

Ref.: Position Paper on the Implementing Act on Requirements for qualified electronic registered delivery services - Art. 44.2

2. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

I. Introduction

The recent publication of the Implementing Act on qualified electronic registered delivery services raises significant concerns regarding its consistency and alignment with the objectives of the eIDAS Regulation. The Act appears to overlook established best practices and risks disrupting currently operational and effective systems that have been successfully supporting trust and digital communication across Europe for many years, such as the Italian use case with over 18 million users and almost 3 billion messages sent only in 2022. Rather than promoting the creation of a truly interoperable and single digital market, the Implementing Act — in its current form — may unintentionally create new barriers to the adoption of cross-border electronic delivery services. This could adversely affect European Trust Service Providers and, by extension, the broader European digital economy.

Moreover, the Implementing Act does not demonstrate sufficient coherence with the European Union's Trust Services List (TSL), which already includes numerous service providers offering qualified electronic delivery services based on the REM standard, in full compliance with the existing EU Regulation 910/2014 as amended by EU Regulation 2024/1183 (so-called "eIDAS2 Regulation"). It is essential that the regulatory framework acknowledge and build upon the experience and trustworthiness of these established providers.

It is also important to emphasize that one of the main innovations introduced by the revised eIDAS Regulation is the strengthened requirement for interoperability of electronic delivery services. In this context, it is expected that the Implementing Act would actively support this objective by relying on well-established standards — such as the REM standard — which have proven to promote true interoperability. The failure to incorporate such standards represents a significant shortcoming in the current text.

At a time when European digital sovereignty is of critical importance, legislative initiatives must foster an environment where trusted European services can thrive, building on best practices and ensuring clarity and consistency. Furthermore, it is important to avoid introducing duplicative regulatory provisions at the implementing act level (such as the level of identification of the Receiver – see detailed later) where the primary legislation, the eIDAS Regulation, already provides sufficient regulation, in order to prevent misunderstanding and confusion among stakeholders.

We ask for the implementing act to be modified as described in the “Conclusions” chapter of this document.

II. Summary and Context

The recent revision of the eIDAS Regulation (EU Regulation 2024/1183) has updated and expanded the trust services that can be provided in the EU internal market.

Among the main objectives of the revision of the eIDAS Regulation are:

- the enhancement of digital tools, which are instrumental in creating value and increasing the competitiveness of companies and the entire European Union economic system;
- the objective to create a **single European digital market** (the realisation and promotion of which is also the basis of the Treaty on the Functioning of the Union).

Also for qualified certified delivery services, the Regulation aims to promote the development of a single European Union market by **fostering interoperability among solutions provided by different trust service providers** (see recital 52 of the eIDAS 2 Regulation).

The REM (Registered Electronic Mail) standard was developed by the European Telecommunications Standards Institute (ETSI) to provide a European interoperable registered (in the sense of 'certified') electronic mail system, with legal value and complying with security and traceability requirements.

Already in 2006, ETSI recognised the need for technical specifications for registered (Qualified) electronic mail services in order to promote cross-border interoperability and facilitate the reliable exchange of e-mail in Europe. In 2008, the first version of the REM standard was published, called ETSI TS 102 640 "Registered Electronic Mail (REM)" and with the entry into force of the eIDAS Regulation (EU Regulation No. 910/2014), ETSI started a further process of harmonisation of REM standards, leading to the ETSI EN 319 5xx series, which defines the requirements for registered electronic delivery services, and of which REM represents a specific implementation based on ordinary e-mail standards and protocols.

To complete the description of the context of this Implementing Act, let us add that the new eIDAS 2 Regulation, which came into force in May 2024, through the provision of two IAs, has sought to address the issue of interoperability so as to harmonise the current situation whereby more than 50 QERDS (Qualified Electronic Registered Delivery Service) systems are active but do not communicate with each other, as they are not based on a specific standard that can guarantee interoperability between them.

