Council of the European Union

Brussels, 27 March 2025
(OR. en)

7383/25

LIMITE

EJUSTICE 16
JAI 369
COPEN 65
EVAL 2
CATS 11

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	14560/24; 6860/25
Subject:	Videoconferencing in the judicial context - Member State's comments

Delegations will find in the Annex the replies of the Member States to the questions of the Presidency on videoconferencing in the judicial context., as indicated in document 6860/25.

ANNEX

Contents

CZECH REPUBLIK

Question 1 on statistics:

The estimated proportion lies between 2% and 3%, with 5% reflecting a highly speculative ceiling, included only for illustrative purposes under the most generous assumptions. I'm attaching an analysis explaining how we got these estimates.

Question 2 on interoperability of systems in the Member States:

In accordance with the Guide on Videoconferencing in Cross-Border Proceedings, the following standards are utilized:

Video:

- H.323 Standard for Video over Internet

Picture and Audio:

- H.263 and H.264
- Echo cancellation microphones (currently, courts are equipped with 454 units and 102 AEC units)

Channels, Bandwidth, and Bridging:

- SIP protocol with TLS encryption (note: this is not covered in the Guide on Videoconferencing)

Question 3 on the methods of proof of identity used by individual MS

Videoconferencing in civil and commercial matters:

Section 102a of the Civil Procedure Code - Use of Video Conferencing Equipment:

2) A hearing may be conducted via video conferencing only if the identity of the person concerned is properly verified. In the case of an examination, special care must be taken to ensure that the person being examined is not in a location where they may be subjected to improper influence.

Identity verification is carried out by showing an identity card to the camera or a document reader. Additionally, it is required to show the entire room to the camera, and throughout the meeting, the camera must be directed at the door to monitor the entrance to the room.

Videoconferencing in criminal matters

How the suspect, accused, convicted or affected person is identified and authenticated?

The identification is made by using official evidence of identification (ID cards, other document the certifies the identity). These documents usually are shown to the camera or verified by an employee of the court, the public prosecutor's office, the chief prosecutor, the head of prison or a member of the police authority.

GERMANY

We confirm that the four use cases for remote identification of participant in a video-hearing, listed in WK 2154/25 (visual recognition, digital identification, trusted third party and self-identification), cover all instances.

- **Question 1 on statistics:**

  What is the proportion, in percentage, of judicial hearing held by videoconference in your country:

  i. in a domestic context, in civil and commercial matters,

  ii. in a domestic context, in criminal justice proceedings?

  iii.. in a cross-border context in civil and commercial matters?

  iv. in a cross-border context, in criminal proceedings?

  In the absence of detailed statistical data, please indicate the estimated value.

- **Reply:**

  - i,iii: The decentralised competencies for the provision of videoconferencing services, with downstream instructions at the level of the relevant justice administrations (federal ministry of justice, ministries of justice at Länder level, higher regional courts, regional courts, local courts), renders the collection of information on a national level difficult. There is no representative and reliable data collection on the exact number of remote hearings in recent years. According to a survey conducted by the German Association of Judges among the 24 higher regional courts more than 50,000 remote hearings were carried out nationwide in the COVID year of 2021, the majority were civil proceedings.

- **Question 2 on interoperability of systems in the Member States:**

  – What are the technical standards for cross-border videoconferencing applied in your country?

– Taking into consideration the Guide on videoconferencing in cross-border proceedings issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?

- **Reply:**

  - There are no legal provisions on technical standards for cross-border video conferencing. Also, the statutory provisions of national procedural laws do not expressly set minimum standards for the technology, and jurisprudence is still developing. But a general understanding has evolved that the technology used must allow for all participants of a court hearing to be able to see and hear every other participant, albeit not necessarily everyone at the same time. This results in a minimum requirement regarding the number and fields of vision of the cameras employed.

- **Question 3 on the methods of proof of identity used by individual Member States**

– What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?

– Indicate if different methods are used in criminal proceedings and civil and commercial matters

- **Reply:**

  - No specific rules laid down in legal provisions;

  - The level of identification of the parties connecting remotely corresponds to the requirements in physical hearings. In physical hearings, no formal identification procedure is foreseen for the parties and their representatives, nor for other participants like witnesses. In the rare cases in which doubts arise about the identity of a participant, this can be verified - both in person and online – e.g. by showing an identity card (methods: visual identification/self-identification); the same method is used in civil and criminal matters.

IRELAND

The four use cases for remote identification listed in WK 2154/25 cover all instances in Ireland.

Question 1 on statistics

What is the proportion, in percentage, of judicial hearing held by videoconference in your country :

i. in a domestic context, in civil and commercial matters,

ii. in a domestic context, in criminal justice proceedings ?

iii.. in a cross-border context in civil and commercial matters?

iv. in a cross border context, in criminal proceedings ? In the absence of detailed statistical data, please indicate the estimated value.

Judicial hearing by videoconference in Ireland is only used in certain circumstances. The vast majority of domestic cases (both civil and criminal) are held in-person in a courtroom where justice can be seen to done. During the Covid-19 pandemic, many cases moved fully online and the rollout of more technology-enabled courtrooms has meant these are now being utilised more than was previously the case. That being said, criminal trials are still conducted physically.

Statistics in the above (i-iv) cases are not currently available. The Courts Service Annual Report 2023 does, however, mention that there were over 20,000 video-link calls between the Courts and the Irish Prison Service. In 2020, the types of hearings in criminal matters to be given via video link was expanded to include arraignments (where an accused is asked to enter a plea), return for trial, sentencing hearings and certain hearings in relation to extradition.

