Ref. Ares(2023)8272056 - 04/12/2023

Co-funded by the European Union

Digital communication and safeguarding the parties' rights: challenges for European civil procedure – DIGI-GUARD

Project ID: 101046660 — DIGI-GUARD — JUST-2021-JCOO

Comparative report on IT systems complexity, confidentiality and ease of access

Deliverable D4.2

based on D4.1 feedback

DIGI – GUARD

https://www.pf.um.si/en/acj/projects/pr10-digi-guard/

November 2023

1 Table of contents

2 Preface to the different aspects of service of documents in the member states of the EU

The DIGI-GUARD research aims to determine whether some unified rules should be created within the EU to service documents at national and cross-border levels. The aim of improving the framework of judicial cooperation within the EU is also in line with the objectives of the Commission set by the Digital Single Market Strategy. As a result, judicial proceedings will be more efficient, and claimants and legal professionals will have easier access to cross-border justice. Considering the preamble to the Service Regulation, according to which all relevant modern communication technologies should be used for service purposes, this project's ambition is to expand the research on new technologies within the whole evidence-taking process.

Specific areas covered by the research are:

1. Service through electronic means. An important area of research will be the different technical solutions for the electronic service of documents, e.g., centralized and decentralized systems; preregistered user accounts, by which documents are downloaded from a dedicated platform; use of e-mail (electronic postal mail, electronic postal registered mail, electronic postal certification mark, electronic postal mailbox). Problems relating to electronic service include measures to ensure the security of the transmission of the documents to the addressee; the extent to which a qualified electronic signature is required for email service; methods of checking the authenticity of an email message without an electronic signature; ways to resolve any doubts concerning the genuine nature of the message; methods for determining the date of electronic service. The project will explore different restrictions on access to electronic service of documents based on the type of addressee (legal professionals, legal persons, companies or other business actors, government bodies, etc.). The priority will be given to electronic service methods since the European Parliament was highly concerned about promoting this topic during the elaboration of the ELI/UNIDROIT Rules.

2. Postal vs. e-mail service: analysis of different postal service providers that may be used to service judicial and extrajudicial documents. Questions on authenticity, confidentiality, and proof of delivery will be tackled.

3. Formal service and the legal effects of service: the requirements for validly effected service in the case of personal service and the case of substituted service.

4. Those responsible for the service of documents: in particular, the distinctions drawn in national laws between the different actors in this process and their roles should be clarified and evaluated (e.g., the initiator of service and the institution or person obliged to perform the actual service of the documents: private operator, detectives or enforcement agents, Judicial Officer, court staff, different platforms for service, available in selected MS).

5. The addressee of the document to be served: personal and substituted service should be distinguished. The means at the disposal of courts and/or parties to identify the addressee's whereabouts should be identified. The importance of proceedings to locate that person and the question of judicial assistance in domestic and international relations.

6. The documents to be served: what constitutes "a document instituting proceedings"? The project will examine different national service systems depending on the nature of the document to be served.

7. Methods of service based on a legal fiction: the legal conditions for using fictitious service should be studied, in particular (1) whether there is any rule that relates to applying such fictitious methods of service on the basis that the addressee is residing abroad, or does not have any address for the purposes of service in the Member State of the proceedings; (2) the point in time at which the document is considered as served under such service methods. The CJEU in the Alder ruling shapes a new landscape in the practice of MS' national courts. The project will focus on the challenge of fictitious service with the starting point that the aim for expeditious proceedings should not undermine or weaken the right to be heard. The use of fictions in the electronic service of documents needs to be examined.

8. Irregularities in the service process. It is necessary to address situations where irregularities in service of the document instituting the proceedings in the state of origin might enable the defendant to obstruct the proceedings by raising the issue of incorrect or invalid service, even though they had the opportunity to prepare their defense. For example, a mistake concerning the place where the document should be delivered will not necessarily prevent recognition of the judgment in another MS, but the judge in the state addressed will have to assess whether the irregularity prevented the defendant from organizing his defense and whether that party's right to equality of arms was ensured.

9. Other means of communication. Regulation No 2020/1784 points out that the use of other means of communication for the transmission of documents may be more appropriate in exceptional circumstances, which could include cases where the conversion of large documents into electronic form would impose a disproportionate administrative burden on the transmitting agency or where the original is required in paper form to assess its authenticity. The criteria for deciding when electronic communication should not be used remain unclear.

10. Costs of service: the costs of the different methods of service of documents under national laws should be compared.

11. Electronic transmission of requests in cross-border service: the questions of efficiency, security and data protection should be studied.

12. Recommendations for minimum standards: identification of possible obstacles or legal uncertainty for parties in cross-border proceedings.

3 Expert report

3.1 Introduction

This expert report synthesizes findings from a comprehensive analysis conducted using the D4.1 questionnaire. We meticulously gathered responses from a representative sample of European Union member states, including Slovenia, Poland, Austria, the Netherlands, and Sweden. Our approach involved a rigorous quality check and information cleansing, ensuring harmonization and coherence in the responses. We also sought additional information and clarifications, supplementing these with extensive research to accurately assess the state of electronic services in the selected member states.

Subsequently, we meticulously organized and refined the questionnaires for publication. The expertly reviewed and edited raw responses are detailed in the appendix of this report, ensuring transparency and accessibility of our primary data.

The core of this report presents a detailed comparative analysis, synthesizing the responses into thematic discussions in the following chapters. This close examination offers a nuanced understanding of the current state of electronic services across these EU member states.

Concluding this report, we summarize the electronic service landscape within the European Union, as reflected by our sample. This is accompanied by strategic recommendations to advance further harmonization within the Single European Market. This report is designed to inform and guide policy and decision-making towards a more integrated and efficient digital future in the European Union.

3.2 A general approach to electronic service

In the context of certified electronic mail systems within the European Union, diverse approaches are evident among member states such as Slovenia, Poland, Austria, the Netherlands, and Sweden, each adopting distinct legal and technological frameworks.

Slovenia, for example, requires specific professionals like attorneys and notaries to use its certified electronic mail system but does not extend this obligation to other entities or the general populace. Meanwhile, Poland presents a more complex scenario with seven different legal regimes, predominantly focused on remote court communications in civil cases. This system, subject to frequent legal amendments, mandates certain legal professionals to receive electronic court correspondence. Poland also utilizes IT systems tailored for particular legal procedures, like registration and bankruptcy, and is moving towards a broader e-delivery approach encompassing public authorities and selected private entities.

Austria takes a comprehensive approach, mandating a wide array of professionals, including those in legal, financial, and insurance sectors, to engage in certified legal mail. This mandate, however, is dependent on the availability of requisite technology. Furthermore, from 2020, Austrian companies are obliged to accept electronic deliveries from public authorities, with exceptions based on annual turnover.

In contrast, the Netherlands adopts a flexible model, offering entirely voluntary registration in its certified electronic mail systems. This stance significantly differs from the more regulated approaches seen in other member states.

Sweden's strategy is characterized by integrating public authorities into an encrypted network for secure email communication. This system ensures secure exchanges within the network, while regular mail or email is used for communication with entities outside the network. Sweden employs secure emails with encrypted links for sensitive information, enhancing confidentiality and data protection. However, traditional postal services are utilized in scenarios where secure email is not viable.

Each member state's approach reflects its unique legal, technological, and operational landscape. From Slovenia's specific professional requirements to Sweden's encrypted communication network, these diverse strategies highlight the varied methods of implementing digital communication in legal contexts across Europe.

The obligation for entities to regularly check for certified electronic mail received varies significantly among countries like Slovenia, Poland, Austria, the Netherlands, and Sweden, reflecting different legal and practical approaches.

Slovenia has no specific regulation mandating regular checks for received mail. However, it is assumed in judicial practice that entities obliged to receive certified electronic mail, such as from the court, are expected to exercise a higher level of due diligence. This assumption extends beyond the court correspondence to tax and administrative proceedings without formal regulatory backing.

Poland's approach is nuanced, with no explicit legal requirement for advocates or attorneys-at-law to regularly check messages on the Information Portal. The legal framework, particularly under the Covid Act, has been extensively discussed within the legal community due to its legislative shortcomings and rapid changes. While professional trial attorneys are now required to have an Information Portal account, the law does not mandate regular account checks. In practice, delivery through this portal can take up to two weeks, with notifications sent to the attorney's regular email. Documents are considered delivered 14 days after submission if uncollected, prompting attorneys to access the portal at least biweekly to avoid missed deliveries. Discussions about blocking deliveries during holidays or illness have surfaced but haven't led to legislative changes.

Austria, meanwhile, does not legally obligate participants to check their official mailboxes regularly. Despite this, it is advisable to do so, especially since notification emails are sent for deliveries. The risk of non-collection due to inadequate infrastructure falls on the addressee. Legal entities are notified of a delivery by email, which is not deemed a delivery address under Austrian law. A document is delivered as soon as it is available for collection or the day after the recipient is notified. The Austrian Supreme Court expects lawyers to organize their office to ensure daily retrieval of the ERV system or, at the very least, an electronic transmission report is available.

In contrast, the Netherlands does not impose regulations requiring regular checks for received mail. However, users receive email notifications for amendments or additions to their files and reminders for unread mail in the Berichtenbox, part of Mijn Overheid. The recommendation to check the Berichtenbox regularly echoes the practice of periodically emptying a physical mailbox.

Sweden's judicial practice mirrors Slovenia's, where entities required to receive certified electronic mail from the court are expected to follow a higher level of due diligence. This extends to all authorities, which must adhere to general demands for practical assistance in contact with private persons and entities as outlined in the Administrative Procedure Act. Internal guidelines often supplement these public demands.

These diverse approaches across Slovenia, Poland, Austria, the Netherlands, and Sweden highlight the varying degrees of formal regulatory frameworks versus practical expectations and

recommendations in checking for certified electronic mail received. Each country balances its legal obligations with applicable guidelines, reflecting the unique legal and operational landscapes within which it operates. The duty of checking for new mail is sometimes hidden in the fact that missing the mail has legal consequences. Therefore, it could be said that checking for mail is required, even though the law does not explicitly require it.

3.3 Addresses, service providers, and compatibility of the systems

In Slovenia, entities and individuals can register more than one email address, with no mandatory requirement to open even a single address. A unique scenario arises in tax administration, where every legal entity must check the tax portal for documents despite the absence of prior registration or typical email addresses. The system, which is exclusively used to serve documents to taxpayers, is closed and not used for court communication or document exchange between entities. The limitation lies in the impossibility of aggregating documents from judicial and tax portals due to the absence of machine-to-machine communication and the legal ramifications of acknowledging receipt.

Poland faces a fragmented and uncertain landscape in electronic service regulation, necessitating multiple accounts and ICT systems. The potential conflicts between the universal e-delivery system and specific systems for civil proceedings create a complex environment. The transition to a comprehensive e-delivery system by 2029 may alter this landscape. Still, civil proceedings are not integrated into the broader system, leaving entities to navigate multiple platforms.

Austria distinguishes between two types of electronic services: ERV and Service under the ZustG. The central electronic mailbox, "Mein Postkorb," is a secure collection point for electronic messages from public authorities. While the system allows for forwarding deliveries to ERV or keeping them separate, participants must register with a transmitting agency, limiting mail aggregation across different systems. Additionally, notifications from tax authorities are delivered to FinanzOnline's Databox but are also displayed in "Mein Postkorb," offering a partial aggregation.

In the Netherlands, citizens access government databases and systems using DigiD without the possibility of aggregating all mail into one system. Each system requires separate access for specific information, indicating a segmented approach to electronic mail management.

Sweden, without a general requirement for certified email, allows individuals and entities to register multiple addresses for secure digital communications. While aggregation in one system is not typically feasible, authorities like the Swedish Tax Agency use digital systems to notify recipients of new messages via email or digital mailbox. The lack of a mandate for digital features marks a flexible, user-driven approach.

In Slovenia, Poland, Austria, the Netherlands, and Sweden, the landscape of local certified electronic systems or providers is characterized by diverse approaches and varying degrees of centralization and compatibility.

Slovenia operates with two governmental senders and two commercial mailbox providers. The courts serve as a primary source of certified mail, utilizing a standardized interface for machine-to-machine communication with commercial providers. The newer public administration system with fewer registered users offers recipient options through a portal and can send documents to other compatible mailboxes, though not fully aligned with the court's protocol. A distinct third system, exclusive to tax

administration, remains closed and does not support automated message exchange, leading to incompatibility among the existing systems.

In Poland, the ICT systems for civil proceedings, including the Information Portal, are managed by the Ministry of Justice, while the ePUAP system for administrative and tax procedures is under the Minister of Digital Affairs. The Electronic Delivery Act of 2020 introduces a dual-basis e-delivery system offering public and private electronic delivery addresses. This structure allows public authorities to use public addresses and will enable others to choose their preferred type of address.

Austria centralizes authority-delivered messages in "Mein Postkorb," with additional deliveries through FinanzOnline for tax-related communications and the ERV for mandatory participants. "Mein Postkorb" is accessible through various portals, catering to different user groups, including citizens and businesses. Austria also utilizes multiple delivery services and transmitting agencies for the ERV, alongside communication systems for non-evidentiary official documents, indicating a multifaceted and distributed system.

The Netherlands features at least two centralized systems: "Mijn Rechtspraak" for court-related matters, accessible through various identification methods, and "Mijn Overheid" for administrative information, consolidating data from multiple authorities in one mailbox (Berichtenbox) after registration.

Sweden's approach is more decentralized, with the courts using a single system connected to one server, ensuring automatic encryption of emails between authorities. However, other authorities often use their systems, making it challenging to quantify the total number of local certified electronic systems in the country.

In Slovenia, the compatibility between the public administration and court systems is partial. Upgrades to the court's protocol are necessary to enable service provision for the public administration, but the systems are not fully compatible out-of-the-box. This suggests a need for specific adjustments to achieve full interoperability.

Poland faces a challenge in system compatibility. Despite legal mandates for interoperability between state-serving systems, effective implementation of this requirement has not been achieved in practice. The compatibility issue's uncertainty is likely to persist until the full implementation of the Electronic Delivery Act of 2020, which may address these challenges.

Austria presents a more flexible approach within its ERV system, where participants can choose their transmission points, although the ERV software and transmitting agency must be compatible. Participants can register with multiple transmitting agencies for outward traffic but must select a specific agency for return traffic to ensure delivery to the court. Additionally, users can integrate deliveries from authorities into the ERV or keep the systems separate, reflecting a customizable approach to system compatibility.

In the Netherlands, the compatibility of systems is primarily based on their shared use of DigiD for login purposes. However, this compatibility does not extend to receiving certified electronic mail from other systems, indicating a lack of direct data exchange between them.

On the other hand, Sweden shows some level of compatibility among its systems, particularly regarding the transmission of secure emails. This indicates a degree of interoperability in the secure communication domain, albeit not universally across all systems.

3.4 eIDAS regulation compliance

Compliance with the eIDAS Regulation, specifically Article 43, varies among the certified electronic mail systems in Slovenia, Poland, Austria, the Netherlands, and Sweden.

In Slovenia, the current electronic mail systems are not compliant with Article 43 of the eIDAS Regulation. This indicates a gap in meeting the European standards for electronic registered delivery services, which may affect the legal recognition of electronically transmitted data within the EU framework.

Conversely, Poland's systems appear to meet the requirements of Article 43 eIDAS. This compliance suggests that the Polish systems provide evidence relating to handling transmitted data, including proof of sending and receiving and protection against risks like loss, theft, damage, or unauthorized alterations.

In Austria, the legal qualification of proof of delivery in electronic service, as per § 35 [3] ZustG, aligns with the conventional delivery methods regarding informative value and function. Although the usual proofs of service are not used in electronic service, the transmitted record to the court is akin to a conventional proof of service, ensuring legal equivalency in electronic transmissions.

The Netherlands, however, expresses uncertainty regarding compliance with Article 43 eIDAS, seeking clarification on whether the question pertains to general compliance with electronic registered delivery services or specifically with the qualified electronic registered delivery service as defined in Article 44 eIDAS. This uncertainty suggests a need for further analysis to ascertain the compliance status of Dutch electronic mail systems with eIDAS regulations.

Sweden, like Slovenia, currently does not have electronic mail systems compliant with Article 43 eIDAS. This non-compliance indicates a potential area for development in aligning with EU standards for electronic communication and data handling.

