are connected via the private network to some device (including firewall traversal) to allow connecting via the Internet to other videoconferencing sets. If done properly, IP is as secure as ISDN. Some tests showed that unstable private networks have a very negative impact, such as losing connection, freezing images and/or staggering sound, on the videoconferencing session.

## High Video Resolution and Good Frame Rate are needed

The type of CODEC (and its parameter settings) defines the video resolution (number of vertical and horizontal lines of pixels) with which images are transmitted to the other end point or MCU and with which images are received from the other end point or MCU (note: resolution received may differ from resolution transmitted). Tests showed that most Member States use CODECs with high resolution (e.g. 1024 x 576 or higher). In some tests different video formats (4:3 versus 16:9 width-to-height ratio) needed adjustment of the camera parameter settings.

The type of CODEC (and its parameter settings) also defines the frame rate (times per second that images received and transmitted are refreshed to simulate continuous images). Tests showed that most Member States use CODECs with good frame rates of 25/sec or 30/sec.

## Bandwidth of 2 Mbit/s works well, Quality of Service is essential

In order to allow a good videoconferencing connection enough bandwidth must be available for the videoconferencing connection. How much bandwidth is needed depends on the amount of information (in terms of bits per second[[9]](#footnote-9)) to be exchanged. The amount of information to be transferred depends highly on the video resolution and frame rate used by the videoconferencing equipment. Tests showed that 384 kbit/s is an option to transport a low-resolution video with 352 x 288 pixel but is not enough to transport a HD video and may then lead to a frozen picture. 2 Mbit/s[[10]](#footnote-10) is in most cases well enough to transport a HD video with a resolution of 1280 x 720 pixel (HD 720p) with 25 or 30 frames per second which allows to achieve even excellent quality of image and sound.

In order to allow a good videoconferencing connection enough bandwidth must be available for the videoconferencing connection *all the time during the videoconferencing session*. That means that once the bandwidth is assigned to a videoconferencing session, this bandwidth should remain available during the whole session. This can be arranged in the private network of an organization or provider by using so-called Quality of Service for videoconferencing. Tests showed that if Quality of Service was not arranged the quality of image and sound can vary during the session in a way that is really disturbing the session. Note that Quality of Service is not available for the part of the connection over the public Internet; this, however, has not been an issue in day-to-day practice.

## Encryption is default, but how to be sure that it is end-to-end?

Tests showed that many videoconferencing sets (end point) were or can be configured to ‘auto’ encryption; that means that encryption is default and will always be used, unless the other end point cannot encrypt (‘best effort’). With an MCU in between the encryption is from the one end point to the MCU and then from the MCU to the other end point. In that situation some tests showed that the end point displays encryption, while only one of both parts was really encrypted. Knowing that signals transmitted and received are end-to-end encrypted or not is very important to legal professionals. It depends per judicial proceeding if encryption is required.

Now some key findings of an ergonomic nature follow.

## Videoconferencing integrated in the Court Room

Practice shows that many (court) rooms used for videoconferencing are also used for ‘traditional’ proceedings. Also many (court) rooms have digital facilities, such as showing objects, documents, videos, data etc. via PC and/or document cameras. That means that the way videoconferencing is integrated in the (court) room determines the ease of use all technology in the (court) room.

When presenting (1) more than one person in close up or (2) part of the court room and a document or computer screen shot, the screen image may consist of more than one picture (so-called picture-in-picture or dual presentation) rather than (choosing) just one big picture of the court room, or a person or a document or screen shot. Tests showed that some Member States have equipment (pre-programmed) for picture-in-picture or additional screens, others do not have that important feature.

## Room Conditions make or break the Quality of Image and Sound

Tests showed that room conditions, like the room size, the use of windows and blinds, the lights and colours in the room, how sounds are dispersed and other acoustic features, the position of chairs and tables versus the videoconferencing equipment et cetera can make or break the quality of the interaction during a videoconferencing session. Especially for large traditional court rooms the implementation of videoconferencing is very complex and needs a very good design. Tests showed:

* switching ceiling lights on or off and keeping daylight out of a videoconferencing facility had a great impact on the image as seen by the other videoconferencing facility;
* large rooms with high ceilings and no sound absorption and loudspeakers with too high volume created echoing; also directional microphones producing only the sound of the person speaking and the need for headphones[[11]](#footnote-11) to get a good sound showed the need for good sound;
* simulating eye contact between persons in the one and persons in the other (court) room is very important for the interaction (body language) between all persons in the videoconferencing session. However, good eye contact could not always be achieved because in one of rooms the camera(s) were not positioned (as close as possible) to the middle of the screen(s) and the position of the screen did not relate properly to the size.

These are all aspects that limit the natural look and feel as if in a real (court) room. Tests showed that these ergonomic features were not always implemented carefully.

As a result of the process to get the tests done there is one finding of an organizational nature.

## Organizational Issues to do Videoconferencing still exist

In requesting a videoconferencing session with another Member State you need to know who to contact. Some tests showed that in some occasions it was hard to find the right person to get things done. Tests also showed that planning the tests (that is finding an agreed date/time, reserving the videoconferencing facilities and, if appropriate, arranging technical staff) takes much more elapsed time than the test (or in real live the proceeding) itself.