Question 2 on interoperability of systems in the Member States:

– *What are the technical standards for cross-border videoconferencing applied in your country?*

The remote hearing will take place via the video conferencing technology used by the Courts Service, Pexip VMR (virtual meeting room). In advance of the hearing, all participants will be provided with log in details to the Pexip VMR which allows them to enter the remote hearing.

Software

A VMR is set up for the purpose of each court sitting. The VMR connection details are made available to the legal representatives in each individual case in advance of hearings. The connection details for High Court Lists are available to practitioners through the members' area of websites of the Law Society and Bar of Ireland. The virtual courtroom is provisioned to facilitate connection from a laptop, PC or tablet using an array of internet browsers. Chrome is the recommended browser. Whatever device is used a camera and microphone will be required. The virtual courtroom also supports connection from traditional video conferencing endpoints, Skype for Business and an assortment of available video technologies. In addition, connection is also available for PCs and tablets using the dedicated Pexip App. The Pexip App can be download from https://www.pexip.com/apps or for tablets available via Google Play and Apple App Stores. An attendee at a virtual courtroom may need local IT assistance where the laptop or desktop administration is restricted by an organisation's IT department. Participants should ensure that their internet connection for the virtual courtroom is strong, stable and meets the requirements specified below.

A stable internet connection is key to achieving a successful video call and avoiding disruption.

Attendees are encouraged to test their internet connection in advance. The assigned virtual courtroom will be opened 10 minutes in advance and you may use the connection detail to test your access prior to the sitting. If you are not able to connect to Pexip, please inform the relevant Court Registrar. The virtual courtroom will close following completion of the sitting. Practical Guide Remote Hearings Ensure all applications on your laptop or device are closed, apart from your video stream. Additional applications may interfere with the quality of your video call and access to the virtual courtroom. If using a tablet, ensure that an incoming call does not automatically override the connection to the VMR.

Access via dedicated Video conferencing rooms and/or Skype for Business

Parties can join a Pexip VMR session from a dedicated video conferencing room with video conferencing end-points by using the video System SIP/H.323 address provided by the Registrar in the VMR connection details. Alternatively, Skype for Business users can connect to the VMR using the MS Skype4B code provided by the Registrar in the VMR connection details.

Non-Courts Service Software

Alternative software that is compatible with the Courts Service Technical Courts infrastructure may also be used subject to the agreement of all parties and approval by the Court. Such alternative options will involve a cost burden to be borne by the parties and whilst the Courts Service will provide details to access, it will be the responsibility of the approved provider to support access. In the event that technology other than the Courts Service provided VMRs is being used, parties should engage with the Courts Service in advance of the selection of any alternative platform to confirm hardware/software compatibility and requirements. In this case, the judge and registrar would need to be provided with the relevant hardware to facilitate the hearing with all necessary software installed, if this is not readily available to them.

Hardware

The Courts Service has stipulated the following minimum hardware requirements for participants in remote hearings:

a) 2.0-Ghz dual-core Intel Core i5 or later;

b) 4 GB of RAM free physical 2GB; and

c) Free disk space of 1GB or more.

A camera and microphone are also required, and it is advisable that participants to any remote hearing dealing with a substantive matter where it is likely the court's attention will be brought to particular documents, would have access to two screens, one for the VMR and a second to view the electronic documents for hearing. Experience has shown that one large screen (24 or 27 inch) can also work effectively by arranging the windows with the VMR session and documents side by side.

Internet Connection

One of the pre-requisites for a successful remote hearing is a stable internet connection. If any participant to a case does not have a sufficiently stable internet connection, then a remote hearing simply cannot take place (at least until such connectivity issues are resolved). The Courts Service has stipulated the following minimum network bandwidth requirements for participants to ensure video quality during remote hearings:

a) High - 1280 kbps (HD)

b) Med - 768 kpbs (SD)

c) Low - 384 kpbs (SD)

Where participants have poor Wi-Fi, the following should be considered:

a) a wired connection into a home router device

b) a USB dongle to connect to a 4G network

c) a mobile phone used as a personal hotspot connecting to a 4G network

d) A secure wired internet connection is preferable. Internet connectivity to the VMR should be tested in advance of hearing.

e) If working on a home connection with a number of users, ensure that the connection is sufficient to ensure smooth running of the technology or, ask other users to refrain from using same for the duration of the hearing.

– *Taking into consideration the Guide on videoconferencing in cross-border proceedings issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?*

Question 3 on the methods of proof of identity used by individual Member States

– *What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?*

The most commonly used method is number one, 'visual recognition'. There is no legal provisions in this area. The Courts service have guidelines and rules on their website as to how proof of identity can be ascertained and often it vary from court to court and judge to judge.

– *Indicate if different methods are used in criminal proceedings and civil and commercial matters*

The methods used are the same.

GREECE

Reply to the Questions of st06860/25

1. Confirm whether the four use cases for remote identification of participant in a video-hearing, listed in WK 2154/25, cover all instances in the Member States
   We confirm that the four use cases for remote identification of participant in a video-hearing, listed in WK 2154/25, cover all instances in Greece, since we mainly use the Third identification use case: trusted third party.

2. Clarifying questions on the use of VTC in a judicial context

Question 1 on statistics

What is the proportion, in percentage, of judicial hearing held by videoconference in your country :

i) in a domestic context, in civil and commercial matters,

ii) in a domestic context, in criminal justice proceedings ?

iii) in a cross-border context in civil and commercial matters?

iv) in a cross border context, in criminal proceedings ?

In the absence of detailed statistical data, please indicate the estimated value.

There is no data yet, since the legislation for the judicial videoconference is in place since 10/3/2025.