That being said, also in compliance with the mandate of the eIDAS 2 Regulation, it is important to emphasise that the REM standard represents a fundamental step towards secure, reliable, legally recognised electronic communication at European level, as well as the ability to address the issue of interoperability. Its evolution has made it possible to harmonise certified e-mail services, facilitating interoperability between different national systems and ensuring compliance with the requirements of the eIDAS Regulation.

The **REM baseline, published as ETSI EN 319 532-4, is a minimum set of requirements designed precisely to maximise interoperability in cross-REM domains.** ETSI has publicly acknowledged (cf. ETSI TR 119 520-1 V1.1.1) the importance of this work, *where Italy has been at the forefront*, which has been joined, for the first time in the context of ERDS, by official interoperability testing on the standard (ETSI Plugtest) among 40 participants, 15 European countries, 4 non-European countries and 5 governmental institutions

The extension of the REM baseline concept to the entire ERDS standard is considered to be a key building block inheriting its advantages and facilitate the integration of various technologies in a transparent manner.

III. Spreading the REM services in the European market

As previously mentioned, as of today there are more than 50 different QERDS systems in Europe. These systems have limited adoption, restricted to the customers of each individual provider, and do not establish an interoperable system at the European level. As a result, they fail to create value at the system level that an interoperable system could provide.

Among these providers, there are already nine that are qualified as QREMs (see EU Trust List), offering services that are potentially interoperable with each other and guaranteeing their users a user experience as simple 'as sending an email'.

Among these, an important example is the Italian system, the Certified Electronic Mail (PEC), which today has over 18 million active users with 10 PEC providers offering their services to Public Administrations, Government Bodies, companies, professionals and citizens.

This system is a real example of how an interoperable delivery system, such as represented by REM, can create value for the system as a whole. A study conducted by IDC Research in 2023 (<https://enterprise.aruba.it/documents/whitepapers/en/benefits-and-opportunities-of-italian-certified-email-whitepaper-2024.aspx>) on the benefits of PEC highlighted that its value is not only environmental, but also contributes to the quality of life of its users, as well as offering economic advantages for the entire system. These economic benefits are estimated to be over 6 billion euros for the period between 2008 to 2026 for the Italian economy.

With specific reference to data on secondary benefits concerning economic and sustainability issues, only in 2024 the PEC usage also generated additional positive outcomes as:

- Reduction of mobility: 321 million kilometers of unnecessary travel to the postal office saved;
- Reduction of Carbon footprint: 100K tons of CO2 not emitted;
- Tree savings: 68.2K trees saved due to the reduced use of paper;
- Freeing-up archiving spaces: 1.64 million square meters of archive space saved;
- No wasting time: 2.9K Full Time Equivalent saved, thanks to the immediacy of document exchanges and the reduction of travel and waiting times at post offices.

IV. Detailed analysis of the Implementing Act

1 - ABSENCE OF REFERENCES TO STANDARDS FOR REGISTERED ELECTRONIC MAIL SERVICE

The proposed Implementing Act does not list the REM reference standards according to which certified electronic delivery services have been implemented and are provided today in Europe. The reasons why this Regulation should establish the list of reference standards for REM services are:

- a. ETSI has recognised the need for technical specifications for electronic mail services since 2008, and the revised and consolidated normative standard that resulted, the ETSI EN 319 53x series, builds on the general ETSI EN 319 52x series, to which it is complementary, and has existed since 2019 precisely to regulate qualified delivery systems based on regular mail protocols. Not referencing these standards would mean creating a technical regulatory vacuum for mail-based systems.