In Slovenia, none of the current systems are certified or connected to the eIDAS network for cross-border functionality. This indicates a lack of integration with the broader European digital infrastructure for electronic mail.

Poland offers a "Trusted Profile," a state-provided advanced electronic signature system that facilitates identity verification and electronic signature creation across various platforms, including ePUAP and the Courts Registers Portal. While this system enhances digital identity verification, it does not directly indicate eIDAS network integration.

Austria does not have a direct connection to the eIDAS network, as such a connection does not exist in a technical sense. However, Austria allows registration with foreign electronic certificates through a "country selection" feature, indicating a degree of compatibility with cross-border digital identification systems.

Although there is no direct system connection to eIDAS in the Netherlands, digital services like MijnRechtspraak and MijnOverheid allow login using eIDAS for citizens and organizations. This approach suggests aligning with eIDAS standards for user authentication in digital services.

Sweden's systems are neither certified according to eIDAS nor connected to the eIDAS network. However, the issue is under evaluation by some authorities, as indicated in reports by the Swedish Prosecutor Office and a Swedish Government Official Report. These reports highlight challenges in implementing eIDAS, including market limitations and the need for more precise rules

and validation principles for electronic signatures. Sweden's public authorities use digital management systems for employer IDs that align with eIDAS requirements, suggesting potential for future development.

3.5 Business model

In Slovenia, the commercial model is based on prices defined by law, with the court being the sole entity that pays commercial service providers for mail/document delivery. There are no similar provisions for public administration, leading to a lack of integration with commercial providers for public services. Consequently, end-users interested in participating in electronic delivery services often have to manage multiple mailboxes for different services (court, public administration, tax administration), reflecting a decentralized approach.

Poland's market for qualified providers is still developing, especially with the ongoing implementation of the Electronic Delivery Act of 2020. Two private qualified providers, KFJ Inwestycje sp. z o.o and ASSECO DATA SYSTEMS S.A., independently set prices guided by market principles. This emerging market suggests a move towards a more competitive environment with the potential for more providers and varied pricing.

Austria negotiates costs for electronic deliveries with delivery service providers, with the receipt of electronic deliveries being free of charge. Fees are incurred for transmissions via the ERV system, charged by transmission agencies, and for using software required to access these services. These costs are typically a part of the procurement process, with the Federal Ministry of Justice compensating transmitting agencies for court deliveries, hinting at a partly government-funded model alongside user-incurred fees.

In Sweden, the public authority bears the cost of using digital systems for communication. While some communications, like applications, may have statutory fees, these are generally not linked to the electronic system itself but to the application process, whether electronic or not. This approach indicates a government-funded model for the operation of digital systems.

3.6 Charging for the service

In Slovenia, the court system is financially responsible for delivering mail/documents paying commercial providers for each service rendered. The fee for each serving is fixed and defined by law, with the system being free for end-users. One of the commercial providers offers additional services at an extra cost. Currently, the court is the sole payer, as sending documents to the court is not permitted for users, making commercial providers dependent on court fees. There are no cost savings from system compatibility or massive re-use. However, this might change if the court begins accepting documents from users, potentially increasing income for service providers as sending parties would then pay for the service.

Poland's current approach offers free services via the Information Portal and the ePUAP system, with no additional costs for submission or receipt of letters. However, court fees for specific procedural activities are separate and payable. The forthcoming Electronic Delivery Act of 2020 will introduce a fee-based model for e-delivery, replacing the existing system of registered letters. Deliveries from non-public entities to public authorities via Poczta Polska's address will be free, but other deliveries will incur charges according to providers' price lists.

In Austria, the ERV system typically operates through transmission agencies, which charge basic and additional fees for each transmission. ERV is free for citizens using the upload service and citizen card function for electronic submissions. Receiving electronic deliveries is also free of charge, indicating a hybrid model balancing direct and indirect costs.

The Netherlands offers a user-friendly model where the system is entirely free for end-users, aligning with the country's digital inclusivity goals.

Sweden's model for the courts is funded by the Swedish National Courts Administration, covering the costs of secure email usage. The price depends on the number of email addresses used, encouraging using a single primary mailbox to minimize expenses. Digital communication is free for individuals and entities, though some applications incur fees payable through the system.

3.7 Accessibility of the system

All service providers in Slovenia offer a web interface, primarily designed for desktop devices, for manually receiving documents. The lack of support for mobile device certificates impedes official mail reception on these devices, primarily due to challenges with electronic signatures. However, introducing new personal IDs with NFC and embedded certificates is expected to improve mobile compatibility. As of late 2022, many of these IDs have been issued, indicating a move towards enhanced mobile accessibility. An alternative, the governmental cloud for cloud-based signatures, is limited to public administration services, though new regulations aim to extend access to commercial entities.

Poland's Information Portal notably has a mobile version for both Android and iOS. While all systems provide a web interface intended for desktops, they are also accessible through mobile devices, offering flexibility.

In Austria, access to electronic deliveries is facilitated via "Mein Postkorb," available on business and citizen service portals and through the "Digitales Amt" smartphone app. The service is optimized for mobile operation, ensuring functionality on smaller screens like smartphones and tablets. The ERV system typically functions through transmitting agencies, with at least one provider offering a browser-based client that does not require installation, potentially enhancing mobile accessibility.

The Dutch-certified electronic systems primarily provide web interfaces for accessing their services without specific mention of mobile compatibility or optimization.

Sweden's approach, particularly for secure email communications from the courts, enables access via both computers and mobile devices. However, challenges such as opening encrypted emails on certain devices and firewall restrictions may pose obstacles. Using Google Chrome as a browser on Android devices can resolve some of these issues, as can the use of common codes for confidential messages linked to phone numbers in digital communications.

In Slovenia, a commercial provider catering to court servings supports multiple operating systems, including Windows, Apple Desktop (OSX), and Linux. This broad compatibility ensures accessibility across commonly used platforms, catering to many users.

Poland presents a varied scenario where compatibility depends on the specific system. For the E-Court system, Windows 7 is required. At the same time, the Courts Registers Portal accommodates Windows,

Linux, and MacOS X. This indicates a range of supported operating systems tailored to different services. However, detailed data for other systems is not explicitly provided.

Austria's electronic mailbox, "Mein Postkorb," is accessible through multiple portals and applications, supporting various operating systems and browsers, including Windows 10, macOS Monterey, Android, iOS, and various browser versions. The "Digitales Amt" app requires Android 8 or higher, iOS 12.1 or higher, and biometric authentication capabilities. Different Austrian platforms like eAMA and FinanzOnline support specific operating systems and browsers, indicating a comprehensive approach to system compatibility. ERV participation requires software applications, with supported platforms varying depending on the software provider, thus accommodating a diverse range of operating systems from Windows 2000 to Linux and MacOS.

In Sweden, the courts use their electronic systems and Microsoft Exchange for email, with digital IDs supporting advanced electronic signatures like Bank-id. This approach focuses on advanced electronic signatures rather than qualified ones, aligning with the practical needs of users while maintaining security.

Overall, these countries demonstrate a commitment to ensuring their certified electronic mail systems are accessible across various operating systems, catering to the diverse technological preferences and requirements of their users. From Slovenia's multi-OS support to Austria's extensive range of compatible platforms and Sweden's focus on advanced electronic signatures, each country adapts its electronic mail infrastructure to meet user convenience and security standards.

The availability and standardization of public APIs (Application Programming Interfaces) for machine-to-machine communication with certified email provider services varies, reflecting different stages of digital infrastructure development.

In Slovenia, a private certified email service provider offers a public API, although it's not standardized and is limited to citizens registered with this provider. Additionally, the Slovenian court system provides a public API aimed at commercial service providers and more significant recipients of certified mail, primarily used by commercial entities. This API is documented, and there's an open-source solution available (Laurencius), indicating a degree of accessibility for software development within the legal framework.

Poland presents a landscape where different systems offer external integration via API, such as the Court Registers Portal and ePUAP. However, each system in Poland operates under its unique rules, and the sharing regulations are not standardized. This situation implies a fragmented approach to API integration, where each system's peculiarities might pose challenges for widespread or unified software development for legal or administrative purposes.

Austria requires special software for recording, sending, and receiving ERV traffic, conforming to the data formats specified by the Federal Computing Centre. The ERV software, provided by commercial entities, necessitates an internet connection to a supported transfer point and a valid address code for participation. Austria's "Mein Postkorb" allows forwarding deliveries post-opening and automatic collection into operational systems, albeit only through a web service interface, not via email programs. This system suggests a more centralized and structured approach to electronic mail, albeit with specific technical requirements for integration.

In Sweden, public APIs are provided by some public authorities, yet this development is not widespread across most authorities. The Swedish National Courts Administration is in the process of developing a

platform for digital infrastructure information exchange, reflecting ongoing efforts to enhance digital communication capabilities within the legal and administrative domains.

The availability of publicly accessible standards for implementing certified electronic services reflects different approaches to transparency and accessibility in digital communication systems.

In Slovenia, the court provides a documented API, and an open-source test system (Laurentius) is available. However, the court itself has not actively maintained or used this solution. This documented API and the open-source system indicate an effort towards transparency and public accessibility, though the lack of active maintenance suggests limited practical utility.

Poland offers a mix of publicly available manuals and technical information for some of its systems, while others do not have their details posted online. However, these can typically be obtained from the platforms' public administrators through access to public information. This approach signifies a degree of public accessibility, although the information is not uniformly available across all platforms.

Austria requires delivery services to fulfill specific conditions and technical requirements, as outlined in § 29 (1) of the ZustG. These include identification and authentication procedures and sender notifications for non-collection. The operation of a delivery service in Austria necessitates a license from the Federal Minister for Digitalisation and Economy. The Federal Ministry of Finance and the Federal Ministry of Justice provide detailed information on approved delivery services, legal bases, specifications, and an overview of software products. This comprehensive availability of information reflects Austria's commitment to transparency and standardized practices in electronic service delivery.

In Sweden, the use of APIs by public authorities is limited, and the systems used are often diverse and not uniformly open to the public. While some systems might be available in the free market, the authorities generally do not provide detailed information about them, considering security risks. Documentation on these APIs could be subject to confidentiality or demand significant effort from the authorities to compile, indicating a cautious approach to publicizing technical details of their digital infrastructure.

The availability and maintenance of open-source solutions depict different levels of commitment to open-source development and support.

In Slovenia, an open-source solution, Laurentius, is designed for the court system. However, this solution is not actively maintained, and the court uses a spin-off code that has not been publicly released. As a result, there is no sustainable support for this software, leaving end-users responsible for its maintenance if they choose to use it. This situation indicates a gap in continuous development and support for open-source solutions within Slovenia's certified mail system.

Austria, on the other hand, demonstrates a more robust approach to open-source solutions. The Federal Ministry of Justice in Austria provides information on approved transmitting agencies and commercial and non-commercial software products. MOA-ZS, an open-source middleware, simplifies access to e-delivery for specialized applications, making it easier to handle communications and process deliveries or proofs of delivery. OpenZUSE is an open-source framework that supports all tasks required for senders within the Austrian document delivery system. It offers Java 6 APIs for modules used in Austrian eGovernment electronic delivery and can be customized beyond the standard MOA-ZS application. This approach suggests a solid commitment to providing and supporting open-source tools for certified electronic mail in Austria.

In Sweden, electronic services for sending and signing documents are established and connected to the Swedish Courts Administration. While these services are open to the public, they are maintained by public entities and are not directly influenced by the government. This indicates that while open-source solutions might not be explicitly promoted, there is an existing infrastructure for electronic services in Sweden, albeit maintained by the public rather than community-driven entities.

3.8 Authentication and electronic signature requirements

In Slovenia, an electronic signature is required to confirm the receipt of documents for judicial servings and public administration. However, a simple click on the "receive" button suffices for the tax administration. This method relies solely on system access authentication without additional technical measures like electronic signatures for servings.

Poland's approach varies with each system. In the Information Portal, collecting a document involves clicking 'collect' and acknowledging the implications of receipt, which constitutes effective delivery in civil proceedings. For specific procedures, like those accessed via the Courts Registers Portal, users have multiple options: Trusted Profile (a state-provided advanced electronic signature), e-ID (ID card with a chip), MyID tool (authorization via online banking), or a Qualified electronic signature. The ePUAP platform follows similar rules, indicating a blend of simplicity and advanced security measures depending on the system and context.

Austria's delivery system with proof of delivery requires notifying the recipient of available deliveries. The delivery's effectiveness is tied to the first notification, deemed effective the following working day. The delivery service must record all notification and collection data, collectively serving as proof of delivery. To access documents via "Mein Postkorb," entrepreneurs must register using FinanzOnline access or a mobile phone signature. Service in the ERV is considered adequate the day after deposit in the recipient's disposal area, with identity verification processes in place for participants.

Sweden's methods vary by service type and authority. Simplified service does not require acknowledgment from the addressee, while standard service might involve oral or written acknowledgment, potentially signed online or in writing. The courts offer a system for digitally signing documents, allowing electronic ID signatures. The Swedish Tax Agency provides similar capabilities in specific cases, indicating a flexible approach to authentication, generally not requiring advanced electronic signatures for ordinary emails from the courts.

The requirement and type of electronic signature for receiving certified electronic mail, in line with the eIDAS Regulation, also differ, each adapting to their technological capabilities and legal frameworks.

In Slovenia, advanced electronic signatures are accepted for judicial servings. For public administration services, the requirements vary: some use the governmental cloud for qualified electronic signatures, while others still rely on advanced electronic signatures. The tax administration, which previously required advanced electronic signatures, has simplified its approach to merely clicking a button in the web application, moving away from electronic signatures.

Austria incorporates electronic signatures, particularly under original court documents and civil court proceedings. A handwritten signature or a qualified electronic signature as per Art. 3 No. 12 eIDAS Regulation is used in civil court matters. The visibility of the qualified electronic signature on the signed document is ensured for verification purposes. Accessing electronic deliveries requires registration at the USP, possibly with a mobile phone signature, among other methods. The "Digitales Amt" app and

FinanzOnline also facilitate access, requiring mobile phone signature activation. The authenticity in electronic public authority procedures is guaranteed by the qualified electronic signature on the citizen card, ensuring unambiguous identification.

In the Netherlands, the advocatenpas (ID pass for lawyers) is qualified at a substantial reliability level under eIDAS. This indicates a focus on a specific professional group and a significant level of security assurance.

Sweden primarily supports advanced electronic signatures like Bank-id and Freja eID for general and digital mailboxes. While services like Bank-id do not offer qualified electronic signatures, discussions about incorporating such requirements have occurred. However, concerns about the limited Swedish market and potential impacts on public revenue pose challenges to implementing stricter standards. No national regulation specifies the formal requirements for an electronic signature's validity. For secure email from courts, encrypted data can be opened without electronic signatures, reflecting a practical approach to security.

In Slovenia, the assurance level for accessing certified electronic mail services is generally considered "high" across all services. This implies a robust security protocol, likely involving multiple authentication factors to ensure secure access and verification.

Poland presents a diversified landscape in terms of assurance levels across different platforms. The Information Portal has no specific requirements, indicating a more accessible but potentially less secure approach. The Courts Registers Portal accepts both advanced and qualified electronic signatures, offering higher security. The E-Court (Electronic Writ of Payment Procedure) requires a qualified or unqualified electronic signature recognized solely within the E-Court System, reflecting a tailored approach to different service contexts.

Austria employs a high assurance level for mobile signatures, involving a dual security mechanism with a personal password and a TAN (Transaction Authentication Number). The process requires entering a mobile number, a signature password, and a TAN received via SMS or approved through the "Digitales Amt" app. This layered security approach ensures robust protection for accessing the electronic mailbox and official letters, aligning with high-security standards.

In Sweden, there is no uniform standard across all authorities, with each entity setting its guidelines. Generally, however, the assurance level is considered high, indicating a prevalent emphasis on solid security measures across various authorities.

3.9 General use of the service systems

The suitability and usage of certified electronic mail services for commercial or personal purposes would form a basis for general use of the service systems.

In Slovenia, the court or governmental systems did not initially envision using certified electronic mail services for commercial or personal purposes. However, commercial service providers, initially catering to court requirements, have expanded their offerings to include commercial options for delivering certified mail. This adaptation was a response to the limited use of the system, primarily financed by court servings, indicating a shift towards broader applicability in the commercial sector.