Question 2 on interoperability of systems in the Member States:

– What are the technical standards for cross-border videoconferencing applied in your country?

The main videoconferencing tools/platforms we use are the following:

- Cisco Webex Room Kit Plus
- Cisco Webex Room Kit

The aforementioned VC platforms used, comply with all the latest technical standards and the EU Guidelines (eg EU Council's Guide on videoconferencing in cross-border proceedings).

– Taking into consideration the *Guide on videoconferencing in cross-border proceedings* issued by the Council (https://www.consilium.europa.eu/media/30606/ qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?

Furthermore to our reply to the previous question, we have to notice that according to relative national legislation, in order for someone to participate to a court hearing in Greece by videoconferencing, he/she can connect ONLY through **certified places** (court rooms, prisons, and consulates). This ensures, among other issues, that there will be no incompatibility issues between different VC systems.

In more detail, in the case that a person outside Greece, needs to participate to a Greek court hearing via videoconferencing, he has to move to a nearby Greek Consulate and the court will arrange to organize a VC session and send a link to the Consulate's officials, in order to be able to connect to the hearing.

Question 3 on the methods of proof of identity used by individual Member States

– What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?

In Greece, we mainly use the Third identification use case: trusted third party.

– Indicate if different methods are used in criminal proceedings and civil and commercial matters.

No, we use the same method, i.e. the Third identification use case: trusted third party.

SPAIN

Question 1 on statistics

What is the proportion, in percentage, of judicial hearing held by videoconference in your country :

i. in a domestic context, in civil and commercial matters,

ii. in a domestic context, in criminal justice proceedings ?

iii.. in a cross-border context in civil and commercial matters?

iv. in a cross border context, in criminal proceedings ?

In the absence of detailed statistical data, please indicate the estimated value.

In Spain, there are no statistics with distinction between domestic or cross-border context. For the period 2020-2025, here are the statistics for judicial hearings held by VC:

– Ministry territory (*), criminal proceedings: 43.6%

– Ministry territory, civil and commercial proceedings: 48 %

– Transferred regions, criminal proceedings: 42.1%

– Transferred regions, civil and commercial proceedings: 47.9 %

(*) Meaning: in the territory covered by the regions which have not taken over competences in the field of justice

Question 2 on interoperability of systems in the Member States:

– What are the technical standards for cross-border videoconferencing applied in your country?

The technical standards are H.323 and SIP.

– Taking into consideration the *Guide on videoconferencing in cross-border proceedings* issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?

SIP protocol should be the preference of use, but H.323 is still widely used for VC.

Question 3 on the methods of proof of identity used by individual Member States

– What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?

In Spain, the only method used for proof of identity is visual recognition with the participants showing their ID during the hearing.

– Indicate if different methods are used in criminal proceedings and civil and commercial matters.

There are no different methods between criminal proceedings and civil and commercial proceedings.

FRANCE[1]

Dans la continuité des travaux du groupe E-justice du 24 janvier dernier, la Présidence polonaise souhaite recueillir les commentaires écrits des autorités françaises sur deux points :

– les cas d'utilisation pour l'identification des participants à une vidéo-audience (WK 731/25 paragraphe 13 à 20 du document)

– les questions sur le projet de cartographie des systèmes de visioconférence (WK942/25 – page 68 à 80 du document)

I. La position des autorités françaises sur l'identification des participants à une vidéo-audience

La présidence polonaise, dans le document de travail soumis, vient répertorier trois cas d'identification des participants :

1. **La reconnaissance visuelle** (§15,16 et 17), s'appuyant sur le principe de confiance mutuelle entre les autorités parties prenantes au dispositif, et par la transmission d'une photo d'un document d'identité (transmise en amont de la vidéo-audience), également de bonnes conditions techniques (bandes passantes et lumière) devront être anticipée dans la participation à distance par visioconférence.

2. **L'identification numérique** (§18) qui se traduit par l'utilisation d'une vérification en ligne de l'identité des participants (ex : système similaire au EU Login) pouvant nécessiter au préalable la création d'un compte utilisateur.

3. **L'identification par un tiers de confiance** (§19, 20), pouvant être mobilisée en cas d'incertitude sur la sécurité juridique des deux dispositifs d'identification précités.

La présidence soumet un **quatrième cas d'identification**, non référencé dans le document de travail, qui consiste en l**a simple déclaration de l'identité du participant.**

[1] It should be noted that these answers were provided based on previous versions of the questionnaire of the Presidency.

Eléments de position :

Les autorités françaises n'ont pas identifié de modes alternatifs supplémentaires de vérification de l'identité des personnes entendues en vidéo-audiences en ce qui relève de la procédure civile.

Courtesy translation :

The French authorities have not identified any additional alternative methods of verifying identity of persons in video hearings for civil proceedings.

II. La position des autorités françaises sur le projet de cartographie portant sur les outils de visioconférence

La présidence polonaise souhaite mettre en place une cartographie des systèmes de visioconférence, pour initier ses travaux elle s'appuie sur les retours des 20 Etats membres ayant répondu à l'enquête dédiée à l'utilisation de la vidéoconférence dans le domaine de la justice dont les retours sur les principales thématiques sont répertoriés dans le document de travail (diapositive 71 à 74). La présidence polonaise souhaite disposer d'éléments de compréhension additionnel dans l'optique de lancer une nouvelle enquête sur ce sujet.

Eléments de position :

<u>Question 1 portant sur les statistiques :</u>

Quelle est la fréquence des vidéoconférences organisées par votre pays suivant le mode :

a) National :

b) Transfrontalier :

Depuis la crise sanitaire liée à l'épidémie de COVID-19, le recours à la vidéoconférence en matière civile a considérablement augmenté.