Area 5. Trust application service providers						
						Sub-areas
						Policy & Security Requirements
EN	3	19	5	2	1	Policy and security requirements for electronic Registered Delivery Service Providers
EN	3	19	5	3	1	Policy and security requirements for electronic Registered Electronic Mail Service Providers
						Technical Specifications
EN	3	19	5	2	2	Electronic Registered Delivery Services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Bindings

EN	3	19	5	3	2	Registered Electronic Mail (REM) Services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Interoperability profiles
						Testing conformance & interoperability
TS	1	19	5	2	4	Testing conformance and interoperability of electronic registered delivery services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of electronic registered delivery service providers
TS	1	19	5	3	4	Testing conformance and interoperability of registered electronic mail services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of providers using same format and transport protocol

Table1 - ERDS and REMS standards

- a. **REM services**, as specific types of certified electronic delivery services based on ordinary e-mail messages, **are widely used in the market** and constitute a reference model for standardisation and interoperability at European and individual Member State level. Currently, approximately 20 million users use the REM system which makes it the de facto standard used by most.
- b. With this in mind, **the European Trusted List already recognises the REM standard as a de facto standard for the qualification of certified electronic delivery services**, providing for a specific identifier (**EDS/REM/Q**) for qualified **REM services** in accordance with ETSI TS 119 612, which represents a specific type

of qualified trust service that can be provided by a trust service provider.

- c. REM services are open and interoperable by their very nature, fully satisfying the core intentions of the eIDAS Regulation and, in particular, recital 52 to the eIDAS 2 Regulation itself, both in terms of developing a single, non-fragmented digital market and fostering new business opportunities and the development of a competitive market.
- d. Also for this reason, this Implementing Act, in full compliance with the principle of technological neutrality, **should list the REM standards** (the entire ETSI EN 319 53x series) and laying the foundations for a homogeneous and recognised regulation of the procedures for sending and receiving data in the context of registered electronic mail services. In this sense, such an absence is inexplicable and would constitute a big mistake towards the subsequent definition of a concrete interoperability framework. **Furthermore, without the listing of the REM standards, this implementing act would contradict itself (recital 2) when the standards and specifications included do not reflect established practices widely recognised within the relevant sectors, and thus seriously violating the principle of technological neutrality.**
- e. The exclusion of the REM (Registered Electronic Mail) standard from the Implementing Act under Article 44 of the eIDAS Regulation raises both legal and practical concerns that merit urgent attention. REM is a well-established standard that demonstrably meets the core objectives of Article 44 — ensuring the secure, reliable, and legally admissible transmission of electronic data. Importantly, several trust service providers across the European Union have already been qualified and listed under the REM framework in the EU Trusted Lists (TSL), confirming its compliance with the essential requirements of the eIDAS Regulation. By omitting REM from the list of "presumed compliant" standards, the Implementing Act risks creating unjustified barriers to its continued use, effectively undermining legal certainty for existing qualified services and constraining the diversity and innovation in the European trust services market.
- f. To safeguard legal continuity, promote market diversity, and respect the principle of proportionality, the Implementing Act must explicitly recognize REM as a compliant standard. Furthermore, it should avoid introducing obligations that would de facto

render REM non-viable or incompatible with qualified status going forward, as described in detail in the continuation of this paper.

- g. The way paragraph 2a of Article 44 of the eIDAS 2 Regulation is worded, if the implementing act is issued with reference to the standards listed in the current version without the REM, it would be impossible to issue a future implementing act under the terms of Article 44.2b because the ‘eligible’ interoperability frameworks would have to be compliant “with the requirements laid down in paragraph 1” of Article 44 and thus would have to be also compliant with the implementing act under paragraph 2.

The Commission is in fact tasked, through a second implementing regulation pursuant to Article 44.2 of the eIDAS 2 Regulation, with establishing a list of reference standards and, if necessary, defining specifications and procedures for the interoperability framework of delivery services. The ETSI-REM standards series includes interoperability profiles defined within the **REM Baseline (ETSI EN 319 532-4)** and is considered by the same standards body (see ETSI TR 119 520-1 V1.1.1) to be a highly important reference for the development of a baseline for other non-postal qualified delivery systems as well. These may be assessed and directly referenced in future implementing regulations.