Poland's existing systems are currently designed solely for communication between individuals and state entities, restricting the use of these platforms for correspondence between private parties like

entrepreneurs and citizens. However, this limitation is set to change with the 2020 Act on Electronic Delivery implementation. The new legislation will facilitate vertical communication (between public authorities and citizens) and horizontal exchanges (between citizens or entrepreneurs), expanding the scope of electronic mail usage.

Austria offers a more flexible approach with its "participant direct delivery" system within the ERV, enabling direct transmission of documents between participants. This system is primarily utilized for transmitting documents in civil court proceedings but also includes a legal framework like § 112 ZPO for electronic mail transmission. Additionally, Austria has developed specific applications like the insurance portal (VU-ERV) for structured communication between lawyers and insurance companies, showcasing a versatile use of electronic mail in various sectors.

In the Netherlands, the "Mijn Overheid" inbox functions like a physical mailbox, where citizens can receive but not send messages. However, the "Mijn Rechtspraak" platform enables citizens, organizations, and professionals to submit documents and motions to the court, indicating a more focused use of electronic mail for legal proceedings.

Sweden's secure communication system offered by the courts is limited to interactions between public authorities and individuals/entities. Private systems in Sweden may offer broader usage options, but the court system is not designed for private-sector communication.

3.10 Existence of address registry and centralization

In Slovenia, there is no central system from which a sender can determine if a recipient has an "official electronic mailbox." Neither natural nor legal persons are required to open or register such a mailbox in any register. The Slovenian government does not provide an "official mailbox" to every individual or legal entity, indicating a lack of a centralized approach to electronic mailboxes.

Poland currently lacks a central database of electronic delivery addresses, including for the ePUAP system used in administrative and tax proceedings. However, this is set to change with the full implementation of the Electronic Delivery Act, which will establish an Electronic Address Database (Baza Adresów Elektronicznych, BAE). Managed by the Minister of Digital Affairs, this public register will contain electronic delivery addresses for public and non-public entities. Addresses will be visible in public databases of entrepreneurs, enabling more streamlined electronic communication.

Austria has introduced a directory of participants that includes all registered persons, companies, and authorities for electronic delivery, aimed at making electronic delivery more efficient. This directory enables delivering authorities to ascertain if a recipient can be reached electronically. Participants in the ERV system are included in this directory, although they may opt out of being listed.

In the Netherlands, registration in electronic mail systems is voluntary, and the government does not automatically provide a mailbox to each person. This approach suggests a more user-driven system where individuals can choose whether to participate.

Sweden does not have a central system for verifying the existence of an "official electronic mailbox" for recipients. While individuals can register for a digital mailbox provided by private companies, there is no obligation for natural or legal persons to have such a mailbox or to be registered. Public authorities and individuals must be connected to the digital mailbox system to exchange documents electronically. The Swedish government is investigating the obligation to have a digital mailbox and

the requirement for public authorities to send and receive secure digital email, with findings expected in 2024.

In Slovenia, the certified electronic service is centralized across different government-run systems for the court, public administration, and tax administration. The court system sends documents exclusively through commercial service providers. In contrast, the public administration offers the option for recipients to receive messages on its portal, with a theoretical opportunity to use commercial providers. The tax administration's system is more restricted, allowing message reception only on its portal without the involvement of commercial service providers.

Poland exhibits a more complex structure, with various centralized electronic delivery modes, including the Information Portal, Courts Registers Portal, e-court, ePUAP, and the upcoming e-delivery system. Each portal has different administrative arrangements: the Information Portal is managed by court presidents but falls under the Ministry of Justice for daily administration. The Courts Registers Portal and e-court are also under the Ministry of Justice, while ePUAP is managed by the Minister of Digital Affairs. The e-delivery system will involve components administered by Poczta Polska (State Treasury-owned) for the public box, private qualified providers for qualified mailboxes, and the Minister of Digital Affairs for the electronic addresses database.

In the Netherlands, the MijnOverheid website is managed by Logius, which is part of the Ministry of the Interior and Kingdom Relations. This indicates a government-centric approach to centralizing and managing the electronic service.

Sweden, like Slovenia, centralizes its service in different procedures for the court, public administration, and tax administration, with each system operated by the respective public authorities. Additionally, Sweden utilizes authorized service companies, regulated under the Act on the Authorization of Service Companies, for delivering services, indicating a blend of government-operated systems and authorized private participation.

In countries where certified electronic service is not centralized, the nodes' operation and the parties' responsibilities vary, with private entities often playing a significant role alongside public authorities.

In Slovenia, private entities run the nodes to receive "certified mail." These entities must meet specific technical requirements and pass a computer interface test to enlist with public entities like the court or public administration. Upon passing the test and signing a contract with the government, they can provide services to end users. This model reflects a partnership between the government and private entities, with the latter handling the technical aspects of service delivery under government authorization.

Austria's approach involves the justice authorities owning the ERV (Elektronischer Rechtsverkehr) and using various back-office systems connected to it, all hosted at the Federal Computing Centre. The ERV system involves transmitting agencies and IT companies authorized by the Federal Ministry of Justice through service concessions. These agencies collect submissions, ensure formal correctness, and forward them to the relevant courts and public prosecutor's offices. The official service "Mein Postkorb" is used for electronic delivery, simplifying registration, and access to electronic messages. This system indicates a collaborative model where the government oversees and authorizes private entities to handle operational aspects of the service.

In Sweden, private entities run the nodes if a public authority does not control certified electronic services, mailboxes, or email. There are no specific regulations for electronic mailboxes; generally, only public authorities are authorized to use electronic service. The quality mark Svensk e-

legitimation (Swedish e-ID) framework offers three levels of security, but no national regulation defines an electronic ID or digital mailboxes. According to financial service regulations, additional requirements exist for such services when used for banking purposes. This approach suggests a less regulated environment where private entities have greater autonomy in service provision, subject to specific security standards.

3.11 Cross-border delivery

In Slovenia, there is no provision for using existing systems to send cross-border certified electronic mail. The lack of such capabilities and implementation plans indicates a national-focused approach to electronic mail services without cross-border functionality.

Poland also does not have systems linked to other countries for cross-border correspondence. This suggests a similar national-centric approach to electronic mail systems, with no current integration for international communication.

However, Austria offers more flexibility with its ERV (Elektronischer Rechtsverkehr) system, which can be used from abroad through an ERV transmitting agency. European lawyers representing clients before Austrian courts are obliged to participate in the ERV and can request an ERV registration code from abroad. Foreign participants in the ERV are not required to have a domestic delivery point to register, indicating a more open and internationally accessible system.

Sweden allows sending secure emails to recipients abroad through its court system. If a code is necessary for security, an area code must be added to the phone number used for the code message, enabling international communication.

3.12 e-Codex integration

The connection of local certified electronic mail services to the e-Codex system, a pan-European project aimed at improving cross-border access to legal information and services, varies across member states in the sample.

The local certified electronic mail service in Slovenia is not connected to the e-Codex system. This indicates a lack of integration with this pan-European digital legal infrastructure.

Similarly, in Poland, no available information confirms any connection between the local certified electronic mail service and the e-Codex system. This suggests that Poland's electronic mail services may not be integrated with e-Codex for cross-border legal communication and information exchange.

In contrast, Austria has successfully connected its ERV (Elektronischer Rechtsverkehr) to e-Codex. This connection signifies Austria's active participation in the pan-European initiative, enhancing its capabilities for cross-border legal communication and digital integration within the European legal framework.

Sweden, like Slovenia and Poland, has no connection between its local certified electronic mail service and the e-Codex system. This lack of integration suggests that, for the time being, Sweden's electronic mail services operate independently of the e-Codex framework.

In Slovenia, there are indications that the e-Codex system is active within the public prosecutors' system. This suggests that while not widespread, e-Codex is being utilized in specific legal sectors in Slovenia.

Poland participated in the eCODEX-Plus project from 2017 to 2019, which aimed to enhance access to the European justice system through ICT solutions. This project involved pilot implementations of electronic submission and delivery of court documents, resulting in the connection of three Polish courts (the District Court for Wrocław-Downtown, the District Court in Wrocław, and the Court of Appeal in Wrocław) to the e-Justice infrastructure. This indicates engagement with e-Codex, primarily in a pilot capacity.

Austria has several years of experience with e-Codex and actively uses it, particularly in EU orders for payment procedures. This active utilization demonstrates Austria's commitment to integrating e-Codex into its legal processes, enhancing its cross-border communication capabilities.

The Netherlands also has an active system, indicating its participation in and utilization of the e-Codex framework for cross-border legal interactions.

In contrast, Sweden is still in the evaluation phase regarding the implementation of e-Codex. The Swedish Prosecutor Office has conducted a report on its findings and proposals, but the system is not yet in active use in Sweden, and there is no clear indication of when it might be.

In Poland, there is limited information on developing the e-Codex system beyond a pilot program under the eCODEX Plus project. The absence of detailed information on government or court websites suggests that e-Codex is not yet widespread or centrally coordinated.

Austria operates the e-Codex system centrally, managed by the Federal Computing Centre on behalf of the Federal Ministry of Justice. The national ERV (Elektronischer Rechtsverkehr) system is linked to e-Codex, theoretically enabling all ERV users (approximately 10,000) to use e-Codex. However, in practice, its primary use is in the EU order for payment procedure, involving Austrian lawyers and the District Court for Commercial Matters in Vienna. The Vienna Public Prosecutor's Office also uses e-Codex in a pilot operation for the EU investigation order, facilitating electronic communication with other European prosecution authorities.

In the Netherlands, the central point for the e-Codex system is the Justitiële Informatiedienst (Justid), an agency of the Ministry of Justice and Security. This centralization indicates a coordinated approach to managing cross-border legal communication.

Sweden is still in the evaluation phase regarding implementing the e-Codex system, with the common IT system not yet implemented. This ongoing evaluation suggests that the adoption and use of e-Codex are still under consideration, and no centralized or decentralized system is currently in place.

3.12.1 Regulation of the "original" document

Slovenia has a specific law on archiving that defines the circumstances under which a document copy is considered equal to the original, primarily applicable to legal persons.

However, Polish civil procedure allows using scanned documents as evidence, with no restrictions on the admissibility of evidence from electronic documents.

Austrian law considers data stored in an electronic documents archive as the original until proven otherwise, facilitating the use of electronic copies in legal proceedings.

There is no explicit distinction between an original document and its digitized copy in the Netherlands. However, the Dutch Code of Civil Procedure allows the filing of copies of original documents in civil procedures, with provisions for parties to request the presentation of original documents.

While some legal transactions require original documents in Sweden, others may apply the principle of free sifting of evidence. The approach to electronic signatures in Sweden suggests that a qualified electronic signature may offer a stronger presumption of validity than a non-qualified one.

The process of verifying whether documents provided to a court can be given the same value as the original varies among different countries. In Poland, Polish law accepts electronic evidence, and the court requests access to the original document only when there are doubts about its authenticity or other justifying circumstances. Failure to provide the original document does not entail specific procedural sanctions, but the court assesses the evidence and determines the significance of the refusal to present evidence.

In Austria, § 299 ZPO allows the court to order a party to submit the original document if necessary. Documents must not be submitted in the original; a copy is generally sufficient. If the original is not presented, the court evaluates the document based on statutory rules of evidence, considering the reasons for not producing the original. Electronic documents stored in archives are deemed to be originals until proven otherwise.

In Sweden, the court may check the documents' source and email addresses' legitimacy. If there are suspicions of document tampering or inauthenticity, the court may contact the party or its representative and request the original document. In court proceedings, the principle of free sifting of evidence applies, allowing the court to determine the evidential value of the document. There are no formal requirements for a valid signature in Sweden, and the eIDAS regulation may be considered for questions regarding electronic signatures. The proof of validation for electronic signatures can help assert their evidential value, even after the signature's control function has expired.

These procedures vary based on each country's legal framework, considering doubts about authenticity and the use of electronic evidence.

4 Findings and recommendations

Findings and recommendations follow after the analysis on the sample of the member states.

4.1 Differences Among Member States

1. Legal and Technological Frameworks: Each member state exhibits unique approaches to legal and technological implementation of certified electronic mail systems.

- Slovenia: Specific professional requirements.
- Poland: Complex system with seven legal regimes focused on court communications.
- Austria: Comprehensive approach, mandating a wide array of professionals.
- Netherlands: Voluntary registration, flexible model.
- Sweden: Encrypted communication network for public authorities.

2. Obligation to Check for Mail: Varies significantly, with Slovenia and Sweden expecting higher diligence, while Austria and the Netherlands have no legal mandate for regular checks.

3. Service Providers and System Compatibility: Member states show diverse degrees of centralization and compatibility in their certified electronic systems.

- Slovenia, Poland, Austria: Multiple systems, varying compatibility.
- Netherlands, Sweden: Decentralized approach, limited compatibility.

4. eIDAS Regulation Compliance: Compliance with the eIDAS Regulation (Article 43) varies.

- Slovenia, Sweden: Not compliant.
- Poland, Austria: Compliant or aligned.
- Netherlands: Uncertainty in compliance status.

5. Business Model and Charging for Services: Distinct approaches to business models and cost structures for electronic mail systems. Some member states have government-funded models, while others have user-incurred fees or a mix.

6. Accessibility and System Use: Varying degrees of mobile and operating system compatibility, with differing approaches to commercial or personal use of the service systems.

7. Cross-border Delivery and e-Codex Integration: Varying capabilities and integration with e-Codex for cross-border electronic mail, with Austria and the Netherlands actively participating.

4.2 Commonalities Among Member States

1. Digital Transformation Efforts: All member states are moving towards digital communication in legal contexts, albeit at different paces and with varying methodologies.

2. Security and Authentication Requirements: Each state has implemented measures to ensure security and authentication in their electronic mail systems, although the rigor and approach differ.

3. Legal Recognition of Electronic Documents: There is a general trend towards accepting electronic documents in legal proceedings, with varying degrees of equivalence to physical documents.

4.3 Certified electronic mail service maturity model

To support further efforts for cross-border electronic mail service, we have designed a maturity model for »certified electronic mail service« or similar service for serving official messages, documents, and similar communication. The model is based on the current findings of the project. The initial maturity model has five different maturity levels. Please note that whether the service is charged per document, flat fee or even provided for free by the government, does not influence the maturity level. User experience and ease of use for the citizen and the sending/receiving entity are the main factors for the system's maturity. The member state may have other systems for accessing the documents (e.g., a judicial portal to access court files by the parties), but these systems are considered separate, specialized systems. Here, we are only concerned regarding the user experience and access to the systems that allow official notification of the citizens and other users in the member state of any activities in the procedure or official notifications between the system users.

In the context of this capability maturity model, we are not interested in particular forms of serving documents, e.g., using detectives. We are focusing on systems that can (or already) replace or supplement regular (snail) mail.

This is an experimental draft of the capability maturity model, and it may be changed based on other results and information collected during the project.

An innovative maturity model to evaluate and enhance certified electronic mail services' capabilities mainly focuses on cross-border functionality and user experience. This model, pivotal for advancing electronic mail services in official communications, is rooted in the project's extensive research and findings. Below is an enhanced and detailed explanation of the model's structure and levels.

The maturity model assesses the progression of electronic mail services for official notifications and document serving. Key to this model is its focus on user experience and accessibility, irrespective of the service's pricing model. The model delineates a path from rudimentary systems to advanced, cross-border capable services.

Levels of Maturity

1. Initial Stage (Level 1)

- Description: The jurisdiction relies solely on physical mail for document serving. There is no electronic service available.
- Characteristics: Dependence on traditional mail, absence of digital infrastructure.

2. Basic Electronic Service (Level 2)

- Description: Limited electronic service exists, but it's restricted to specific procedures (e.g., court use).
- Characteristics: Introduction of digital service in a narrow scope, limited digital transformation.

3. Fragmented Services (Level 3)

- Description: Multiple electronic services are available but lack integration and compatibility. Users must navigate various platforms for different document types (e.g., courts, tax authorities).
- Characteristics: Presence of multiple digital platforms, high user effort due to lack of system integration, potential confusion, and inefficiency.

4. Integrated National Service (Level 4)

- Description: A comprehensive service or compatible multiple services exist for serving electronic documents, accessible to all entities (public, private, individuals). Users have a unified access point, enhancing convenience.
- Characteristics: National-level integration, single or compatible multiple service providers, streamlined user experience, but limited to national boundaries.