Ainsi, les autorités françaises recensent un total (toutes juridictions confondues, procédures nationales et transfrontières) de 7 277 vidéoconférences en 2020 et de 11 854 vidéoconférences en 2023, ainsi que près de 14 446 vidéoconférences en 2024 (données provisoires et non consolidées à ce jour).

Ces données sont certainement sous-estimées, dès lors que le taux de réponse moyen des juridictions se situe entre 85 % et 95 %. Elles peuvent s'expliquer par la progressive acculturation des juridictions à l'usage de la vidéoconférence dans la réalisation des activités judiciaires.

En l'absence de données statistiques détaillées pour la gamme ci-dessus, veuillez indiquer la valeur estimée.

Courtesy translation

<u>Question 1 on statistics</u>

What is the scale of videoconferencing organized by your country in the mode:

a) Domestic

b) Cross-border

In the absence of detailed statistical data from the above range, please indicate the estimated value

Since the health crisis linked to the COVID-19 epidemic, the use of videoconferencing in civil cases has increased considerably.

A total of 7,277 videoconferences in 2020, 11,854 videoconferences in 2023 and almost 14,446 videoconferences in 2024 (provisional and unconsolidated data to date) were recorded by the French authorities (all jurisdictions combined, national and cross-border proceedings).

These figures are certainly underestimated, given that the average response rate from courts is between 85% and 95%. They may be related to the gradual acculturation of courts to the use of videoconferencing in judicial activities.

Question 2 portant sur les problèmes d'interopérabilité des systèmes dans les États membres :

Les systèmes de vidéoconférence dans votre pays sont-ils basés sur des solutions cloud, par exemple Cisco Webex, Zoom, Microsoft Teams, tout en équipant les salles d'audience de solutions de vidéoconférence simples (par exemple, une caméra intégrée dans un pont) ?

Le ministère de la justice utilise un système de visioconférence hébergé dans ses datacenters. La solution utilise les standards du marché et interconnectable avec Webex, zoom (à l'exception de Microsoft Teams/Skype) ou tout système utilisant les standards.

Courtesy translation

Question 2 on problems in the area od interoperability of systems in the Member States

Have videoconferencing systems in your country been based on cloud solutions, ie Cisco Webex, Zoom, Microsoft Teams, While equipping courtrooms with simple videoconferencing solutions (e.g bridge-integrated camera)?

The Ministry of Justice uses a videoconferencing system hosted in its data centres. The solution uses market standards and can be interconnected with Webex, zoom (with the exception of Microsoft Teams/Skype) or any other system using the standards.

Questions 3 et 4 portants sur les problèmes d'interopérabilité des systèmes dans les Etats Membres :

- **Quelle norme existe-t-il pour la vidéoconférence transfrontalière dans votre pays ?**
- **Selon vous, suivant quelle norme cette connexion devrait-elle avoir lieu ?**

Pour les connections avec l'extérieur, notre plateforme permet les connections entrantes et sortantes avec l'ensemble des protocoles suivants (standards audio/vidéo) :

- **Supported protocols : H.323 ; SIP ; WebRTC**
- **Audioc codecs:**
- **• G.711(a/μ)**

- **• G.722**
- **• G.722.1, G.722.1 Annex C (SIP only) (licensed from Polycom®)**
- **• Siren7™, Siren14™ (licensed from Polycom®)**
- **• G.729, G.729A, G.729B**
- **• Opus**
- **• Speex**
- **• AAC-LC**
- **Video codecs:**
- **• H.261**
- **• H.263, H.263+**
- **• H.264 AVC**
- **• H.264 SVC**
- **• VP8**
- **• VP9 (for connections to Conferencing Nodes with processors using AVX2 or later)**
- **Content sharing:**
- **• H.239 (for H.323)**
- **• BFCP (UDP for SIP)**
- **• VP8, VP9 (for WebRTC high frame rate)**
- **• JPEG (for apps and web).**

A l'exception de Microsoft Teams, le ministère n'a pas de préférence sur le protocole à utiliser.

Courtesy translation :

Questions 3 and 4 on problems in the area of interoperability of systems in the Member States

- ***What is the standard for cross-border videoconferencing in your country?***

In your opinion, in what standard should such a connection take place? For external connections, our platform enables incoming and outgoing connections using all the following protocols (audio/video standards):

- ***Supported protocols : H.323 ; SIP ; WebRTC***
- ***Audioc codecs:***
- ***• G.711(a/μ)***
- ***• G.722***
- ***• G.722.1, G.722.1 Annex C (SIP only) (licensed from Polycom®)***
- ***• Siren7™, Siren14™ (licensed from Polycom®)***
- ***• G.729, G.729A, G.729B***
- ***• Opus***
- ***• Speex***
- ***• AAC-LC***
- ***Video codecs:***
- ***• H.261***
- ***• H.263, H.263+***
- ***• H.264 AVC***
- ***• H.264 SVC***
- ***• VP8***
- ***• VP9 (for connections to Conferencing Nodes with processors using AVX2 or later)***
- ***Content sharing:***
- ***• H.239 (for H.323)***

- • *BFCP (UDP for SIP)*
- • *VP8, VP9 (for WebRTC high frame rate)*
- • *JPEG (for apps and web).*

With the exception of Microsoft Teams, the Ministry has no preference on which protocol to use.

Questions 5 et 6 portants sur les méthodes de preuve d'identité utilisées par les différents États membres :

- **Quelles sont les méthodes de preuve d'identité utilisées dans votre pays (y compris les éventuelles dispositions légales sur ce sujet) ?**

Le Titre XXIII : De l'utilisation de moyens de télécommunication au cours de la procédure (Articles R53-33 à R53-39-1) du code de procédure pénale (CPP) ne prévoit pas de méthode de preuve d'identité particulière pour le recours à la visioconférence.