Finally two remarks rather than key findings conclude this section.

## Other technologies for Videoconferencing might also be considered

Legal professionals determine the user requirements (in terms of the quality of image and sound, the look and feel of being as if in one room, the ease of operation etc.) to get a good human interaction. These user requirements might differ per type of legal case: some cases involve more participants and/or are more emotional (body language!) than others. It was noted that this may lead to high-end (true-to-life) videoconferencing solutions. It is good to know that cheaper standard-conformant technology[[12]](#footnote-12) becomes available, such as videoconferencing software, like ‘Jabber’ for PCs or even for smart-phones and they can also be useful for a subset of legal procedures. Also new data communication technology, such as IPv6, will have its impact on the use of videoconferencing.

Recommendations are the next step

Work-stream 3 delivers practical hints and tips to prevent failures and make the connection work.

List of Abbreviations

| *Acronym* | *Explanation* |
| --- | --- |
| AVIDICUS | AVIDICUS 3 is an EU funded project running from 2013 to 2015, focusesing 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

List of References

Council of the European Union. (2015, July 31). 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’.

Council of the European Union: Working Party e-Law (e-Justice) - Expert Group on videoconferencing. (2015, March 02). Final Report - Informal Working Group on Cross-border Videoconferencing (plus appendices).

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

e-Justice Portal. (n.d.). *European e-Justice Portal*. (E. C. States, Editor) Retrieved October 2016, from Tools for courts and practitioners - Videoconferencing: https://e-justice.europa.eu/content\_videoconferencing-69-en.do

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

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

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

Scottish Government. (2014, June). Video Conferencing Standards for the Scottish Public Sector. UK (Scotland).

SNCA - Swedish National Court Administration. (2016, 06). 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.

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

1. Appendix I - Template for Connectivity Details of VC Facility

|  |  |
| --- | --- |
| **System management** | **VC Facility Dordrecht** |
| System manager name: | **Peter J.A. van Rotterdam** |
| Phone: | **+31-6-37170157** |
| Mobile: | **+31-6-37170157** |
| Fax: | **n/a** |
| E-mail: | [**pjavanrotterdam@quicknet.nl**](mailto:pjavanrotterdam@quicknet.nl) |
| Authority: | **Regional Court of Dordrecht** |
| Department: | **Facilities / IT** |
| Address: | **Steegoversloot 36** |
| City: | **Dordrecht** |
| Postal code: | **3311 PP** |
| Country: | **The Netherlands** |

|  |  |
| --- | --- |
| **Site information** |  |
| Location of hearing room: | **Court Room Wantijzaal** |
| Local time zone: | **Central European Time** |
| Phone in/near hearing room: | **+31 ?????????** |
| Fax in/near hearing room: | **+31 ?????????** |

|  |  |
| --- | --- |
| **Technical information** |  |
| Video system: | **Cisco** |
| Model/type: | **TB3000** |
| Software version: | **n/a** |
| IP address: | **n/a (via central unit in NL)** |
| Maximum transmission rate (IP): | **2 Mb/s SDSL** |
| ISDN number(s): | **n/a** |
| Maximum transmission rate (ISDN): | **n/a** |

|  |  |
| --- | --- |
| **Meeting test session** |  |
| Preferred date: | **Friday 18 December 2015 at 09.15-09.45 (NL time) = 08.15-08.45 (UK time)** |
| Alternative: | **n/a** |

|  |  |
| --- | --- |
| **Remarks:** |  |
|  | **Purpose: Connectivity Test with …** |

1. Appendix II - Test Procedure and Test Log

This appendix contains the steps of the Test Procedure and by that the Test Log to be completed with the chronological record of relevant details about the execution of the test

(\*) use tick-boxes for remarks that are relevant to copy into the Test Report.

|  |  |  |  |
| --- | --- | --- | --- |
| **TimeStamp** | **Steps in Test Procedure** | **Remark** | **(\*)** |
|  | MS1 connects to MS2  (choose IP or ISDN as appropriate) |  |  |
| *Welcoming Step* | | | |
|  | One by one all participants specify their name and function and talk a bit to get familiar with this VC session. Please write down remarks you wish. |  |  |
| *Operation – Steps to be done by VC Facility of MS1* | | | |
|  | Mute Microphone(s) |  |  |
|  | Unmute Microphone(s) |  |  |
|  | Pan, Tilt and Zoom Camera(s) |  |  |
|  | Show Object on Doc.Camera(s) |  |  |
|  | Show Document from PC(s) |  |  |
|  | Switch light(s) off and on |  |  |
|  | Dim light(s) |  |  |
|  | Close/open blind(s) and/or curtain(s) |  |  |
|  | Move papers near microphone(s) |  |  |
|  | Place papers over microphone(s) |  |  |
|  | Make noise away from microphone(s) |  |  |
|  | Open/close door(s) / window(s) |  |  |
|  | Clap hands |  |  |
|  | .. |  |  |
|  | .. |  |  |
| *Closing Step - Measure Working Parameters* | | | |
|  | IP or ISDN  H.263 or H.264  video frame rate  video pixel resolution  Bandwidth (Kb/s or Mb/s)  Latency (msec)  Jitter (yes/no)  Package loss (percentage)  Encryption (yes/no; type of encr.)  .. |  |  |
|  | MS1 disconnects from MS2 |  |  |

1. Appendix III - Template for the Test Result and Relevant Events

This two-page appendix contains for each test to be executed the template for the test result and for documenting any event during the testing process that is relevant to report.