5. Cross-Border Capable Service (Level 5)

- Description: Advanced service with cross-border functionality, adhering to eIDAS regulation (Article 43) standards and compatible with international systems like e-Codex.
- Characteristics: Global compatibility, seamless cross-border communication, adherence to international standards, facilitating international legal and administrative processes.

This model applies to systems facilitating the official notification and exchange of documents electronically within a member state. While the model currently focuses on intra-country systems, its ultimate aim is to pave the way for robust cross-border electronic communication services.

It is intended as a dynamic model and subject to refinement based on ongoing research and evolving technological landscapes. It serves as a guideline for member states to assess their current standing and strategize toward achieving higher levels of digital integration and cross-border compatibility in electronic document serving.

Through this model, the DIGI-GUARD project aims to assess and inspire the evolution of electronic mail services, ultimately contributing to a more interconnected and efficient digital European Union.

Level	Description
1	There are no services for serving electronic documents in place. Documents are only served physically by regular (snail) mail.

2	There is a service for serving electronic documents in place, but it is only intended for one procedure (e.g., used by the courts). Other procedures are not covered.
3	Many services for serving electronic documents exist. They are not compatible, not integrated, and not interconnected. A citizen must check many different »mailboxes, «e.g., from the court, public administration, tax authority, and similar, to receive official documents in various procedures and from other system users (e.g., any legal entity).
4	General service for serving electronic documents is in place, or there is more than one service, but they are compatible in a way that they are entirely interchangeable. Any entity can use the service, whether public or private entities, citizens, courts, public administration, or similar. Users of the service can either choose one of the service providers, or there is only one service provider for all official document services. An example would be one or two commercial entities providing the service for any registered user or governmental service for every citizen. Every citizen must register only with one service provider and check one »mailbox« (e.g., a portal or in whatever form it is implemented) to receive any/all official documents in any/all types of proceedings. Legal entities and natural persons can also use the system to exchange documents or other messages between them. The system's limitation is that it is confined to a country lacking cross-border capabilities.
5	General service for serving electronic documents is in place. It is compatible with other services in the same local market if the system is decentralized or a central system supports serving in any procedure or private/commercial use. The system works in cross-border scenarios. For example, it is implemented as an electronic registered delivery service according to eIDAS regulation (Article 43). It uses standards and protocols compatible with other member states or works by serving through the e-Codex network.

We have performed a self-assesment according to the proposed maturity model and determined the following maturity levels for the sampled member states:

- Austria is achieving level 3.
- Poland is achieving level 3.
- Slovenia is achieving level 3.
- The Netherlands is achieving level 4.
- Sweden is achieving level 3.

4.4 Recommendations for Harmonization

We have identified the following possibilities to reach further harmonization:

1. Standardize Legal Frameworks: Develop a unified legal framework across the EU for electronic mail systems to ensure consistency and ease of cross-border communication. For example, this is already in progress with the eIDAS and other initiatives, although with limited results.

2. Enhance System Compatibility and Interoperability: Invest in technology to improve compatibility and interoperability between national systems, possibly through a centralized EU platform. One of the issues that we are identifying is the very high technical complexity of the legal frameworks and accompanying technical standards. Significant investments needed to achieve interoperability are a prohibiting factor, especially in the SME space.

3. Align with eIDAS Regulation: Encourage member states to align their systems with the eIDAS Regulation to ensure a uniform standard of security and authentication across the EU. This is also already in progress, again with limited results.

4. Promote Cross-border e-Codex Integration: Foster greater integration with the e-Codex system to facilitate smoother cross-border legal communication and services. E-Codex is geared toward member states' communication and cooperation; therefore, it does not promote wide usage of the system in the overall market.

5. Encourage Open-source Development and Support: Support developing and maintaining open-source solutions for certified electronic mail systems to enhance accessibility and innovation. There are already initiatives that drive software implementations towards open-source solutions. The issue with such projects is maintaining the source code once the project is finished. Again, this is the cost that SMEs cannot afford to be included in the general "email" service system.

6. Focus on User Accessibility and Inclusivity: Design systems with user accessibility in mind, ensuring compatibility across various devices and operating systems and considering the needs of all user groups. Following this path would virally promote the use of systems, but the essential requirement is the simplicity of the data exchange systems. Existing systems are trying to do too much at once. All the frameworks are trying to solve many legal and technical issues in a single place – electronic service. But why? Physical (snail) mail does not do such a thing. It is just a secure, reliable delivery service. Changing the strategy to provide reliable, simple, confidential communication between any party in any member state would promote developing and using a general electronic service system that courts and other authorities can use.

The KISS principle in information technology stands for "Keep It Simple, Stupid" or sometimes "Keep It Simple and Straightforward." It is a design and development philosophy that encourages simplicity and straightforwardness in system and software design. The principle suggests that complex solutions should be avoided in favor of simple, easy-to-understand ones whenever possible. This is important because complexity can lead to errors, difficulties in maintenance, and increased chances of failure.

To help legal experts understand the KISS principle in information technology, let's consider a legal document management system as an example:

1. Simple Document Naming Conventions: Instead of creating a complex document naming convention with numerous rules and codes, a legal document management system adhering to the KISS principle would use straightforward and intuitive names. For instance, naming documents by case number and document type (e.g., "Case1234_Complaint.pdf").

2. User Interface Design: The KISS principle would advocate for a clean and straightforward layout when designing the user interface for legal professionals to access and manage documents. It would avoid clutter, excessive menus, or unnecessary features that could confuse users.

3. Search Functionality: In implementing a search feature within the document management system, the KISS principle would prioritize a simple and effective search algorithm. It would focus on essential search criteria like keywords, document type, and date, avoiding overly complex search options that may overwhelm users.

4. User Permissions: When setting user permissions within the system, the KISS principle would recommend a straightforward approach. For example, legal experts should have clear and easily understandable permissions, such as read-only or edit access, without unnecessary complexity.

5. Document Retrieval: The KISS principle would promote a straightforward document retrieval process. Legal professionals should be able to access documents quickly and without unnecessary steps or convoluted procedures.

6. Data Security: Data security is crucial in legal systems, but the KISS principle suggests implementing straightforward security measures. For instance, using strong, regularly updated passwords and encryption without overcomplicating the security process.

7. Integration with Other Systems: If the legal document management system needs to integrate with other legal software or databases, the KISS principle advises keeping integration processes as simple as possible to ensure compatibility and ease of use.

In summary, the KISS principle in information technology for legal experts means designing and implementing systems and software with simplicity in mind. It focuses on making technology accessible, user-friendly, and easy to maintain, enhancing efficiency and reducing the risk of legal process errors.

This approach would solve many issues of current systems. Not to get too technical, but all current systems are based on the SOAP technology, which was developed at the end of the 20th century. Staying with these technological solutions is even paving the way to becoming increasingly reliant on Java technology as other platforms are starting to drop support (e.g. .NET), confining developers to one platform and causing a platform monopoly to arise. All commercial providers use REST technology (Google, Microsoft, Amazon) for simplicity. However, their systems work and are used by billions worldwide.

The popularity of the systems would encourage interoperability, user-friendliness, competition between the providers, and accessibility. It would also mean that with enhanced interest in the open-source code, the chance of it becoming supported would grow.

There is no real technical reason to try to incorporate every angle of legal requirements into the standard protocol for the service of messages. This can all be done locally, as it is performed with the physical mail. It would also allow for further extensions. For example, to enable the recipient to sort received mail according to the content, standardized attachments could be defined, e.g., JSON (popular text-based data transfer format) or XML document could be sent together with all other attachments, and it would be the choice of the recipient to use it in automated or manual way. Forcing specific legal regulations and technical requirements into the protocol does not work. We have proved it on a large scale – across the whole EU.

The other argument is widespread use. All entities, private and commercial, need reliable service messaging between them as well. Why would developing a separate system for the courts and other authorities make sense? This already results in many incompatible systems, requiring recipients to check for mail in many electronic systems. This is the same as putting specific mailboxes on your property to support receiving packages and envelopes from specific logistic providers. If that does not make sense in the physical world, why would it in its electronic sibling?

Adopting modern, widely used technologies like REST and a localized approach to legal compliance presents a promising path forward for enhancing electronic delivery services. This approach simplifies the technical framework and aligns with user expectations and global technological trends, paving the way for a more efficient, user-friendly, and adaptable system. Using properly tuned maturity model could be showing the path in the right direction.

5 Appendix I

Combined answers from the questionnaire D4.1

5.1 Which persons/entities have the obligation to receive certified electronic mail?

Certain persons/occupations in Slovenia must connect to the certified electronic mail system, e.g., attorneys, notaries, enforcement agents, and liquidators. The court currently does not provide electronic serving to other entities at all. There are no other obligatory requirements for any entity or person to register for a certified electronic mail address, and such address is not provided to all entities/citizens by the government.

In Poland, there are seven different legal regimes possibly concerning remote communication with the court in civil proceedings. There have been changes in this regard as a result of the law being amended several times already after the date of rendering the national reports. The legal situation regarding electronic service in civil proceedings is unclear and unstable. Regulation of electronic service from the court to professional trial attorneys in civil proceedings during the COVID-19 pandemic (one-sided; lawyers only receive court correspondence online but have to submit pleadings to the court on paper via traditional postal services). The legal basis is Article 15 zzs(9) of the COVID-19 Act. The provision provides for the service of court documents by allowing access to the content of these letters in the ICT system, called the Information Portal of the Courts. On this basis, court correspondence is (mandatory) received by: advocates (adwokaci), attorneys-at-law (radcowie prawni), patent attorneys (rzecznicy patentowi) and the Office of General Counsel to the Republic of Poland (Prokuratoria Generalna Skarbu Państwa; the entity was established to protect the legal interests of the State Treasury and legal entities in which the State Treasury holds a stake). The regulation of e-service from the COVID-19 Act was transferred to the Code of Civil Procedure by an amendment act signed by the President of the Republic of Poland on 28 August 2023. This means that the solution of service for professional trial attorneys is no longer limited to the COVID-19 period and applies to unilateral correspondence (from the court to the individual, not vice versa). The regulation will apply, once in force, to advocates (adwokaci), attorneys-at-law (radcowie prawni), patent attorneys (rzecznicy patentowi), public prosecutors (prokutarorzy), pension authorities (mainly Zakład Ubezpieczeń Społecznych) and the Office of General Counsel to the Republic of Poland (Prokuratoria Generalna Skarbu Państwa). There are selected procedures in civil proceedings that are entirely carried out in an IT system dedicated to a given procedure. This happens in the case of registration proceedings before the registration court - the National Court Register (the court dealing with the official company register of Poland) or in bankruptcy proceedings. All these proceedings (including submitting documents by participants in these proceedings) take place online through a system called the Courts Registers Portal (https://prs.ms.gov.pl/). This means that all entities involved in these proceedings, including those listed in the National Court Register (such as companies, foundations, etc.) and entities involved in bankruptcy proceedings, including the creditors of the bankrupt, are required to utilize the Courts Registers Portal for the submission of court documents. Communication from the court to the party also occurs through the indicated system. For example, Article 6942a of the Code of Civil Procedure reads: 'If the proceedings before the registry court take place via an IT system, the activities of the court, the court referendary, and the presiding judge are exclusively recorded in this system, and the data generated as a result, in electronic form, are signed with a qualified electronic signature'. There is also one optional procedure, the electronic writ of payment procedure, which also takes place on a dedicated online portal. This procedure is for monetary claims dealt with by one court in the country - the district court in Lublin(we call it 'e-court'). Communication between the e-court and the plaintiff in electronic writ proceedings takes place via the system available at https://www.e-sad.gov.pl/. Therefore, if the plaintiff (or his/her attorney) decides to use this mode, he or she must communicate with the court online. If they do not want to use this procedure, they can use traditional writ

proceedings before the court, which is based on general rules for submitting procedural documents. Detailed regulations also apply to land and mortgage register proceedings. For all parties involved in civil proceedings and their legal representatives, land and mortgage register proceedings are conducted on paper. There is an exception for notaries, bailiffs, and heads of tax offices who, in accordance with Article 6264 of the Code of Civil Procedure, must submit applications for entry in the land and mortgage register exclusively via the ICT system, with a qualified electronic signature. When the basis for an entry in the land and mortgage register is a paper document (which is often the case, as all notarial deeds in Poland are in paper form), notaries, bailiffs, and heads of tax offices are required to send the paper document to the court responsible for maintaining the land and mortgage register within three days from the date of submitting the application for entry Another form of regulation regarding e-service can be found in the general provisions of the Code of Civil Procedure, which, since 2016, have theoretically allowed for electronic delivery to all parties involved in civil proceedings. This includes not only professional trial attorneys (advocates, attorneys-at-law, etc.) but also parties in various civil processes. According to the Code of Civil Procedure, 'The court shall deliver documents via an IT system (electronic delivery) if the recipient has submitted the letter via the IT system or has opted for electronic document submission.' However, it's worth noting that the envisioned general system for managing online correspondence in civil proceedings, as outlined in these regulations, has never been established, and these provisions in the Code have remained inactive for seven years. The latest e-service regulation having impact on civil proceedings was introduced through the Electronic Delivery Act of 2020, although its implementation has been postponed several times. Ultimately, its goal is to ensure that all correspondence from public authorities is sent in electronic form (not only in civil procedures but in all court and administrative procedures), including communication between citizens if they choose this option. E-delivery under this act aims to replace traditional paper registered letters, which are currently used in various procedures throughout the country. Once fully implemented, all public authorities (including courts starting from 2029) and select non-public entities, such as entrepreneurs, advocates, and attorneys-at-law, will be required to communicate online. For others, having an electronic delivery address will be optional. Public authorities will exclusively produce electronic documents, but for individuals who do not have an electronic delivery address, Poczta Polska (a public postal operator) will handle the printing of electronic files and the delivery of paper printouts (providing assistance for those not digitally connected). In addition to deliveries via a public electronic delivery address (provided through the Poczta Polska application), individuals can establish an electronic address with a qualified provider, as defined by the provisions of the eIDAS regulation, and the effects of such deliveries will be identical. As a result of this system, all professional legal representatives will be obliged to use e-delivery, as will parties to proceedings who are entrepreneurs, while other entities will have the option to do so.

In Austria the following parties are obliged to participate in certified legal mail ("Elektronischer Rechtsverkehr"; hereinafter: ERV) (§ 89c [5] and [5a] of the Austrian Court Organisation Act ["Gerichtsorganisationsgesetz"; hereinafter: GOG]): Lawyers, Notaries, Financial institutions, Domestic insurance companies, Social insurance institutions, Pension institutions, Construction Workers' Leave and Severance Pay Fund, Pharmaceutical Salary Class, Insolvency Remuneration Fund, IEF-Service GmbH, Umbrella organisation of social insurance institutions, State Financial Procurator's Office, Bar associations, Expert witnesses, Interpreters. This obligation does not apply if the required technologies are not available (§ 89c [5] GOG in conjunction with § 11 [1a] ERV 2006) for the for the public authority. Since 1st January 2020, companies are obliged to accept electronic deliveries from public authorities and public authorities are obliged to use electronic delivery. This does not apply to companies that are not obliged to submit advance VAT returns if their turnover is below the threshold (§ 1b E-GovG). This means that the action must be served electronically in accordance with the provisions

of the third section of the Austrian Service of Documents Act ("Zustellgesetz", hereinafter: ZustG), unless the company is represented by a lawyer, or participates in the ERV voluntarily.

In the Netherlands registration in each system is on a voluntary basis.

In Sweden certain public authorities are connected to an encrypted network of public authorities. This connection enables sending secure and encrypted email between authorities. For example, ecommunication between courts is always secure from the start, as the email which is transmitted within the system never leaves the shared server. If an authority is not connected to the system, regular email or mail is used. There is a second system called e-skick (e-sending) which is used between some authorities for secure communication. The authorities have lists of the authorities connected to each system. Private parties or entities are not required to have an email address. However, if they have provided the authority with an email address, encrypted and secure email will regularly be used for communication and service. The Swedish National Courts Administration also offers a digital service where parties and others can submit documents digitally. This can be done with or without a digital signature and works in the same way as encrypted email. When using secure email to send sensitive documents, the recipient will usually receive an encrypted link in the email that opens in a secure window and allows the recipient to download the document. If the document or information is confidential, the rule is that a code must be sent to the recipient's phone number and a secure email to a registered email address.2 The code is needed to open the information in the email. If there is no phone number, the court must use regular mail. If it is not possible to use secure email to communicate with a person or an entity, regular mail must be used, not regular email.