En pratique, pour les personnes qui ne sont pas détenues, l'huissier audiencier ou le greffier d'audience vérifie l'identité de la personne qui est entendue, principalement sur présentation d'une pièce d'identité.

En matière civile et commerciale, l'arrêté du 13 mai 2022 précisant les modalités techniques des moyens de télécommunication audiovisuelle pour la tenue de visioaudience ou de visioaudition en matière non pénale prévoit que le logiciel de visioconférence susmentionné doit fournir une définition d'image suffisamment bonne pour que la personne convoquée soit identifiable (article 2)

Outre cette précision qui impose que l'identification visuelle de la personne soit possible, aucune disposition spécifique n'impose une méthode de preuve d'identité plutôt qu'une autre.

En pratique, les cas d'identification 1 et 4 sont utilisés en France (déclaration des éléments d'état civil connus, comparaison de l'apparence physique de la personne avec la photographie présente sur la pièce d'identité préalablement transmise ou figurant dans le dossier de la juridiction ou montrée par la partie en visioconférence, voire reconnaissance de la partie par le magistrat si la personne est déjà connue de lui).

- **Ces méthodes dépendent-elles de la catégorie de l'affaire (pénale, civile, économique, etc.) et, dans l'affirmative, veuillez indiquer les liens existants ?**

Compte tenu de la réponse précédente, cette question n'appelle pas de développement supplémentaire concernant les procédures pénales.

Courtesy translation

Questions 5 and 6 on the methods of proof of identity used by individual Member States

- ***What methods of proof of identity are used in your country (including legal provisions if any)?***

Title XXIII: De l'utilisation de moyens de télécommunication au cours de la procédure (Articles R53-33 à R53-39-1) of the Code of Criminal Procedure (CPP) does not provide for any specific method of proof of identity for the use of videoconferencing.

In practice, for people who are not detained, the bailiff or court clerk verifies the identity of the person being heard, mainly on presentation of an identity document.

In civil and commercial matters, the Order of 13 May 2022 specifying the technical terms and conditions of audiovisual telecommunication means for holding video hearings in non-criminal matters stipulates that the above-mentioned videoconferencing software must provide an image definition that is good enough for the person summoned to be identifiable (art. 2).

Apart from this stipulation that it must be possible to identify the person visually, there is no specific provision imposing one method of proof of identity rather than another.

In practice, identification methods 1 and 4 are used in France (declaration of known civil status details, comparison of the person's physical appearance with the photograph on the identity document previously sent or contained in the court file or shown by the party on video, or even recognition of the party by the judge if the person is already known to him or her).

- ***Are these methods dependent on the category of cases (criminal, civil, economic, etc.), and if so, please provide these dependencies?***

In view of the previous answer, this question does not require any further development with regard to criminal proceedings.

CYPRUS

The four use cases for the remote identification of participants in a video hearing, as outlined in WK 2154/25, cover all instances applicable in Cyprus.

Question 1 on statistics

What is the proportion, in percentage, of judicial hearing held by videoconference in your country:

i. in a domestic context, in civil and commercial matters,

ii. in a domestic context, in criminal justice proceedings?

iii. . in a cross-border context in civil and commercial matters?

iv. in a cross border context, in criminal proceedings?

In the absence of detailed statistical data, please indicate the estimated value.

We do not maintain statistical data on exact percentages. However, based on nationwide data from the past two years, the annual average is as follows: 10 cases in a domestic context related to civil and commercial matters, 18 cases in a domestic context related to criminal justice proceedings, 18 cases in a cross-border context related to civil and commercial matters, and 22 cases in a cross-border context related to criminal proceedings

Question 2 on interoperability of systems in the Member States:

– What are the technical standards for cross-border videoconferencing applied in your country?

There are no fixed technical standards applied in all cases. Typically, we use the equipment and platforms provided by the relevant authorities. However, in cases where external partners are involved in coordinating the logistics of the procedure, the technical standards applied include H.323 for video, H.263, H.264, and H.239 for picture, G.711 and G.729 for audio coding, and H.264 for codecs.

– Taking into consideration the *Guide on videoconferencing in cross-border proceedings* issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?

Although we do not possess specialized expertise in this area, we believe that the standards outlined in the Guide on Videoconferencing in Cross-Border Proceedings should be the commonly adopted framework for cross-border connections.

Question 3 on the methods of proof of identity used by individual Member States

– What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?

1) First identification use case: visual recognition

3) Third identification use case: trusted third party

4) Fourth identification use case: self-identification

– Indicate if different methods are used in criminal proceedings and civil and commercial matters.

No different methods of identity verification are used in criminal proceedings, civil, and commercial matters.

HUNGARY

1. What is the percentage of court hearings held by videoconference in your country, expressed in percentage?

– In the domestic "setting", in civil, commercial, administrative and labour cases together about 8%,

– In the domestic "context", approximately 90% of all remote hearings in criminal proceedings,

– In a cross-border context, in civil and commercial matters, around 0.5%,

– In a cross-border context, in criminal proceedings, about 1.5%.

In the lack of statistics, estimated values are given.

The current Hungarian court VTC system allows the use of videoconferencing in all court cases.

In 2024, more than 27,000 remote court hearings took place in Hungary, involving a total of more than 19,000 defendants and more than 3,000 persons subject to infraction proceedings, as well as numerous litigants, witnesses and experts heard during the proceedings.

Most of these were in criminal proceedings, where the use of video and audio recordings was the most widespread.