2 - SPECIFICATIONS FOR THE INITIAL IDENTITY VERIFICATION OF THE RECIPIENT

The draft regulation defines **disproportionate specifications for verifying the identity of service users**, with particular reference to the recipients of communications. What is intended to be established by the aforementioned act constitutes a **regulatory framework that is not fully relevant to the mandate of the eIDAS Regulation** and the real needs of the major part of the market; here is a detail of what is meant here:

- a. An ERDS (Art. 3, definition 36) is a service designed for the transmission of data between third parties by electronic means and provides evidence related to the handling of the transmitted data, including proof of the sending and receipt of the data, while protecting the transmitted data from the risk of loss, theft, damage, or unauthorized alterations. Although data sent and received through such a service—when qualified (Art. 43.2)—also benefit from the presumption of having been sent by the identified sender and received by the identified recipient, an ERDS is not a service

focused on the identity of users or the authorship of the transmitted data, but rather on the secure transmission of the data. For these reasons, the provision already included in Article 44.1 of the eIDAS Regulation is considered more than appropriate.

- b. Moreover, the requirements for QERDS in Art. 44.1 have not been amended by the eIDAS 2 Regulation and stipulate that qualified services shall ensure,
 - i. with a high level of confidence the identification of the sender, and
 - ii. identification of the recipient prior to transmission of the data.

The ETSI standards for ERDS services, against which more than 50 TSPs have already been qualified, provide precise provisions for EU QERDSPs and configure a security profile, generally considered appropriate for the nature and purposes of the service, that includes 'substantial' or 'high' or equivalent levels of assurance.

- a. In particular, with reference to the provision in the amended REQ-QERDS-5.2.1-01 (d) and notwithstanding recital 52 of the eIDAS 2 Regulation, the requirement of 'complete certainty' for the identification of the addressee:
 - i. is not feasible or verifiable;
 - ii. outlines a security profile that is excessive, distorted and 'out of scope' with respect to the mandate of Article 44.1 of the eIDAS Regulation.
- b. In addition, with reference to letter d) of the new requirement REQ-QERDS-5.2.1.1-01A, in order to facilitate interoperability under the eIDAS Regulation, **the case where the sender or the recipient or both are subscribed to another QERDSP is better explained in the current wording of the standard**, which should be retained. The case in which the provider of the sender and receiver are distinct entities shall be managed as well as the case in which both the sender and the recipient are subscribed by other QERDSPs. The e-delivery communication may happen indirectly, involving a number of intermediate REMSs as well, which may provide routing assistance, trust gateway, and other auxiliary functions (an intermediate ERDS could also provide such protocol conversion, thereby acting as a

gateway between a REM and a non-REM ERDS). This extended scenario is defined as '**multi-hop**' by the ETSI 319 532-1 standard and supported by the current text of the ETSI 319 521 standard.

- c. These amendments constitute a framework of technical rules that does not fully contemplate the heterogeneity of the services developed and the use cases supported. Indeed, many ERDS develop service models in which there **is no defined distinction between sender and receiver users. For instance, REM services are based on traditional mail protocols and communication flows are often bi-directional.** Nevertheless, it must be considered that the theft or compromise of a sender user's access credentials, in general even for non-postal electronic delivery services, has an impact equivalent to that of a recipient user's credentials in terms of unauthorised access to any data managed by the service. In this sense, the demand for identification practices that are generally too stringent, or when required for the addressee user only,
 - i. regardless of the type of data processed, and
 - ii. without considering any reference to the operational and risk scenarios in which these services are typically placed,

seems excessive and poses a too high entry barrier in view of market development and full interoperability between QERDSPs in the EU.