5.2 Can persons/entities send certified electronic mail (unstructured) to courts? How about structured documents? Please also explain the options in other proceedings.

Currently only certain persons/entities, e.g. attorneys, notaries, enforcement agents, liquidators can file documents but only in limited, prepared cases (parts of the procedure) in Slovenia. This documents are structured and data has to be entered through a portal (web interface). In other cases, when there is no suitable structured entry form in place, they have to use regular snail mail. Natural persons and organizations do not have the possibility to send documents or file anything, even though this is already defined in the law. The supreme court that runs the central system for certified electronic mail is refusing to accept any documents or filings, even though the system for communication is in place and operational. The unilateral action of the Supreme Court is legally questionable.

In Poland in special cases it is possible to transmit procedural correspondence electronically. However, this can only be done through the dedicated ICT systems and not via an unstructured message. As per the current legal framework, it is not possible for anyone to effectively submit a document to a civil court online. Professional trial attorneys can receive letters exclusively through the Information Portal but do not have the capability to send documents. The situation differs in administrative and tax procedures, where during proceedings before a public administration body, both citizens and entrepreneurs (along with their representatives) can utilize the online communication system known as ePUAP - the electronic platform for public administration services. This system, in operation since 2008, facilitates two-way communication between the authority and the involved entity. However, it's important to note that for communication with the court, neither standard email nor correspondence through the ePUAP system holds legal validity.

In Austria users of the ERV can submit submissions electronically to the court or the public prosecutor's offices via a transmitting agency or submit submissions via the upload service. Submissions via transmitting agencies require registration with a transmitting agency and are generally available to everyone. Certain institutions must participate in electronic legal transactions. Here, mutual communication takes place exclusively by electronic means. By submitting documents via the upload service, all citizens can submit documents electronically to courts or public prosecutors' offices using the Austrian citizen card (chip card or mobile phone signature). In this case, the transmission of documents is not bidirectional. According to § 6 Decree of the Federal Minister of Justice on Electronic Legal Transactions 2021 ("Verordnung der Bundesministerin für Justiz über den elektronischen Rechtsverkehr 2021", hereinafter: ERV 2021), submissions via email are only admissible if this mode of transmission is expressly ordered by law or regulation. According to recent Supreme Court case law, pleadings submitted to the court by email are inadmissible and irrelevant. Submissions in the ERV are generally subject to the same formal requirements as written submissions (cf. the pleading requirements in § 75 of the Code of Civil Procedure ["Zivilprozessordnung"; hereinafter: ZPO]). In addition, the provisions on the content of written submissions. The Austrian ERV is not based on the exchange of text documents, but almost entirely requires precisely defined structure files in XML technology. If no separate structure is available for the submission, the pleading must be submitted as "other initial submission" including a PDF attachment. Orders for payment actions, applications for enforcement and actions in the European order for payment procedure as well as applications to the land register shall be submitted in a structured form that allows for further processing supported by automation (§ 1 [3] No. 3 ERV 2021); their submission as PDF attachments is not permissible. Submissions and attachments by persons obliged to participate in the ERV may only be submitted in scanned form if they are not available to the submitting person in original electronic form (§ 1 [3] No. 3 ERV 2021).

As of 16 October 2023, it is possible in the Netherlands to conduct certain proceedings digitally concerning family / children and commercial matters in the court of Rotterdam. This includes electronic receipt of documents and digital notifications if there are any changes to the file. Documents may be filed by professionals. In the course of 2024, all Dutch courts will offer this possibility. As of 4 September 2023, it is possible to lodge an appeal electronically against (national) tax decisions. Documents may be filed by citizens and professionals.

In Sweden, persons and entities can send emails to the courts, regular and certified mail, and can also upload documents, with or without signing through the court's website. Other authorities offer different types of methods. A person/entity could therefore send secure email to an authority through a special form on a website, the so called digital upload of documents with or without signing. If a person/entity replies to a secure email from a court, the reply message is automatically sent in a secure way.

5.3 Is there a regulation in place that requires the receiving entity to check for the received mail regularly?

Not in Slovenia. In the judicial practice it is assumed that entities, that are currently required to receive certified electronic mail from the court, have to follow a higher level of due diligence. There are also no special requirements in the tax proceedings or administrative proceedings, neither in the regulations governing postal services.

In Poland, no regulation imposes an obligation for an advocate or attorney-at-law to regularly check messages on the Information Portal. The Covid Act did not mandate having an account on the Information Portal for professional trial attorneys. The numerous legislative shortcomings of the Covid Act in this regard, and the hurried pace at which changes to the law were processed, were widely discussed within the legal community. Following the transfer of provisions regarding deliveries through the Information Portal into the Code of Civil Procedure, an omission was corrected by introducing the obligation for professional trial attorneys to have an account (resulting in appropriate amendments to the Act on Attorneys-At-Law and the Act on Advocates). However, there is still no legal requirement to regularly check this account. In practice, delivery through the Information Portal can take maximum 2 weeks. A notification of the document's availability is sent to the attorney's regular email inbox, followed by a reminder a week later, and a final request for collection two weeks later. If the document is not collected, it is considered delivered 14 days after it was submitted in the system. Consequently, each attorney should access the Information Portal at least once every two weeks to avoid the risk of missed deliveries. Within legal circles, there have been discussions regarding the need to establish the possibility of blocking deliveries during holidays or in case of a attorneys's illness, but these voices were not heeded by the legislator.

In Austria there is no legal obligation to check one's official mailbox regularly. Although notification e-mails should be sent in the case of deliveries, it is advisable to check regularly. The risk of the legal Bundesministerium für Justiz, 'Elektronischer Rechtsverkehr (ERV)', visited 3 July 2023, consequences of non-collection of the document due to lack of adequate infrastructure shall in any case rest with the addressee. Participants of the ERV are notified of a delivery by e-mail, whereby this e-mail address is neither a delivery address within the meaning of § 2 No. 5 ZustellG nor an "electronic delivery point". The document is deemed to be delivered as soon as it has been made available for collection or on the working day after the recipient has been notified of the transmission (see § 89d [2] GOG). According to the Austrian Supreme Court ("Oberster Gerichtshof"; hereinafter: OGH), a lawyer is obliged to organize his office in such a way that either a daily retrieval of the ERV computer system is guaranteed or, in any case, at least an electronic transmission report of the decision transmitted is available as well.

In the Netherlands there is no regulation applicable. However, users get email notifications each time the file is amended or a document is added to their file. Users will also receive a reminder if there is unread mail in the mailbox (Berichtenbox in Mijn Overheid). Mijn Overheid recommends the following: “Check your Berichtenbox regularly so you don't miss digital mail. Just as you regularly empty your (physical) mailbox, it is wise to check your Berichtenbox regularly.”

In Sweden it is understood in judicial practice that entities that are currently required to receive certified electronic mail from the court, have to follow a higher level of due diligence. Authorities have to follow the general demands considering effective assistance in contacts with private persons and entities (see Chap. 6 § of the Administrative Procedure Act). The authorities often provide internal guidelines regarding such questions.

5.4 Is it usual/possible for an entity to have only one certified email system address or does an entity usually have more than one certified email system (please also consider tax procedures, administrative procedures and similar)? If there are more addresses/systems, is it possible for the recipient to aggregate received certified electronic mail and view and receive mail in one system only? If yes, please shortly explain how.

An entity (the same is for natural persons) in Slovenia may register more than one registered email address, though there is no obligation that it should be opening even a single address. A special case is tax administration. There every legal entity has to check whether there is a document waiting in the tax portal, though there is no prior registration and there are no addresses with similar meaning as with electronic mail. Every legal entity is a tax payer and has access to the portal using certificate. The system is closed and cannot be used by the court or to exchange documents between entities. It is solely intended for serving documents to taxpayers. Aggregation of received documents from the judicial portal and tax administration portal is not possible. First, there is no support for machine-to-machine communication in tax administration. That means that documents have to be accessed and downloaded manually. Second, aggregation of documents would result in confirming that the document has been received and that would result in "deadlines" to start running. Consequently, it would be impossible to make an aggregation system that would not at the same time have side-effect in legal consequences for the recipient.

In Poland the regulation of electronic service in civil proceedings is currently fragmented, inconsistent, and uncertain. It necessitates the use of multiple accounts and various ICT systems. Theoretically, the situation may be altered by the full implementation of the Act on Electronic Delivery (point 7 of the first question), which is set to apply to courts only in 2029. However, in practice, uncertainty persists regarding the potential 'conflict' between the universal e-delivery system and the specific systems used in civil proceedings. Article 3, point 1, letter d of the Act on Electronic Delivery stipulates that the Act does not apply to the delivery of correspondence if separate provisions dictate the submission or delivery of correspondence using technical and organizational solutions other than the electronic delivery address. This includes accounts in ICT systems supporting court proceedings or document repositories. This provision allows for the coexistence of a common e-delivery system alongside specific systems in civil proceedings, with the specific systems taking precedence over the general model outlined in the Act on Electronic Delivery. Regarding the ePUAP system (for administrative and tax procedures), the Electronic Delivery Act outlines a phased-out transition (leading to the complete replacement of ePUAP with the e-delivery system). However, the Act does not establish a similar transition plan for any system in civil proceedings. Consequently, there is a risk that civil proceedings will be excluded from the country's general e-delivery system due to the existing solutions. Despite numerous imperfections, it's worth noting that civil proceedings remain the best-digitized court procedure in Poland.

In Austria a distinction must be made between 2 types of electronic service: Service by ERV and Service in accordance with the provisions of the 3rd section of the ZustG. In Austria, there is the electronic mailbox "Mein Postkorb", which is a central and secure mailbox for electronic messages from public authorities. The electronic mailbox is the collection point for the deposited documents. If the e-mail address to which notifications of service are to be sent changes, this shall be announced in the display module. It is the responsibility of the recipient to be reachable at the specified e-mail address for notifications of service. If the recipient has provided several electronic addresses,

notifications must be sent to all of these addresses. When addressed to a natural person, the notification of service is made in the citizen service portal oesterreich.gv.at or the app "Digitales Amt". Such deliveries should not be forwarded to the ERV. If an item is addressed to a company, it will be delivered either via usp.gv.at or, if applicable, the ERV. In addition, users of the ERV can choose whether they want documents delivered by the authorities to be delivered to the ERV as well (i.e. they will be forwarded), or whether the systems should remain separate. Obligated participants of the ERV will continue to receive all documents delivered to the ERV. In the ERV, electronic mail is not transmitted directly from the ERV participant to the competent court and back, but via specially authorised providers ("transmitting agencies"). Everyone who wants to participate in ERV must register with a transmitting agency. In principle, the ERV participant is free to choose which transmission point to use. However, the ERV software and the transmitting agency must match. For ERV outward traffic, participants can even register with several transmitting agencies at the same time. However, this is generally not advisable, because each exchange charges ongoing (basic) fees for its services and there would be several contact persons. For ERV return traffic, a participant must choose a specific transmitting agency so that the court knows where the return traffic will be delivered. In addition, there are also notifications of the tax authorities according to the BAO, which continue to be made via FinanzOnline using the "Databox". Furthermore, info mails are also sent to this databox informing that deliveries have arrived in the USP account. A notification should also be sent to the email address deposited with FinanzOnline. FinanzOnline and e-delivery are two different systems. However, both systems offer the possibility to receive official messages via an electronic mailbox. If a document has been delivered in FinanzOnline, USP will show that a delivery has been made in FinanzOnline. This means that messages from the tax authorities are still delivered to the FinanzOnline Databox, but the delivery is displayed as a message in "Mein Postkorb". In addition, "Mein Postkorb" enables the forwarding of deliveries after they have been opened; alternatively, an automatic collection into one's own operational system can also be configured via the "Mein Postkorb" menu. However, collection is only possible via a web service (SOAP-interface) and not via an e-mail programme. It is therefore possible to retrieve the messages automatically via a web service interface in one's own software solutions. For recipients of different delivery systems, the so-called "display module" ("Anzeigemodul") pursuant to § 37b ZustG provides a uniform overview of the delivery items held for them. It enables the function of a consolidated display and makes it possible to pick up the documents. However, the delivery items themselves remain with the respective delivery service and are only accessed via the display module.

In the Netherlands, citizens may consult government databases and systems using DigiD, which may be accessed by downloading an app or by username/password/SMS control. It is not possible to view and receive all mail in one system only. The user must access the relevant system to obtain the specific information.

In Sweden there is no general requirement to have a certified email. Individuals and entities can also register multiple email addresses that can be used for secure digital communications. It is not possible to view and receive mail in only one system, but this is usually possible if the document is sent to the person's email address. On the other hand, some authorities, such as the Swedish Tax Agency, use their own digital systems that require personal login information. When a message is sent via such a system, the recipient usually receives a notification via their email or digital mailbox. There is still no requirement for anyone to use these kinds of digital features.

5.5 How many local certified electronic systems (or providers) do you have?

Currently there are two governmental senders and two commercial mailbox providers in Slovenia. The courts are one source of certified mail and they are sending mail to commercial providers by the means of standardized interface (machine-to-machine communication). Development of additional receiving systems is possible (the system is open). The commercial providers are paid for every serving they make. The public administration has a separate system. The system is newer and has fewer registered users as recipients. Recipient can receive documents using portal but there is an option to send documents from this system to other compatible "mailbox" providers using standard protocol. This protocol is not fully compatible with the protocol of the courts. Because the public administration claims that there is no legal ground for paying to commercial service providers, currently there is no interest from them to join the network. Consequently not many users that already have a "court" mailbox are considering opening another one for public administration. The third system is the portal of tax administration. This system is fully closed as it does not even foresee the possibility for "machine-to-machine" communication and does not provide any open/public standard to allow for automated exchange of messages. The existing systems are incompatible.

In Poland all existing ICT systems in civil proceedings, including the Information Portal, fall under the administration of the Ministry of Justice. In contrast, the ePUAP system (for administrative and tax procedures) is administered by the Minister of Digital Affairs. The e-delivery system, established by the Electronic Delivery Act of 2020, will operate on a dual basis. This means that the address for electronic delivery can either be public (established through Poczta Polska) or private (created with a qualified provider as defined in the eIDAS regulation). Public authorities will be required to use a public address, while other individuals or entities will have the option to choose which address they prefer to use.

In Austria in principle, the authorities deliver messages centrally in "Mein Postkorb". In addition, the tax office continues to deliver to FinanzOnline (cf. § 5b FOnV 2006). In addition, there is also the ERV, to which the mandatory participants of the ERV receive the documents. The electronic mailbox "Mein Postkorb" can be accessed via the following portals: oesterreich.gv.at for citizens App "Digitales Amt" for citizens Business service portal usp.gv.at for businesses, eAMA for companies various public authority portals for employees of the administration, JustizOnline for citizens. Delivery services for electronic delivery are: Hpc DUAL Österreich GmbH (Briefbutler), Post Business Solutions GmbH (eVersand), Österreichische Post AG (MeinBrief), Bundesrechenzentrum GmbH (BRZ Zustelldienst), VENDO Kommunikation + Druck GmbH (Mein Postfach). In addition, there are communication systems of the authorities for the delivery of non-evidentiary official documents on the internet: AMA-KSB (operated by VENDO Kommunikation + Druck GmbH), SV-Postfach (operated by Dachverband der Sozialversicherungsträger), Bildungsportal – bildung.gv.at (operated by Federal Ministry of Education, Science and Research). In addition, there are some transmitting agencies that can be used to use the ERV: ADVOKAT Unternehmensberatung Greiter & Greiter GmbH, EDV-Technik Dipl-Ing. WENT GmbH, MANZ'sche Verlags- und Universitätsbuchhandlung GmbH, ÖGIZIN GmbH, UVST Datendienste GmbH.

In the Netherlands there are (at least) two centralised systems where citizens can obtain notices from the government. The courts have a specific system "Mijn Rechtspraak". This system may be accessed by citizens (using DigiD and eIDAS), organisations (using eHerkenning and eIDAS) and by professionals (via advocatenpas and eHerkenning). The Dutch administration has a centralised system "Mijn Overheid", where all the information of Dutch administrative authorities (including ministries, municipalities, as well as national and municipal taxes) is gathered in one place. Once logged in, the

citizen has access to one mailbox (Berichtenbox) for administrative matters. Citizens are not automatically conferred a mailbox. They need to register for these services

In Sweden the courts use one system connected to one server. Other authorities use different systems but they could be compatible in the sense that emails between authorities could automatically be encrypted. This means that emails are automatically encrypted. Other authorities do not use any of these systems. As each authority generally uses its own system it is hard to say how many local certified electronic systems there are in Sweden.