In cases where the person to be heard is held in a penitentiary, 52-53% of cases are conducted using VTC and less than half of the cases involve the physical presence of the defendant in court.

In sentence enforcement related cases, sentence enforcement judges contact prisoners almost exclusively via VTC system, i.e. in almost 100% of these cases by means of a remote hearing.

The use of such a system is not yet widespread in civil, administrative, and labour cases. However, an amendment to the Code of Civil Procedure now allows for ‘simplified telepresence’ in courts via electronic communication platforms such as MS Teams, Skype, and Zoom. Under appropriate technical conditions, it also allows for continuous audio and video recording of proceedings. Given these developments, the use of remote court hearings in these areas is expected to grow, and the National Office for the Judiciary (NOJ) plans to increase the number of endpoints over the next three years.

The number of cross-border remote hearings remains limited. However, if required in any proceedings, Hungary will ensure a seamless interconnection, without technical obstacles.

2. Regarding the interoperability of Member States' systems:
What technical standards are applied in your country for cross-border videoconferencing?

The national videoconferencing system (Via Video/VIKI system), provided by NISZ National Infocommunication Service Provider Ltd. (NISZ Zrt.) for the courts, has a security classification of 4:4:4. All calls and videoconferencing connections within the system use TLScompliant signalling and media transmission. This ensures that a certificate at the endpoint generates a symmetric key for the duration of the call, encrypting both the setup and content to protect against manipulation and interception from the network and the Internet.

During encrypted calls, the symmetric key is always securely generated at the endpoint. NISZ Zrt., the system provider, does not have access to these keys, nor can they be generated or retrieved at the central office. The company transmits media in a "transparent proxy" manner, meaning that while encrypted media is switched and relayed over the NTG network, the content of the calls remains inaccessible.

Strict and secure authentication has also been applied to the court, i.e. user side, using the videoconferencing service. On the court side, four levels of authentication have been defined:

– General Conferencing requires 1-factor authentication (1FA: username + password)

– Remote Listening requires 2-factor authentication (2FA: username + password + personal certificate, which is implemented by a personal USB token or SmartCard), while

– Recording Manager and Broadcast Manager also require 2-factor authentication.

The secure management of recordings is thoroughly detailed. Recordings are automatically and securely transferred to the VIKI Transition Repository through a closed process, ensuring that they are stored in the designated institutional library. It is a closed and automated process! The recording is automatically started when the conference room is used, if a recording has been set up by the organiser. During the conference, the recording can be temporarily stopped and restarted by the Listener or the Organiser, but in any case the system records this request in the description file. NISZ Zrt. guarantees the storage of recordings in the Transitory Repository for 5 days, during which time the institutions must download the recordings. On the provider side, a script cleans the recordings in the Transitory Repository, ensuring that there is always space available and deleting recordings older than 5 days when necessary to free up storage capacity. No deletion is performed either by the institution or the service provider! Each court has read-only access to its own library, thus protecting the ownership of media content.

NISZ Zrt. provides a secure interface (sFTP) with two-factor authentication for the bulk transfer of recordings to specialised institutional systems. Additionally, this secure interface operates within NTG's HVR firewall system, where server access is restricted by IP filtering. As a result, only authorised institutional systems can connect to the VIKI Transition Repository and access the designated library, ensuring that unauthorised persons cannot gain access.

To ensure the authenticity and integrity of the recordings, NISZ Zrt. provides an XML description file for each recording. This file contains essential conference data, including timestamps, subject, participant logins, and recording start times. Additionally, a hash print of the original recording (in .mp4 format) is generated to verifiy that the file has not been changed since it was created by the Via Video/VIKI system. This ensures that the recording’s integrity can be verified at any time. In addition, the VIKI server also provides each recording with a GovCA time stamp, authenticating the time of creation, and the VIKI server signs the file with a GovCA certificate to authenticate that the media was released by the VIKI system

In addition, at the request from a court or a user, the system can also ensure that a cryptographic function can be set automatically for each recording. Decryption is only possible using the private key of the certificate held by the institution. This ensures that access to media is restricted solely to the institution, completely eliminating the risk of unauthorised extraction and network threats.

In addition to general protection, the interfaces provided by the system also have specific security features.

For private conferences, only designated endpoints with call IDs specified by the organiser during setup can connect to the conference room. This setting can be adjusted online, ensuring that participants can only join if their caller ID matches exactly. The system ensuresstrict access control, allowing only authorised participants to connect.

When using the locked conference function, no one can join the conference once it is locked, which is also an online configurable switch. When all necessary participants have joined the conference, the room door can be locked.

When the PIN code function is used, external participants must first enter the PIN code provided when joining the conference room and only then can they join the room.

The system guarantees and ensures that the exact number and type of calls that can connect to a conference are clearly defined, along with the exact number of participants.

This also shows that the content and connection of the videoconference calls are protected at multiple levels by default and can be further protected by the organiser.

Based on the above, it can be stated that, for the courts, recordings are only accessible to the National Judicial Authority (NOJ), with its specialised system managing the recordings and ensuring access protection. The automated and closed recording management subsystem within the VIKI system ensures that the recordings cannot be manipulated by the service provider, NISZ Zrt. Only the content owner has access to the content.