3 - SPECIFICATIONS FOR THE AUTHENTICATION OF THE RECIPIENT

The proposed regulation sets out disproportionate specifications for user authentication practices within the service, particularly concerning the recipients of communications. This is especially relevant considering that service holders are often legal entities and complex organizations. What is intended to be established by the aforementioned act constitutes an excessively strict and binding regulatory framework, which is not fully relevant to some of the key areas of application of the service. Below is a detailed account of the concerns raised in this regard:

- a. As with the points mentioned above, the requirements set out in Article 44.1 have not changed from the eIDAS 1 Regulation to the eIDAS 2 Regulation, and the relevant ETSI standards adopted by QERDS establish an appropriate framework of specifications for the authentication of service users, as defined by the Regulation itself.
- b. REM services, being developed based on traditional email messages, encompass widespread usage scenarios that rely on market-available email clients, where multi-factor authentication mechanisms are typically not supported. As already provided for by the ETSI standard, these usage scenarios—which have been one of the key factors in the success and widespread adoption of delivery services—should continue to be supported, including through authentication mechanisms that offer an equivalent level of security or are adapted to the specific risk profile.
- c. Within the diversity of services currently developed and offered under certified electronic delivery systems, a number of services have emerged in less strictly controlled environments that rely on the automatic pre-processing of messages. These services are often integrated with other systems that support document protocols and archiving—not only to further reduce the need to print, sign, and scan documents, but also to accelerate the sorting of messages. For instance, in the public sector, services that route messages from a centralized mailbox of an administration to the relevant departments are quite common. These increasingly widespread and sophisticated integration scenarios are geared toward or intended to implement artificial intelligence and robotic process automation tools aimed at maximizing user benefits, whether the users are employees of public bodies or companies, or citizens themselves.

In this context, authentication requirements that are overly strict and insufficiently flexible are seen as excessive and create a high entry barrier in terms of service continuity, development, and enhancement. As an example, the removal of the possibility to authenticate the recipient using mutual TLS authentication, or the limitation of machine-to-machine scenarios as outlined in requirement REQ-QERDS-5.2.2-03, are particularly problematic.

- a. An overly closed specification such as the one proposed here, which seems to address only certain service models, such as the 'Store & Notify' type, does not seem able to outline a regulatory framework capable of supporting two-way message delivery and interchange systems, which by their very nature are open and interoperable, and thus fail to meet the EU's intentions.
- b. In general, when the regulatory approach indiscriminately raises the security requirements for all trust services, without taking into account the differences in usage and purpose, there is a real risk that, in practice, the market and users may gravitate toward non-qualified services that are easier to access and less constrained by technical regulations. The outcome of this process is that the actual perceived level of security could decrease rather than increase.

V. CONCLUSIONS: We ask the Implementing Act to be modified according to this chapter

In light of these considerations, we respectfully call on the European Commission to amend the Implementing Act to explicitly include the REM standard among those presumed compliant under Article 44 of the eIDAS Regulation. Additionally, we urge that no technical or procedural obligation be introduced that would hinder or preclude the continued use of REM by qualified trust service providers. Such measures are essential to ensure legal certainty for existing providers, uphold the principles of technological neutrality and proportionality, and preserve the diversity and competitiveness of secure electronic delivery services across the European Union. We stand ready to engage constructively with the Commission to ensure that the Implementing Act reflects these foundational objectives and safeguards both innovation and legal continuity within the internal market. **In view of the above, it is absolutely necessary for this implementing act to refer to the full technical standards scope of the REM model that ensure full interoperability between different systems and not to add requirements that constitute too high of an entry barrier in terms of continuity of market development and interoperability between QERDSPs in the EU;** a wording for this implementing act could be as follows:

Article 1 [NEW]

Definitions

Registered electronic mail service (REMS) means a special type of electronic registered delivery service which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging.

Article 1 2

Reference standards and specifications for qualified electronic registered delivery services

~~The reference standards and specifications referred to in Article 44(2) of Regulation (EU) No 910/2014 are set out in the Annex to this Regulation.~~

Compliance with the requirements laid down in Article 44(2) of Regulation (EU) No 910/2014 shall be presumed where the qualified electronic registered delivery services, concerning the processes for sending and receiving data, comply with the standards listed in the Annex I to this Regulation.