5.6 Are these certified electronic systems compatible? Is a user of one system able to receive certified electronic mail from other systems?

In Slovenia the public administration system is partially compatible with the court system in the sense that some upgrade of the protocol of the court is needed to provide the service for the public administration. But the systems are not fully compatible "out-of-the-box".

In Poland the systems are not compatible. While the law mandates interoperability between state-serving systems, this requirement is not effectively implemented in practice. It remains uncertain how compatibility will be achieved once the Electronic Delivery Act of 2020 is fully implemented.

In principle in Austria the ERV participant is free to choose which transmission point to use. However, the ERV software and the transmitting agency must match. For ERV outward traffic, participants can even register with several transmitting agencies at the same time. However, this does not make sense in the rules, because each exchange charges ongoing (basic) fees for its services and one would have several contact persons. For ERV return traffic, a participant must choose a specific transmitting agency so that the court knows where the return traffic will be delivered. Moreover, users can choose whether they also want documents delivered by the authorities to be delivered to the ERV (i.e. these will be forwarded), or whether the systems should remain separate.

In the Netherlands the systems are compatible since both use DigiD for logging in. However, once logged in, the user is not able to receive certified electronic mail from the other system. Therefore there is no direct data exchange between the systems.

In Sweden some of the systems are compatible with each other when it comes to sending secure emails.

5.7 Are any of the certified electronic mail systems compliant with the eIDAS Regulation, Article 43?

Not in Slovenia.

In Poland it seems that all of the systems described meet the requirements of Art. 43 eIDAS.

The legal qualification of the proof of delivery in case of e-delivery (§ 35 [3] ZustG) in Austria does not differ from conventional delivery. In the case of electronic service, none of the otherwise usual proofs of service are used, however, the record transmitted to the court is quite similar to a conventional proof of service in its informative value and function. The printout from electronic service or the electronic transmission of proofs of service must be considered as proof of service in analogy to § 116 Geo.

In the Netherlands Article 43 of the eIDAS Regulation is about the legal effect of an electronic registered delivery service. 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations; Do you rather mean if the electronic mail system is compliant with Article 44 of the eIDAS Regulation i.e. qualified electronic registered delivery service' means an electronic registered delivery service, which meets the requirements laid down in Article 44? (Either way, at the moment we have no specific information but would like to get a clarification on this point).

Currently not in Sweden.

5.8 What kind of charging model is in place to cover the costs of the certified electronic mail?

Currently in Slovenia only the court system is paying commercial providers to deliver the mail/documents. The pricing system is simplified, and the provider of the service is paid for every serving. The price for a serving is defined in the law and is fixed. The system of the commercial providers is free for the end users. One of the two commercial providers is offering additional services for additional price. Currently, because sending of documents to the court is not allowed, the commercial providers are completely dependent on a fee, collected from the court. Therefore, in essence, only the court is paying for the system and there would be no meaningful difference if the court provided the service end-to-end if the costs for the system would not exceed the costs that the court is now paying to the commercial service providers. Consequently, there are no cost-savings that would arise from compatibility and massive re-use of the existing systems. This may change, though, when the court starts accepting documents sent from the users (parties). When this happens, the income for the service providers will increase as the sending party will have to pay for the serving.

In Poland services via the Information Portal, correspondence through dedicated portals for individual procedures, as well as the ePUAP system, are currently entirely free. For example, the mere submission or receipt of a letter via the Courts Registers Portal does not incur additional costs. However, it's important to note that court fees related to specific procedural activities, such as entry in the register, are separate and must be paid accordingly. The situation is set to change upon the full implementation of the Electronic Delivery Act of 2020. E-delivery will replace registered letters, which currently involve fees at the post office. Therefore, e-delivery will generally be subject to a fee. An exception to this fee will apply for deliveries from non-public entities (such as citizens, entrepreneurs, or attorneys) to a public authority when using the delivery address provided by Poczta Polska. However, other deliveries, including those from a public authority to a non-public entity or deliveries by certified provider, will incur charges. Specific rates will be outlined in the providers' price lists.

The use of the ERV in Austria does not usually take place directly, but is handled by transmission agencies for which a fee is charged. The costs to the transmitting agency are a basic fee and fees for each transmission (for organisations that have to participate in ERV). On the other hand, ERV is free of charge for citizens using the upload service and the citizen card function to make electronic submissions to courts or public prosecutors' offices. Costs for mailings by way of electronic legal communication from ERV participants directly to others – such as for service pursuant to § 112 ZPO on other legal representatives – are not to be remunerated. The receipt of electronic deliveries is free of charge.

The system is free to the end user in the Netherlands.

In Sweden as far as the courts are concerned, the Swedish National Courts Administration, covers the costs for the courts' use of secure email. The cost of the product depends on the number of email addresses from which emails are sent. It is therefore recommended to use only one main mailbox for email in order to keep the costs down. Digital communication is free for individuals and entities. A fee is charged for some applications, which can be paid through the system used for uploading and signing of documents.

5.9 What are the options to receive certified mail (e.g. web interface, dedicated application)? Is it possible to receive certified mail using mobile devices?

Currently in Slovenia all service providers provide web interface (portal) for a manual reception of the documents. The web interface is mainly intended for desktop devices. Due to the lack of support of certificates on mobile devices, currently it is not possible to receive official mail on mobile devices. The main issue is electronic signature on mobile devices. This is supposed to improve with the introduction of the new personal ID that supports NFC and has certificate stored on the personal ID card. Slovenia is issuing new personal IDs from March 2022. At the end of 2022 about 300.000 IDs have been issued (Slovenia has about 2.000.000 citizens). An alternative would be to use governmental cloud for cloud-based signatures. Unfortunately the access to electronic signatures in the cloud is currently only allowed for public administration services. The new regulation is in place allowing access even to commercial entities, but technical standards are not yet in place and access is not yet operational.

It seems that only the Information Portal in Poland has a mobile version (both for Android and iOS). All systems provide web interface (portal) for a manual reception of the documents. The web interface is mainly intended for desktop devices, but you can freely use it through mobile devices.

Access to electronic deliveries in Austria is possible via "Mein Postkorb". This is available to businesses at the business service portal (usp.gv.at) and to citizens at the citizen service portal (oesterreich.gv.at). In addition, the "Mein Postkorb" service can be accessed via the smartphone app "Digitales Amt" for citizens as well as via the internet service portal of Agrarmarkt Austria and various public authority portals for employees of the administration. During the redesign of the electronic mailbox, special attention was paid to the mobile operation of the mailbox, so that optimal operation is also ensured on smaller screens such as smartphones or tablets. In contrast, the ERV is usually not used directly, but via transmitting agencies that forward the submissions to the Bundesrechnungszentrum GmbH, which in turn distributes them to the relevant courts and authorities (§ 2 ERV 2021). Furthermore, ERV software must also be obtained. At least one of the providers allows the use of a browser-based ERV client, which does not require installation on the ERV participant's terminal device.

Dutch certified electronic systems provide a web interface to access their services.

In Sweden at least regarding secure email communications from the courts, the messages could be accessed via computers and mobile devices. However, there may be a problem with opening the encrypted email on some devices and for some individuals and entities for example because of firewalls. The latter problem could be solved by the person or entity agreeing to open the links. Documents and attachments may not open with the standard web browser on Android devices, but this is possible if Google Chrome is used as the browser. If a document is sent with a code to several recipients, a common code should be used. The code used for confidential or sensitive messages will always be associated with a phone number when communicating digitally.

5.10 What kind of authentication is used when signing advice of receipt? Is it enough to just click a button "receive" or is there some kind of advanced procedure, e.g. electronic signature?

In Slovenia for the judicial servings and in public administration, electronic signature is required. For the tax administration, clicking on the button "receive" is enough to confirm the receipt of the document/message, therefore only authentication to access the system is used and later, when receiving servings, there are no additional technical measures, especially electronic signature is not in use.

In Poland each system is governed by its own set of rules. In the Information Portal, collecting a document is as simple as clicking 'collect' and confirming with a checkbox that you understand the implications of receiving the letter, which constitutes effective delivery in civil proceedings. In systems dedicated to specific procedures, there are distinct rules to follow. For instance, when accessing the Courts Registers Portal (and confirming your identity), you have several options: Using a Trusted Profile (a free, state-provided advanced electronic signature as per eIDAS). Using an e-ID (plastic ID card with a chip). Using the MyID tool (authorization performed via online banking). Utilizing a Qualified electronic signature as defined by eIDAS. Similar rules apply to the ePUAP platform.

In the case of deliveries with proof of delivery in Austria, the recipient must be notified that a delivery is available. In principle, the effectiveness of the delivery is linked to the first notification and is deemed to be effected on the first working day after the sending of the electronic notification. (§ 35 [5] and [6] ZustG), at the latest the item is deemed to have been delivered when it is collected. Pursuant to § 35 (3) ZustG, the delivery service has to record all data on the notifications and the collection of the document and transmit them to the sender. The entirety of this data constitutes the proof of delivery. If the document was not collected, this is evident from the proof of delivery. Nevertheless, it is up to the recipient to prove that an effective delivery did not take place (e.g. no knowledge of the electronic notification or absence from all delivery points). To pick up documents via "Mein Postkorb", which is provided for entrepreneurs on the business service portal, registration is required either via the FinanzOnline access or by means of a mobile phone signature.50 Service in the ERV is also deemed to be effected on the working day following the deposit in the recipient's electronic disposal area (irrespective of the actual collection, see § 89d [2] GOG). In addition, pursuant to § 2 (3) ERV 2021, the transmitting agency shall verify the identity of the natural person participating in electronic legal transactions and the identity of the person representing a legal entity including a partnership with legal capacity by means of an official photo ID, by means of another documented proof of reliability equivalent to that of a legal person (Art. 24 [1] lit a eIDAS Regulation), by using the citizen card function (mobile phone signature or chip card) or, in accordance with the technical possibilities, by means of the electronic proof of identity (E-ID, see §§ 4 et seq. E-GovG). In Sweden this varies according to the method of service and from authority to authority. Simplified service does not require an acknowledgement from the addressee. Acknowledgement could be oral or written in the case of standard service. An acknowledgement could be signed online, e.g. with a Word document, or in writing with a signature. As mentioned above, the courts also offer a system for digitally signing documents. This makes it possible to sign with an electronic ID. The Swedish Tax Agency offers similar possibilities, but currently only in a few specific cases. In general, there is no need to use advanced electronic signatures to open ordinary e-mails from the courts.

5.11 If electronic signatures are supported, what kind of electronic signature is required to receive certified electronic mail (according to eIDAS Regulation, e.g. qualified electronic signature)?

For the judicial servings in Slovenia, advanced electronic signatures are accepted. For the public administration service, it depends on the service. Some services were upgraded to use governmental cloud to require/create a qualified electronic signature, others are still using advanced electronic signatures. Tax administration used to require advanced electronic signatures but has lowered technical expectations to clicking a button in the web application (electronic signature is not in use anymore).

In accordance with the technical possibilities in Austria, signatures may be executed electronically, in particular under original documents of court decisions and protocols. In matters of jurisdiction in civil court proceedings, a signature shall be executed by means of a handwritten signature or by means of a qualified electronic signature (Art. 3 No. 12 eIDAS Regulation). If a signature is made by means of a qualified electronic signature, this shall be made visible on the signed document in a manner that makes it possible to recognise and verify who the signature is from (§ 89c [2] GOG). To collect electronic deliveries, the company must be registered at the USP, which is possible, for example, with the mobile phone signature. In addition, there is the app "Digitales Amt", which contains, among other things, a link to "Mein Postkorb". Activation of the mobile phone signature is required for this application. To use FinanzOnline, it is also possible to have an access code consisting of participant identification, user identification and PIN (or mobile phone signature). Pursuant to § 4 (1) of the E-Government Act ("E-Government Gesetz"; hereinafter: E-GovG), the citizen card serves as proof of the unique identity of an applicant and the authenticity of the electronic application in electronic public authority procedures. The authenticity is guaranteed by the qualified electronic signature contained in the citizen card. The unambiguous identification of a natural person is affected in his or her citizen card by the so-called personal binding.

The advocatenpas (the ID pass for lawyers) has been qualified in the Netherlands on the eIDAS reliability level as substantial.

In general, in Sweden, the only electronic signatures that are supported are those that result from the use of advanced electronic signatures such as Bank-id and Freja eID. This is generally also a requirement for digital mailboxes offered on the open market. However, services such as Bank-id, do not currently offer qualified electronic signatures. Questions regarding requirements for qualified electronic signatures have been discussed and evaluated. A general problem is that the Swedish market is limited and that such a requirement could hinder public revenue. There is no general national regulation regarding formal requirements of e.g. security level, for an electronic signature to be considered valid. As far as secure email for courts is concerned, the encrypted data can be opened without electronic signatures.

5.12 If signing advice of receipt or authentication to access certified electronic mail is in use, what assurance level is required to receive certified electronic mail?

In Slovenia it is most probably "high" for all services.

In Poland Information Portal has no specific requirements. Courts Registers Portal – both advanced and qualified electronic signature. E-Court (Electronic Writ of Payment Procedure) –

qualified electronic signature or unqualified electronic signature recognized only in the E-Court System.

In Austria the login for the mobile signature is doubly secured with a personal password and a TAN. First of all, the mobile number and the freely selectable signature password must be entered and then a window opens for entering the TAN. An SMS with a TAN and a comparison value is sent to the mobile phone, which must be entered in the TAN field or, alternatively, approved via the "Digitales Amt" app. Accordingly, a high level of security is provided for the reception because access to the electronic mailbox and the letters from the authorities is secured by the use of the mobile phone signature. If there is only a low-threshold login to the communication system of the authority by means of a username and password, only non-verifiable deliveries of that communication system will be displayed.

In Sweden there is no general answer to this question, as each authority has its own guidelines. But in general, the level of assurance is set at high.

5.13 Which operating systems are supported for receiving certified mail?

In Slovenia one of the commercial providers for court servings is providing signatures for Windows, Apple desktop (OSX) and Linux operating systems.

In Poland it depends on the system. In the case of E-Court, it must be Windows 7. The Courts Registers Portal allows Windows, Linux, and MacOS X. Other systems do not provide detailed data in this regard.

In Austria the electronic mailbox "Mein Postkorb" can be accessed via the following portals: oesterreich.gv.at for citizens, App "Digitales Amt" for citizens, Business service portal usp.gv.at for businesses , eAMA for companies, various public authority portals for employees of the administration, ustizOnline for citizens. "Mein Postkorb" as well as the download of message attachments was tested with the following operating systems and browsers: Windows 10 10H2, macOS Montery 12.0.1, Android 13, iOS 16.4, Chrome 113.0, Firefox 102.11.0esr, Safari 16.5, Edge 112.0. In order to use the "Digitales Amt" app, the smartphone or tablet must have the operating system version Android 8 or higher, or the operating system version iOS 12.1 or higher, as well as the fingerprint or facial recognition/iris recognition function. In the case of an Android device, a device that supports the Android BiometricPrompt API is required. eAMA is only supported by the operating systems Windows 11 and Windows 10 as well as the browsers Google Chrome, Mozilla Firefox and Microsoft Edge. FinanzOnline is supported by Microsoft Edge from version 12, Mozilla Firefox from version 27, Opera from version 12.18, Google Chrome from version 30, macOS Safari from version 7, iOS Safari from version 6 and Android browsers from version 5.0. In order to participate in ERV, the use of a software application is required. The platforms supported by the respective software providers differ depending on the software provider: The software "avviso" from DATA-team GmbH supports the Citrix terminal server. The software "jurXpert" from ACP Business Solutions GmbH supports Windows 2000 to Windows 7 as well as Win-Server 2003, Win-Server 2008 and Linux. The software "KIM ERV" from PSC Public Software & Consulting supports Windows XP or higher. The software "MANZ webERV" from MANZ Verlags- u Universitätsbuchhandlung GmbH supports Firefox, IE, Safari, Chrome and all platforms. The software "medixPro" from Meix Informatik GesmbH supports Windows 2000 to Windows Vista as well as Apple (e.g. with Parallels). The software "POWER ANWALT" from Uhrwerk - Zeitgerechte Computerlösungen Mag. Karl M. Bauer GmbH supports MacOSX, Win2000, Win XP and Win Vista. The software "R/WIN" from ACP Business Solutions GmbH supports Windows. The software

"WinCaus.net" from EDV2000 Systembetreuung GmbH supports Windows XP, Windows Vista, Windows 7, Win-Server 2003, Win-Server 2008, Terminal Server and Citrix.