The protection of the content generated in the VIKI system is ensured by the fact that the system provides a descriptive meta-data file (XML file) for each recording (mp4 file), which contains data ensuring the integrity of the media content (the recording). Therefore, the following data is stored in the XML file:

– Timestamp service data (hash) provided by GovCA (Government Authentication Centre) digitally records the creation time of the VIKI remote listening content, verified by an external service (GovCA). This timestamp is located at the end of the XML: <xds:EncapsulatedTimeStamp>

– As the content producer, the VIKI system ensures the integrity of the created file (recording) through its own electronic signature (hash). This verifies whether the media file has been altered since its creation. The signature is located at the top of the XML: <ds:SignatureValue>

The access protection to the content generated in the VIKI system is ensured, as only the institution, acting as the data host, has access to its own remote hearing organisation data and its institutional library, where the institutional recording is stored. This access is granted by 2- factor authentication (simultaneous existence and use of username + password + token personal authentication certificate). The VIKI system is a closed system, with a 4:4:4 security process ensuring that the record is transferred to the institutional library when it is created. Additionally, the integrity of file transfers is ensured by the Transient Repository, which guarantees that court and institutional users can only access the NOJ institutional library by using two-factor authentication. Within the library, NOJ remote hearing recordings are always stored in an encrypted format. This encryption can only be removed by the NOJ, which holds the necessary private key (NOJ-owned certificate) to generate the playable media (.mp4) file.

Taking into account the Council's Guidelines on Videoconferencing in Cross-Border Proceedings (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf), particularly Annex III, what standard should generally apply to cross-border videoconferencing connections?

The standard outlined in the annexed guidelines has been applied in the design of the Hungarian remote consultation system.

3. On the methods of verification of identity used by some Member States:
Which of the four methods of proof of identity (including legal provisions, if any) as defined in WK 2154/25 are used in your country?
Please indicate if different methods are used in criminal proceedings or in civil and commercial cases.

Hungarian courts may use all of the four identification methods described in the discussion paper when conducting remote hearings.

The continuous transmission of images and sound allows for

– visual identification of the party,

– digital identification,

– identification through the intermediary of a trust service provider, and

– a declaration of the party's identity.

The remote hearing system includes a "document camera" on the device side, enabling the display of the content of an identifiable (public) document to the judge and recording the document, even in instances where the party requests confidentiality. This is made possible by a technical development that allows the image of the presented document to be "obscured" from the other participants in the remote hearing, ensuring that only the judge can view it.

NETHERLANDS

Please find below from the Judiciary of The Netherlands answers on the questions raised in the annex of document 6860.en25 regarding videoconferencing in the judicial context.

Question 1 on statistics:

Unfortunately, we don't have data available to give any indication on the statistics asked.

Question 2 on interoperability of systems in the Member States:

To our opinion, the technical standards mentioned in the appendix https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf are quite outdated on a technical level (H.323, ISDN, ...). We use Microsoft Teams for Online sessions in combination with a Cloud Video Interop so that we are interoperable with H3323 and Sip protocols.

Question 3 on the methods of proof of identity used by individual Member States:

After a quick analysis of the use cases, we concluded that we only recognize use cases 1 Visual recognition and 4 Self-identification. We have not yet encountered digital identification in our organization, either internally (2) or from a third party (3). However, invitations for video interviews are exchanged digitally

POLAND

First part

Poland confirms that the four cases of use of remote identification of participant in a video-hearing, listed in WK 2154/25, cover all instances in Poland.

Second part - The replies of PL to the clarifying questions on the use of VTC in a judicial context that can be found in the annex

Question 1 on statistics:

– What is the proportion, in percentage, of judicial hearing held by videoconference in your country:

i. in a domestic context, in civil and commercial matters,

ii. in a domestic context, in criminal justice proceedings ?

iii.. in a cross-border context in civil and commercial matters?

iv. in a cross border context, in criminal proceedings ?

In the absence of detailed statistical data, please indicate the estimated value.

PL answer:

Statistics are conducted for all videoconferences, with no division between domestic and cross-border videoconferences and no division between civil and criminal videoconferences.

According to our estimate, approximately 90-95% of videoconferences are conducted in civil cases.

According to the statistics for 2024, there were:

567,069 videoconferences in the Jitsi system

16,820 videoconferences in the Equinox system

583,889 videoconferences per year

Question 2 on interoperability of systems in the Member States (part one)

– *What are the technical standards for cross-border videoconferencing applied in your country?*

PL answer:

The videoconferencing systems used by Polish courts operate on an on-premises model, which means that the entire infrastructure, including servers, software and data, is maintained and managed locally, in-house. The system is not based on cloud solutions, which ensures full control over security, availability and data management.

All courts in Poland use a uniform standard of videoconferencing solutions integrated with the court recording system (eProtocol). The standard is the recording of all hearings in civil and misdemeanour proceedings, regardless of whether they are held in a fixed, remote or hybrid form (some participants connect remotely, some are physically present in the courtroom).

Polish courts generally use two systems, Jitsi and Equinox.

The national systems are based on:

1) the Jitsi system is based on WebRTC

2) the Equinox system is based on the H323 standard.

The Jitsi system is the dominant system.

For direct connections (terminal-to-terminal), the Equinox system is most commonly used due to the H323 protocol used.

Question 2 on interoperability of systems in the Member States (part two)

– *Taking into consideration the Guide on videoconferencing in cross-border proceedings issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?*

PL answer:

Cross-border videoconferencing, should be based on a proven, open standard for audio-video transmission such as WebRTC (Web Real-Time Communication). The WebRTC standard allows audio-video communication directly in the web browser (e.g. Chrome, Firefox, Edge, Safari) without the need to install additional software, supports modern codecs (VP8, VP9, AV1, Opus, etc.) and ensures effective integration with web applications. All this makes the solution universal and secure. Polish courts use a videoconferencing solution based on the WebRTC standard on the Jitsi platform.

Question 3 on the methods of proof of identity used by individual Member States (part one)

– *What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?*

PL answer:

In Poland, identity is verified by an ID card (other document proving the identity) presented to the court. If the hearing is held remotely, the document is usually shown to the camera (self-identification method).