**Test Result Operation**

Each participant expresses his/her findings on operation as below:

*OPERATION*

|  |  |
| --- | --- |
| From my perspective it is my opinion that for the room I was in, that … | Score |
| I (my staff) could switch on the system within 1 minute | Y/N |
| I (my staff) could set up the system according to its type of use within 1 m. | Y/N |
| I (my staff) could disconnect from the other location within 1 minute | Y/N |
| I (my staff) could switch off the system within 1 minute | Y/N |
| I (my staff) could use the mute function | Y/N |
| I (my staff) could use the volume control function | Y/N |
| I (my staff) know who and how to contact in case of technical problems | Y/N |
| the system is vandalism-resistant | Y/N |

**Test Result Image and Sound**

Each participant expresses his/her findings on ‘image and sound’ as below:

* Excellent – clear picture and clear audio with no problems noticed;
* Sufficient – some (minor) problems noticed, but the session could be practically used
* Poor – major problems noticed, that really affected practical usability of session
* Very Bad – problems hindered session to be established or session totally unusable.

*IMAGE AND SOUND*

I found the image and sound quality

|  |  |  |  |
| --- | --- | --- | --- |
| Very Bad | Poor | Sufficient | Excellent |
|  |  |  |  |
| Explanation | | | |

**Relevant Events**

Remarks from the Test Log that are relevant to report are further amplified below.

|  |  |  |  |
| --- | --- | --- | --- |
| **TimeStamp** | **Step in Test Procedure** | **Remark** | **(\*)** |
|  |  |  |  |
| **Amplification:** | | | |
|  |  |  |  |
| **Amplification:** | | | |
|  |  |  |  |
| **Amplification:** | | | |
|  |  |  |  |
| **Amplification:** | | | |

End of Document

The final version of this document has been added to the action’s archive.

1. Multi-Aspect Initiative to Improve Cross-Border Videoconferencing - WS2 - Practical Testing of VC-connections - Test Plan, version A, 20160208. [↑](#footnote-ref-1)
2. The working parameters have been specified in the Test Procedure (i.e. Measure Working Parameters) and are of a technical nature (like IP/ISDN, ITU standard H.263/H.264, video frame rate, video resolution, bandwidth, latency, delay, jitter, package loss, encryption) rather than of an ergonomic nature (like eye-contact, lip sync). [↑](#footnote-ref-2)
3. With 12 test participants the number of bilateral (point-to-point) tests is 12 x 11 / 2 = 66; each test will be split into two subtests: from point 1 to point 2 and the vice versa subtest; so the number of subtests is 132. [↑](#footnote-ref-3)
4. Not all 66 tests are done; 11 tests not done due to limited contribution by associate partners from Latvia and Scotland; 1 other test not done. Additional to originally planned 2 tests done. In total 56 bilateral tests are done. Out of 56 Test Logs 42 are final, i.e. both test parties have agreed their Test Log. 12 Test Logs are not (yet) final. [↑](#footnote-ref-4)
5. A multipoint control unit (MCU) is a device which can connect several VC endpoints into one videoconference [↑](#footnote-ref-5)
6. Connectivity has been valued as (1) ‘easy’, if the connection was established the first time right (as planned), as (2) one way only, if the connection could not be established by one MS calling the other and could only be established by the other MS calling, and (3) workaround needed, if the connection could not be established at all and technical staff had to find out a work around varying from changing some parameter settings up to and including going to another VC Facility. [↑](#footnote-ref-6)
7. H.323 is a recommendation from the ITU Telecommunication Standardization Sector (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. [↑](#footnote-ref-7)
8. The Session Initiation Protocol (SIP) is a communications protocol for signalling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol (IP) networks. [↑](#footnote-ref-8)
9. When measuring the working parameters at the end of a test, some tests showed that the signal received by one end point was not equal to the signal transmitted by the other end point; and some tests showed that for an end point the working parameters for transmitting signals were not equal to working parameters for receiving signals. [↑](#footnote-ref-9)
10. Here 2 Mbit/s is mentioned rather than 1.5 Mbit/s, because (1) tests indicated that 2.0 M bit/s gives a better chance to get excellent quality of image and sound than 1.5 Mbit/s and (2) real-world court hearings might require more bits to be transmitted (more activity in rooms, more cameras used, et cetera) than the low complexity test situations. [↑](#footnote-ref-10)
11. Using headphones for people with hearing problems is of course as natural as in traditional court proceedings. [↑](#footnote-ref-11)
12. The problem with technologies like Microsoft Skype or Skype for Business and other proprietary VC solutions is that they do not conform to the international VC standards and therefore require complicated and expensive gateway solutions to have them integrated. [↑](#footnote-ref-12)