In Sweden the courts use their own electronic systems and Microsoft Exchange for email in general. The system accepted by the courts for electronic signatures is digital IDs with advanced, but not qualified, electronic signatures, such as Bank-id.

5.14 Is there public API (Application Programming Interfaces) available, that would allow machine-to -machine communication (e.g. developing own software to receive certified mail in a law office for example) with the certified email provider services? If yes, are they standardized or different for every provider?

In Slovenia there is a public API provided by one of the private certified email service providers but it is not standardized and works only for those citizens who have registered with this service provider. There is also a public API for the machine-to-machine communication provided by the court system. It is intended for both, commercial service providers for end users and for larger recipients of certified mail. Currently only commercial providers are using this API. The API is documented and opensource solution exists (Laurencius). This answer is still in detailed research.

In Poland the systems offer external integration via API (see e.g. the Court Registers Portal - ; ePUAP -). However, it's important to note that each system has its own unique rules, and sharing regulations are not standardized.

In Austria special software is required to record and send the data and to receive the ERV return traffic. The software converts the data into exactly those data formats that are specified by the Federal Computing Centre. Data that do not comply with these specifications cannot be submitted to court. The software for using the ERV is offered by commercial providers. Requirements on the participant side for participation in the ERV are: Software application for webERV (solutions of the software providers or own development), Internet connection to the transfer point supported by the respective software application or certified by the transfer point. Valid address code (ADVM code). An overview of commercial and non-commercial software products can be found in the "Ediktsdatei" of the Federal Ministry of Justice. "Mein Postkorb" enables the forwarding of deliveries after they have been opened; alternatively, an automatic collection into one's own operational system can also be configured via the "My Inbox" menu. However, collection is only possible via a web service (SOAP interface) and not via an e-mail programme. In the course of automatic collection, deliveries are retrieved via a web service interface and can be transferred to your own software solution.

In Sweden there is a public API provided by some public authorities. However, it is generally not developed for most public authorities in Sweden. The Swedish National Courts Administration is working on developing a platform for digital infrastructure for information exchange.

5.15 Are standards for the implementation of certified electronic service publicly available? If yes, please provide a link to the specification.

In Slovenia there is documented API provided by the court. IT is also implemented in a form of a test system (Laurentius) that is open sourced, but this solution is not used by the court itself and is not being maintained. This answer is still in detailed research.

In Poland for some systems, there are many publicly available manuals and technical information. In the case of others, they may not be posted on the portal's website, but they can always be obtained from the platform's public administrator through access to public information.

In Austria delivery services must deliver official documents to recipients. According to § 29 (1) ZustG, delivery services must provide certain services or fulfil certain conditions, such as certain technical requirements for the receipt of documents (No. 1), offer a procedure for identification and authentication (No. 3) or ensure notification of the sender in case of non-collection (No. 5). Accordingly, delivery services must ensure the proper fulfilment of the delivery service, have the necessary technical and organisational capacity and sufficient legal reliability.70 The operation of a delivery service requires a licence issued by the Federal Minister for Digitalisation and Economy (§ 30 [2] ZustG). On its website, the Federal Ministry of Finance provides information on the approved delivery services including further information on the legal basis and specifications. These regulations and specifications are derived from the Delivery Act, the Delivery Services Ordinance and the Delivery Forms Ordinance. Technical information on the ERV, transmitting agencies and interface specifications as well as authorised transmitting agencies and an overview of commercial and non-commercial software products can be found on the website of the Federal Ministry of Justice.

In general in Sweden, no. The use of APIs by public authorities is still very limited and in most cases authorities uses different systems. The systems might be publicly available in the free market, but this is not something that the authorities provide information about in consideration of security risks. Documents regarding authorities APIs could be official ones according to the The Freedom of the Press Act, but in some cases these documents will be confidential in the relation to the suppliers, or it will demand a unreasonable work effort from the authority resulting in that a compilation of APIs will not be considered as an official document.

5.16 Is there an opensource example solution for certified electronic mail readily available that can be used by the entities receiving and sending certified mail? If yes, is there a sustainable support for further development of the solution and is it regularly updated or has development stalled?

In Slovenia there is an opensource solution for the court system (Laurentius). It is not being actively maintained. The court is using a spin-off code that was later not publicly released. Therefore, sustainable support for the sample receiving software does not exist. End-users of this solution are left to their own efforts to maintain the software if they intend to use it. Poland: I'm not aware of any Polish open-source software for these tasks.

In Austria The Federal Ministry of Justice publishes approved transmitting agencies and information on commercial and non-commercial software products on its website. MOA-ZS is an open-source middleware designed to facilitate access to e-delivery for specialised applications by simplifying the number of interactions with e-delivery components such as the subscriber directory and delivery services. The main focus is on easy handling of communication with MOA-ZS via a uniform interface for easy sending of deliveries or processing of proofs of delivery and status information. There is also openZUSE. openZUSE is an open source framework, which implements all necessary tasks for senders of the Austrian document delivery system (DDS), the official Austrian certified mail system for the public sector. This project provides Java 6 APIs for all modules used in Austrian eGovernment for electronic delivery (eDelivery). It provides basic building blocks to communicate with Austrian central

and distributed electronic delivery systems and can be used to create a more customized application than the standard MOA-ZS Application.

In Sweden in general, only the electronic services for sending and signing electronic documents are established. These services are connected to the Swedish Courts Administration and support is available via the website where the user can contact the relevant court. The use of electronic mailboxes is open to the public but these services are maintained by public entities and are not currently influenced by the government.

5.17 Are certified electronic mail services suitable / can be used for commercial/personal use (e.g. can a company send certified electronic mail only to the court or can it use the same system to send certified electronic mail to another company)?

This is not something that was envisioned by the court or some kind of governmental system in Slovenia. Commercial service providers that are providing services for the court have also implemented commercial options to deliver certified mail. This was their solution to diminishing returns of the system as it is not widely used and is more or less financed only by the court servings.

In Poland all existing systems only facilitate communication between individuals and state entities. Therefore, entrepreneurs and citizens cannot use these platforms to exchange correspondence with each other. However, this situation will change with the implementation of the 2020 Act on Electronic Delivery, which will enable remote communication not only vertically (between a public authority and a citizen) but also horizontally (between citizens or entrepreneurs).

In Austria direct service by participants" ("Teilnehmer-Direktzustellung", not explicitly regulated by law) is the - technically enabled - possibility of direct transmission of documents between participants in the ERV within the framework of computer programmes used for the ERV. It is primarily used for the transmission of documents intended for an opposing party in civil court proceedings by one party to another party of the proceedings. In this regard, there is a legal framework, such as § 112 ZPO, which also allows for such transmission by electronic mail: § 112 ZPO provides that if both parties are represented by lawyers, each of the lawyers who submits a pleading has to send a copy of the pleading intended for the opponent to his lawyer by messenger, post or by fax or electronic mail. This electronic transmission is possible via all webERV transmitting agencies. In addition, there is the insurance portal (VU-ERV). Some large insurance companies approached the working group of ERV companies in order to be able to communicate legal protection cases between lawyers and insurance companies in a structured and large-scale manner. For this purpose, an IT company specialised in insurance applications developed a new data structure based on the aforementioned participant direct delivery.

In the inbox (Berichtenbox) of “Mijn Overheid” in the Netherlands, like a regular (physical) mailbox, citizens can receive messages. However, the sending of messages by citizens via that inbox is not possible. Via “Mijn Rechtspraak” the citizen / organisation / professional may submit documents and motions to the court.

The secure communication offered by the courts in Sweden could only be used between public authorities or between persons/entities and public authorities. Private systems could be used in other ways.

5.18 Is there a central register of certified electronic mail addresses allowing the sender to learn whether the recipient accepts certified electronic mail?

There is no single central system in Slovenia from which a sender could determine if the recipient has an "official electronic mailbox". There is also no requirement for either natural or legal person to open such a mailbox or registered it in any kind of register. The government does not provide an "official mailbox" to every natural or legal person.

There is currently no central database of electronic delivery addresses in Poland (including for the ePUAP system functioning for administrative and tax proceedings). The situation will be changed by the full implementation of the Electronic Delivery Act, which will result in the creation of an centrally administered Electronic Address Database (Baza Adresów Elektronicznych, BAE). The database will be a public register maintained by the Minister of Digital Affairs, and will contain information on addresses for electronic delivery of public and non-public entities. Both public addresses (from Poczta Polska) and qualified addresses (from private qualified providers within the meaning of the eIDAS regulation) will be entered there. Entering an address for electronic delivery in the database will be tantamount to a request for delivery of correspondence sent by public entities to this address. In the case of entrepreneurs, their electronic addresses will also be visible in public databases of entrepreneurs (the National Court Register for companies and the Central Register and Information on Business Activity for entrepreneurs-individuals).

In order to make electronic delivery more efficient in Austria, a directory of participants was introduced, which includes all persons, companies and authorities of all delivery services that are registered for electronic delivery (§ 28a ZustG). This subscriber directory can be queried by delivering authorities, which makes it possible to find out whether a recipient can be reached. Participants in the ERV are also included in this directory. However, those obliged to participate in the ERV may object to the transfer to the directory of participants pursuant to § 28b (5) ZustG. According to § 34 ZustG, the delivering authority has to determine by electronic query of the directory of participants whether the participant is registered with the directory and whether there is any reason for exclusion. In the course of this query, the authority is also informed whether deliveries can only be made via a specific delivery system.

In the Netherlands registration in each system is on a voluntary basis. The government does not provide a mailbox to each person.

There is no central system in Sweden that would allow a sender to determine whether the recipient has an "official electronic mailbox". There is also no obligation for a natural or legal person to open such a mailbox or to be registered in any kind of register. The government does not provide every natural or legal person with an "official electronic mailbox". It is possible for a person to register for a digital mailbox, but this system is provided by private companies. If a person has a digital mailbox, this information can be made available to public authorities using such a system, making it possible to receive documents from public authorities directly through the digital mailbox. This requires that both the authority and the individual are connected to the digital mailbox. There is currently no legal requirement for such a connection. The same could be said about electronic IDs. The courts do not currently use digital mailboxes to communicate with individuals or organisations. Some authorities also provide their own alternatives to digital mailboxes, such as My Pages and other solutions. In general, this requires the user to be able to identify him or herself by means of an electronic ID. However, the Swedish Government has appointed a government inquiry into the obligation for persons and entities to have a digital mailbox and the obligation for public authorities

to send and receive secure digital email to digital mailboxes. The findings of the inquiry shall be reported in 2024.

5.19 Is certified electronic service centralized, if yes, who runs the service (e.g. government)?

The service is centralized in Slovenia in different procedures. For example, the court has a sending/receiving system, one was developed for the public administration and a separate one for the tax administration. All three systems are run by the government. Though from the court the documents cannot be served directly to the end user, the court is sending only through the commercial service providers. On the other hand public administration allows recipients to receive messages on the portal of the public administration, although theoretically an option to send messages through commercial service providers exists. For the tax administration the messages can only be received directly on the portal of the tax administration and there is no possibility to serve through commercial service providers.

All the described modes of electronic delivery can be considered centralized in Poland, with the exception of the Information Portal. Formally, an Information Portal is established for each court appellation (Poland has 11 courts of appeal, so there are 11 Information Portals in total). On the other hand, the Courts Registers Portal, e-court, ePUAP, and the upcoming e-delivery system are/will be standardized nationwide. As previously mentioned: The Information Portal is formally established by the president of the court, but day-to-day administration falls under the Ministry of Justice. The Courts Registers Portal and e-court are also systems under the Ministry of Justice. ePUAP is managed by the Minister of Digital Affairs. The e-delivery system, on the other hand, will consist of several components: The public box will be administered by Poczta Polska, which, although formally a joint-stock company, is wholly owned by the State Treasury. De facto, the e-delivery portal currently operates on state servers (within the government domain, gov.pl). Qualified mailboxes will be administered by qualified (private) providers. The database of electronic addresses will be managed by the Minister of Digital Affairs.

The management of the MijnOverheid website is carried out by Logius in the Netherlands. Logius is the digital government service, part of the Ministry of the Interior and Kingdom Relations.

In Sweden the service is centralised in different procedures like in Slovenia. For example, the court has a sending/receiving system, one has been developed for the public administration and a separate one for the tax administration. All systems are operated by the respective public authorities. In general, the authorities use their own servers for storing and sending digital communications. There are also authorised service companies that provides service. This is regulated by lag (2010:1933) om auktorisation av delgivningsföretag (Act on thef Authorisation of Service Companies).

5.20 If the certified electronic service is not centralized, who is running the nodes? Public entities or private entities? What are the responsibilities of the parties involved? Please explain relations between the entities.

Private entities are running the nodes to receive "certified mail" in Slovenia. Private entities can enlist with the public entities (that is court or public administration) if they fulfil certain technical

requirements and pass the test of the computer interface. If they pass the test, they can sign a contract with the government and then provide the service to the end users.

The justice authorities are the owners of the ERV and use various back-office systems that are connected to it in Austria. All these systems are hosted at the Federal Computing Centre. These are especially the European order for payment procedure (EUM), the land register (GT), the company register (FB) and the procedural automation of the justice system (VJ). With the ERV, electronic mail is not transmitted directly from the ERV participant to the competent court and back, but via specially authorised providers ("transmitting agencies"). The transmitting agencies collect the submissions from their end users, check them for formal correctness and forward them to the Federal Computing Centre. From there, they are distributed to the courts and public prosecutors' offices. The justice authorities have thus transferred a number of subtasks to transmitting agencies within the framework of the ERV. These are IT companies that have applied for the service to be provided by means of award procedures and have been commissioned by the Federal Ministry of Justice for a limited period of time. Legally, the Ministry of Justice grants them service concessions. In purely practical terms, they are entrusted with (partial) operational and distribution aspects of services provided by the Federal Government. The transmitting agencies are connected to the Federal Computing Centre via dedicated lines or virtual channels (VPN).84 Approved transmitting agencies are:85 ADVOKAT Unternehmensberatung Greiter & Greiter GmbH EDV-Technik Dipl.-Ing. WENT GmbH MANZ'sche Verlags- und Universitätsbuchhandlung GmbH ÖGIZIN GmbH UVST Datendienste GmbH. In the case of electronic delivery, delivery is carried out via the official delivery service "Mein Postkorb".86 "Mein Postkorb" simplifies the registration for electronic delivery and the access to electronic messages. After the registration, all messages can be viewed and collected in one place.87 Approved delivery services are:88 Hpc DUAL Österreich GmbH Post Business Solutions GmbH Österreichische Post AG Bundesrechenzentrum GmbH VENDO Kommunikation + Druck GmbH.

If the certified electronic service, mailbox or email, is not controlled by a public authority, private entities will run the nodes in Sweden. There are no specific regulations for e.g. electronic mailboxes. In general, only public authorities are allowed to use electronic service. There is a framework of rules concerning the quality mark Svensk e-legitimation (Swedish e-ID) which has three levels of security. However, there is no national regulation on the definition of an electronic ID (or digital mailboxes). There are also requirements for such services when they are used for banking purposes, according to the regulations on financial services.

5.21 How does the commercial model for the certified electronic mail system work? Is it government funded? If not, how are the prices regulated/formed?

In Slovenia the model is based on the price defined in the law. Only the court is paying commercial service providers to deliver the mail/documents. Public administration has no such provisions. Currently that means that only for the courts commercial providers are willing to deliver the messages and there is no interest for integration with the public administration. The consequence of this is decentralization of mailboxes for the end users – If they want to participate in electronic delivery services, they need to check three different mailboxes (for now).

The market for qualified providers is still in its early stages of development in Poland, as the Electronic Delivery Act of 2020 is currently being implemented. We only have two qualified providers: KFJ Inwestycje sp. z o.o, and ASSECO DATA SYSTEMS S.A. These entities are privately owned. Each of these

entities (more may emerge over time) independently sets prices through regulations, guided by market principles.