Article 47c. Act of 27 July 2001. Law on the system of common courts (i.e. Journal of Laws of 2024, item 334, as amended).

The presiding judge may check the personal data of persons present at the place where the judicial activity is being performed on the basis of an identity card or other document proving identity. If a person refuses to submit to an identity check or if it is not possible to check his identity, the presiding judge may oblige such person to leave the place where the judicial activity is being performed.

Article 52a Act - Law on the system of common courts

§ 1. The provisions of Article 47c and Article 48 § 1 and 2 shall apply mutatis mutandis to persons participating in a hearing conducted by means of technical devices enabling it to be conducted by means of remote communication who are outside the court building.

In practice courts also use subsidiary methods of identity verification by, inter alia, confirmation of identity by another participant, e.g. a professional representative, an out-of-court body. This method may be used if such a participant attends the hearing (trusted third party method).

Question 3 on the methods of proof of identity used by individual Member States (part two)

– *Indicate if different methods are used in criminal proceedings and civil and commercial matters.*

PL answer:

The provisions indicated above are applied in criminal and civil procedure.

Due to the nature of criminal proceedings, the identity of parties and witnesses is verified before trial at the pre-trial stage by law enforcement authorities. In the case of a defendant deprived of liberty, the identity is verified by the Prison Service.

PORTUGAL

Question 1 on statistics

What is the proportion, in percentage, of judicial hearing held by videoconference in your country :

i. in a domestic context, in civil and commercial matters,

ii. in a domestic context, in criminal justice proceedings ?

iii.. in a cross-border context in civil and commercial matters?

iv. in a cross border context, in criminal proceedings ?

In the absence of detailed statistical data, please indicate the estimated value.

Data is not available. We cannot give any estimated value.

Question 2 on interoperability of systems in the Member States:

– What are the technical standards for cross-border videoconferencing applied in your country?

All courtrooms in Portugal are equipped with videoconferencing equipment, with rotating cameras, which connects to software that allows remote communication. In Portugal, it is possible to use any means of remote communication, but it is not possible to determine which is the most used, although the Webex application is common. This application allows integration with existing videoconferencing systems in the courts. The technical requirements for the videoconferencing equipment installed in the different courts are available on the Portal.

– Taking into consideration the *Guide on videoconferencing in cross-border proceedings* issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?

In Portugal, it is possible to use any means of remote communication, but it is not possible to determine which means is most used.

Question 3 on the methods of proof of identity used by individual Member States

– What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?

For the identification and authentication, on the day of the hearing, the witness identifies himself to the court clerk or to the official of the public service where the testimony is being given. From that moment on, the hearing is held before the judge of the case and the parties' representatives, using technological equipment that allows communication, by visual and audio means, in real time, without the need for intervention by the judge at the place where the testimony is being given (article 502, no. 4 of the Civil Procedural Code).

In Portugal, when there are videoconferences, individuals are identified before a court clerk by showing their identification document. The fact that videoconferences always take place in front of a court guarantees the identification of the person being heard. In these cases, the person in question does not need to be in possession of a Portuguese Citizen's Card, they just need to have a valid identification document that they show to the court clerk and the judge.

There is no computer or digital authentication

– Indicate if different methods are used in criminal proceedings and civil and commercial matters.

The Civil Procedural Code applies to civil, commercial, and administrative matters. For criminal matters, the applicable legislation is the Penal Procedural Code and the Portuguese Judiciary Organisation Law. Videoconferencing applies to all the matters referred above, but the application of the rules is different, criminal matters are stricter in the use of videoconferencing, but the identification is done in the same way.

SLOVAKIA

Question 1 on statistics

What is the proportion, in percentage, of judicial hearing held by videoconference in your country :

i. in a domestic context, in civil and commercial matters,

ii. in a domestic context, in criminal justice proceedings ?

iii.. in a cross-border context in civil and commercial matters?

iv. in a cross border context, in criminal proceedings ?

In the absence of detailed statistical data, please indicate the estimated value.

SK: statistical data are not available in required format.

Question 2 on interoperability of systems in the Member States:

– What are the technical standards for cross-border videoconferencing applied in your country?

SK: courts are using Cisco TelePresence SX80 and TANDBERG EX90 technology and there are no specific technical standards for cross-border videoconferencing.

– Taking into consideration the *Guide on videoconferencing in cross-border proceedings* issued by the Council (https://www.consilium.europa.eu/media/30606/qc3012963enc.pdf) and principally its Annex III, what standard should be commonly used for such a cross-border connection?

SK: Cisco TelePresence SX80 supports H.323 protocols and H.261, H.263, H.263+ and H.265 video standards.

Question 3 on the methods of proof of identity used by individual Member States

– What methods of proof of identity are used in your country (including legal provisions if any), among the four methods identified in document WK 2154/25?

SK: Courts are currently using fourth identification use case: self-identification, participant(s) are invited to show to the camera their identity documents.

– Indicate if different methods are used in criminal proceedings and civil and commercial matters.

SK: N/A.

FINLAND

Unfortunately, for now, we are only able to provide answer to the question 3 (below). As regards to the questions 1 and 2, we are still waiting more detailed information from our stakeholders. We'll return to the matter as soon as possible.

Question 3 - methods of proof of identity:

At the beginning of a hearing, chairman of the court proceeding typically requests the heard person or party to express their identity. If required, in certain situations, also identity card might be requested. Identification is not carried out by third parties/authorities. In the new videoconferencing service in the Finnish courts there is also possibility to use strong electronic identification to identify participants in a videoconference call.