Article 3 [NEW]

Reference standards for qualified registered electronic mail services

Compliance with the requirements laid down in Article 44(2) of Regulation (EU) No 910/2014 shall be presumed where the qualified electronic registered delivery services based on registered electronic mail service, concerning the processes for sending and receiving data, comply with the standards listed in the Annex II to this Regulation.

Article 2 4

Entry into force

~~This Regulation shall enter into force on the twentieth day~~ twenty-four months following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

ANNEX I

List of reference standards and specifications referred to in Article 1 2

The standards ~~ETSI EN 319 521 V1.1.1 (2019-02)~~, ~~(‘ETSI EN 319 521’)~~, ~~ETSI EN 319 522-1 V1.2.1 (2024-01)~~, ~~(‘ETSI EN 319 522-1’)~~, ~~ETSI EN 319 522-2 V1.2.1 (2024-01)~~, ~~(‘ETSI EN 319 522-2’)~~, ~~ETSI EN 319 522-3 V1.2.1 (2024-01)~~, ~~(‘ETSI EN 319 522-3’)~~, ~~ETSI EN 319 522-4-1 V1.2.1 (2019-01)~~, ~~(‘ETSI EN 319 522-4-1’)~~, ~~ETSI EN 319 522-4-2 V1.1.1 (2018-09)~~, ~~(‘ETSI EN 319 522-4-2’)~~ and ~~ETSI EN 319 522-4-3 V1.1.1 (2018-09)~~, ~~(‘ETSI EN 319 522-4-3’)~~ apply with the following adaptations:

- For ETSI EN 319 521:

.....

~~(14) 7.14 Supply chain~~

~~—REQ-ERDS 7.14-01: The requirements specified in ETSI EN 319 401 [1], clause 7.14 shall apply.~~

- EN 319 521 V1.1.1 - Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 522-1 V1.2.1 (2024-01) - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture
- ETSI EN 319 522-2 V1.2.1 (2024-01) - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents
- ETSI EN 319 522-3 V1.2.1 (2024-01) - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats
- ETSI EN 319 522-4-1 V1.2.1 (2019-01) - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings (standard reviewed and confirmed by ETSI, without changes, in September 2024)
- ETSI EN 319 522-4-2 V1.1.1 (2018-09) - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings (standard reviewed and confirmed by ETSI, without

changes, in September 2024)

- ETSI EN 319 522-4-3 V1.1.1 (2018-09) - Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings standard reviewed and confirmed by ETSI, without changes, in September 2024)
- TS 119 524 V 1.2.1 (2023-12) - Electronic Signatures and Infrastructures (ESI) - Testing Conformance and Interoperability of Electronic Registered Delivery Services Standards for registered -electronic mail services

ANNEX II [NEW]

List of reference standards referred to in Article 3

- EN 319 531 V1.1.1 - Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Registered Electronic Mail Service Providers
- EN 319 532 - Electronic Signatures and Infrastructures (ESI) - Registered Electronic Mail (REM) Services,
 - ETSI EN 319 532-1 V1.1.1 (2018-09) - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and Architecture
 - ETSI EN 319 532-2 V1.1.1 (2018-09) - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic Contents
 - ETSI EN 319 532-3 V1.3.1 (2024-01) - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats
 - ETSI EN 319 532-4 V1.3.1 (2024-01) - Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4:

Interoperability profiles

- TS 119 534-1 V1.2.1 (2023-12) - Testing conformance and interoperability of registered electronic mail services

In conclusion, we appreciate the opportunity to provide our detailed comments and feedback on the proposed Commission Implementing Decisions. We believe that our insights will contribute to the effective functioning of the Digital Single Market and support the continued excellence of European market.

For any further contributions or discussions, please feel free to contact us at:

European Signature Dialog (ESD) Email: office@european-signature-dialog.eu

We look forward to continued collaboration with the European Commission to ensure a secure, interoperable, and innovative trust services ecosystem.

Thank you for your attention and consideration.



Hackhofergasse 5/16
A-1190 Vienna
phone: +43 676 940 9309
office@european-signature-dialog.eu