The costs for electronic deliveries are negotiated with the delivery service providers in Austria. The receipt of electronic deliveries is free of charge. When using the ERV, a basic fee and fees for each transmission are charged by the transmission agency. No costs are incurred when using the ERV by way of the upload service. In addition, the use of software is required, for which fees are charged. D. Zoubek, supra n. 8, p. 192. Bundesministerium für Justiz, 'Elektronischer Rechtsverkehr (ERV) und elektronische Akteneinsicht (eAe)', , visited 10 July 2023. Amt der Steiermärkischen Landesregierung, 'Elektronische Zustellung', , visited 10 July 2023. 87 Bundesministerium für Finanzen, 'Allgemeines zur elektronischen Zustellung', , visited 10 July 2023. Bundesministerium für Finanzen, 'Technische Informationen', , visited 10 July 2023. Bundesministerium für Finanzen, 'FAQs – eZustellung für Behörden', , visited 10 July 2023. Bundesministerium für Justiz, 'Elektronischer Rechtsverkehr (ERV)', , visited 10 July 2023. Die Kosten dazu aufgeschlüsselt von ADVOKAT, 'Web-ERV vom Marktführer', , visited 10 July 2023; EDV-Technik DI Went GmbH, 'WebSUITE-Combi. Automatisches Abfrageprogramm – Useware', , visited 10 July 2023; MANZ, 'Elektronischer Rechtsverkehr. webERV Service', , visited 10 July 2023; UVST Datendienste GmbH, 'Über UVST Datendienste GmbH', , visited 10 July 2023. The amount of the fees is an evaluation criterion in the course of the procurement procedure. Typical services to be remunerated are, for example, a fee for a delivery item from an addressee to a court, monthly basic fees per addressee or fees for the issuing of certificates. The Federal Ministry of Justice remunerates the delivery of courts to an addressee per delivery item to transmitting agencies. The amount of the remuneration is a single-digit percentage of the costs that the justice system would incur for postal delivery.

In Sweden the public authority in question will bear the cost of the use of its digital systems when communicating with the parties. For some communications, such as applications, there may be a statutory fee associated with the application. However, this is generally not related to the use of the electronic system, as the fee is linked to the application, whether or not it is completed electronically.

5.22 Is it possible to send cross-border certified electronic mail using existing systems? If yes, please explain shortly how.

Currently there is no possibility to use existing systems for cross-border servings in Slovenia. We could not find any information that such capabilities were planned.

In Poland none of these systems are linked to systems in other countries for cross-border correspondence.

The ERV in Austria can also be used from abroad, namely by way of an ERV transmitting agency, from which an ERV registration code can be requested. Especially European lawyers providing services are obliged to participate in the ERV when representing clients before Austrian courts. Foreign participants in the ERV, do not have to have a domestic delivery point to register with a delivery service (§ 35 [6] ZustG).

At least as far as the courts are concerned, it is possible to send secure emails to recipients abroad in Sweden. If a code is required, an area code must be added to the phone number used for the code message.

5.23 Is your system of certified electronic mail directly connected to eIDAS network (cross-border)?

Currently none of the systems are either eIDAS certified or connected to the cross-border eIDAS network in Slovenia.

It appears that a "Trusted Profile" (a free advanced electronic signature provided by the state) has been reported from Poland. It allows for identity verification, the creation of the account and submission of an electronic signature in various systems, including ePUAP and the Courts Registers Portal.

There is no direct connection to the eIDAS network in Austria, because this does not exist in a technical sense. However, registration with foreign electronic certificates is possible via a "country selection".

Not in the Netherlands, though to access the digital services MijnRechtspraak of the Dutch courts, it is possible to log in using eIDAS (as citizen and organization). It is also possible to access MijnOverheid logging in with eIDAS.

Currently none of the systems are either certified in accordance with eIDAS or connected to the cross-border eIDAS network in Sweden. However, this issue is being evaluated by some of the designated authorities at the request of the Swedish government. The Swedish Prosecutor Office has published a report concerning the evaluation. The report states that an alternative could be to purchase a service that meets the requirements of the Regulation. However, it is also mentioned that the relevant Swedish market is limited and that there are only two registered providers according to the Central Authority's list of entrusted national services. It is also an exception that Swedish authorities use such electronic signatures and that the national law is in no case stricter than the Regulation. There are also very few authorities that have developed systems for validating such signatures and stamps. The report lists several problems with the implementation of eIDAS, mainly related to the unresolved national issue of the implementation of the e-CODEX system. On the other hand, some public authorities are using systems for the digital management of employer IDs, which seems to be in line with the requirements of eIDAS and could be a basis for further development. The same can be said about the e-ID solutions offered by the open market, such as Bank-id, but the report states that these services are not compatible with the highest security level of eIDAS. There is also a published Swedish Government Official Report on the topic which describes and evaluates the eIDAS system. One of the main findings of the report is that the development and need fo digitisation in the public administration is increasing, bringing with it new challenges, demands and expectations. However, the report states that there is no isolated value in increased use of entrusted services in public administration. Instead, the value was described as purposeful usage of entrusted services. The report also states that the main need for development concerns the use of electronic signatures, for example clearer rules and principles for validation. Another problem raised was the Webpage of the Swedish Government regarding assignment to inquiry the implementation of digital communication. Report from the Swedish Prosecutor Office regarding implementation of digital communication for legal cooperations in the European Union, preservation of documents with electronic signatures. A solution to this problem was presented namely the use of a proof of validation.

5.24 Is local certified electronic mail service connected to the e-Codex system?

Currently not in Slovenia.

For Poland there is not any information confirming this.

The ERV in Austria has been connected to e-Codex.

Currently there is no connection in Sweden.

5.25 Is e-Codex system in active use in your Member State?

There are some indications that e-Codex is active in the system of the public prosecutors in Slovenia.

In the years 2017–2019, the project consortium in eCODEX-Plus project aimed to ensure easier access for citizens and entrepreneurs to the justice system in Europe by using ICT solutions, by creating IT tools to handle cross-border civil proceedings. As part of the project, technical solutions enabling electronic submission of procedural documents and delivery of court documents were implemented on a pilot basis. As a result of the technical pilot, three Polish courts were connected to the e-Justice infrastructure - the District Court for Wrocław-Downtown in Wrocław, the District Court in Wrocław and the Court of Appeal in Wrocław.

Austria already has many years of experience with e-Codex and successfully uses this electronic means of transmission, for example, in the EU order for payment procedure.

There is active system in the Netherlands.

The Swedish government has commissioned the Swedish Prosecutor Office and a number of other designated public authorities to evaluate the implementation of the system. The Swedish Prosecutor Office has published a report its findings and proposals. The system is not yet in use in Sweden and there is no indication of when it might be actively used.

5.26 Is the use of e-Codex system centralized or decentralized? Can you please list the entities using the e-Codex system, what are the roles and responsibilities of those entities in the system?

There is no information of any development of the system in Poland, except for the pilot program under the eCODEX Plus project. There is no information about this on government or court websites.

e-CODEX is currently operated centrally in Austria by the Federal Computing Centre on behalf of the Federal Ministry of Justice. The national ERV and e-CODEX are linked so that theoretically all ERV users, i.e. about 10,000, can also use e-CODEX. In reality, e-CODEX is currently used primarily in the EU order for payment procedure by Austrian lawyers and the competent District Court for Commercial Matters in Vienna and in the EU investigation order, for which a pilot operation is currently running at the Vienna Public Prosecutor's Office for electronic communication with other European prosecution authorities.

In the Netherlands Justitiële Informatiedienst (Justid), an agency of the Ministry of Justice and Security, is the central point in the Netherlands.

The implementation of the system is still being evaluated and the common IT system has not yet been implemented by Sweden.

5.27 Do you have any laws in place defining when and under what circumstances the (digitized) copy of the original document has the same value as the original document (e.g. if you scan physical document in electronic form, like PDF format)?

Slovenia has a special law on archiving that defines under which circumstances the copy of the document is equal as the original under the law. Though this law is (because of complexity) only practically applicable to legal persons. There are no clear provisions for the natural persons (that would for example want to send a scanned document to the court as a proof – either by certified electronic mail or during a teleconference). This answer is still in detailed research and needs further elaboration.

In accordance with procedural regulations, the catalog of evidence in civil proceedings remains open in Poland. A scanned document may be utilized as evidence in civil proceedings since Polish civil procedure imposes no restrictions on the admissibility of evidence from electronic documents (it is considered a permissible form of evidence). Only in exceptional cases, as per Article 129 § 4 of the Code of Civil Procedure, 'If justified by the circumstances of the case, the court, upon the request of a party or ex officio, may require the party submitting a copy of the document to also submit the original document.' In terms of substantive law, the fundamental regulations concerning electronic format can be found in the Civil Code. The regulations concerning the form of legal acts (contracts or unilateral declarations of intent) prescribe several types of forms. When addressing this question, two key forms come into play: electronic form and documentary form. ELECTRONIC FORM: As per Article 781 of the Civil Code, the electronic form is upheld when the declaration is submitted electronically and bears a qualified electronic signature. In such cases, the submitted declaration of intent is deemed equivalent to a written declaration of intent. DOCUMENTARY FORM: Conversely, the documentary form is a broad category encompassing all types of documents. A document, as defined by Article 773 of the Civil Code, is any medium that enables the content of information to be read (including email, text messages, etc.). Therefore, if we have an electronic document that lacks a qualified signature under the eIDAS regulation, we are dealing not with an electronic form but a documentary form. According to Article 771 of the Civil Code, to maintain the documentary form of a legal act, it is sufficient to submit a declaration of intent in the form of a document in a way that enables the identification of the person making the declaration (e.g., sending an ordinary email from your mailbox).

Austria: § 89c (2) GOG stipulates (to the extent required by the ordinance pursuant to § 89b [2] GOG) that enclosures to electronic submissions must be attached in the form of electronic documents (original documents or electronic copies of paper documents) in Austria. The creation of an electronic documents archive has made it possible for the version of a paper or electronic document stored in the archive to be considered the original. With effect from 1st January 2007, the data content stored in such an archive shall be deemed to be an original of the document stored until proven otherwise. The reference to the storage in the archive combined with the sending of a utilisable version of the electronic document or an effective authorisation to access the data of the stored document shall be deemed equivalent to the submission of the original of the document (§ 13 ERV 2021; § 91c [2] GOG in conjunction with § 91b [7] GOG, "fictitious original submission"). This electronic transmission replaces the submission of an original. The data stored in this archive is considered to be the original of the recorded document until proven otherwise (§ 91b [7] GOG). There are exceptions to the requirement that the electronic document must be stored in a document archive (e.g. document archive of the Austrian notary's office). According to § 1 (1a) ERV 2006, documents provided with an official signature pursuant to §§ 19 et seq. E-GovG may be submitted by public authorities as PDF attachments in accordance with the interface description pursuant to § 5 (2) ERV 2006.

There are no rules defining the terms original or copy in the Netherlands. However, the Dutch Code of Civil Procedure (RV) has rules on the use of copies of documents in the civil procedure. Based on article 85 para 1 RV, the parties have the right to file copies of the original documents, which they filed as evidence in the procedure. According to article 160 para 1 RV, these copies have the same effect as the original document. However, based on article 85 para 2 RV the parties have the right to claim to see the original document and not the copy. In such a case, the party who filed a copy of a document is obliged to show the original document to the court as well as to the other party. In such an event, the court examines whether the original document corresponds with the copy.

In Sweden the value attached to a document depends on the particular case and its circumstances. In some parts of the legal system, for example regarding transfers of real property and testimonies, there are special formal requirements for a contract to be legally binding. This may mean that a copy of the original document is invalid. In other situations, the answer is no and the principle of free sifting of evidence will apply (see question 32). With regard to electronic signatures, an old law, now rescinded, provides some guidance. The rescinded law was an implementation of the earlier Directive 1999/93/EC and contained provisions according to that Directive, for example some definitions and provisions on the issuance of certificates. According to the preparatory works, the usual rules of burden of proof should be applied with regard to objections of counterfeiting should be applied. It was not considered appropriate to lay down special rules for electronic signatures, taking into account the medium used. Instead, it was stated that the crucial point was what kind of information was confirmed by the signature, what kind of legal act was relevant and what relationship should be proven where the relationship between the parties could also be relevant. However, these reasons should not be seen as an exclusion of specific advantages associated with qualified electronic signatures in relation to questions of evidence. One possible conclusion could be that a qualified electronic signature confers a stronger presumption of validity than a non-qualified one.

5.28 How would the court proceed when checking if the documents provided to the court can be given the same value of proof as to the original?

This answer is still in detailed research and needs further elaboration, but during expert meeting in Wroclaw other member states reported that the court (in some other member states) would accept the proof and request access to the original only in a case if there was some kind of doubt in the authenticity of the document.

This procedure is accurate under Polish law. The court accepts electronic evidence and requests access to the original only when there are doubts about the document's authenticity or if there were other circumstances justifying the need to view the original. It should be noted that, in principle, the failure to provide the original document does not entail specific procedural sanctions. Nevertheless, if the request is not honored, the court assesses the evidence. According to Article 233 paragraph 2 of the Code of Civil Procedure, the court, after a comprehensive review of the collected evidence, determines the significance of the party's refusal to present evidence.

§ 299 ZPO provides for the possibility of ordering a party to submit the "Urschrift", i.e. the original in Austria. Therefore, according to the prevailing opinion, documents do not have to be submitted in the original, a copy ("Abschrift") is sufficient. If the original is not presented, the statutory rules of evidence (§§ 292, 294, 310, 312 ZPO) apply and the document is fully subject to the free assessment of evidence. In doing so, the court shall take into account the reasons given for the failure to produce the original. The electronic documents deposited in the archives of documents are deemed to be

originals (§ 91c [2] in conjunction with § 91b [7] GOG; cf. § 110a [5] NO; §§ 140b and 140e NO). Until proven otherwise, the data stored in the certification archive of the justice system shall be deemed to be the original of the stored document (§ 91b [7] GOG).

In Sweden, for example, the court might check who is providing the documents and whether the email address looks legitimate. If there are indications that the document is not genuine or has been tampered with, the public authority could try to contact the party or its representative. It could also ask for the document in its original form. In court proceedings, the general principle of free sifting of evidence applies (Section 35, Chapter 1 of the Swedish Code of Judicial Procedure). This means that it is up to the court to decide what evidential value the document may have. A limitation in general civil litigation, which may be a problem in complex cases, is that a court may not ex officio collect evidence (Section 35, Chapter 6 of the Code of Judicial Procedure), which may prevent the use of special competence in questions concerning the validity of electronic acts, if the parties do not refer to such evidence.26 This addresses the general problem that the courts do not always have adequate knowledge of electronic documents and their validation, which can be seen as a consequence of the lack of rules on the subject. The use of electronic signatures as evidence has been addressed by the Swedish Supreme Court in for example NJA 2017 s. 1105. In the case, the Supreme Court stated that if a user of an electronic ID objects that his or her ID has been used without authorisation, the actor demanding payment on the basis of the signature must prove that the user's ID has been used. If this is proven, it is up to the holder of the ID to presume that the ID has been used without authorisation (which is a low standard of proof). The case also contains general findings about electronic signatures and shows how the use of electronic signatures is reflected in topical judicial issues. However, the existence of an advanced electronic signature in this case has been debated and the findings of The Supreme Court that the financial company had proven that a qualified electronic signature had been used have been questioned. Regarding questions of the validity of electronic signatures, the main rule is that there are no formal requirements for a valid signature which means that the principle of free sifting of evidence will apply. However, the eIDAS-regulation and its requirements may be useful in asserting such questions but the answer is uncertain due to lack of sources. It has been suggested that a signature that does not meet the requirements of Art. 26 eIDAS, might still be valid as an electronic signature but with a lower level of security. The conclusion is therefore that in situations where there are no formal requirements for validity, the question will be targeted as an evidential one where an advanced one might have a stronger presumption of validity reflected in a lower burden of proof and evidentiary requirements. In relation to documents with electronic signatures, a government inquiry found that it should be considered whether it is appropriate to use validation proofs for such documents. This could provide a derivable chain of evidence to show the original validation of the signature, even after the signature's control function has expired. This has also been described as being in line with the principle of free sifting of evidence and the Swedish Supreme Court case cited above. In conclusion, the proof of validation could be helpful to courts in asserting the evidential value of electronic signatures. The Agency for Digital Government also provides a validation service for electronic signatures which includes components that can be used by public authorities or individuals and entities to create their own validation system of validation and proof of validation.