ETSI TR 119 520-2 V1.1.1 (2024-04)

Electronic Signatures and Trust Infrastructures (ESI);
Framework of ERDS/REM standards;
Part 2: Impact of emerging technologies on ERDS/REM Models

Reference
DTR/ESI-0019520-2

Keywords
e-delivery services, registered e-delivery services,
security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.13].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

An Electronic Registered Delivery Service (ERDS) is specified in ETSI EN 319 521 [i.4] and defined as a service that makes it possible to transmit data between parties by electronic means, by adding the provision of 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 unauthorized alterations. ERDS evidence is data generated within the ERDS service provision, which aims to prove that a certain event has occurred at a certain time, and are defined in clause 8 of ETSI EN 319 522-2 [i.6].

Registered Electronic Mail (REM), is a specific type of electronic registered delivery, which builds on the formats, protocols and mechanisms used in ordinary electronic mail messaging (see ETSI EN 319 531 [i.7] and ETSI EN 319 532 [i.8]).

The legal effect of an ERDS depends on the specific legal framework, for example as provided in the European Union by Regulation (EU) No 910/2014 [i.1] (eIDAS Regulation) and is not in scope of ETSI standards.

New technologies and models are emerging that can be used in the context of ERDS/REM but not considered by the current set of ETSI standards: when implemented independently by different providers as part of ERDS without common standards they have no chance to interoperate.

The approach followed in the present document, is to:

- Monitor emerging ERDS/REM technologies and models that have been identified. The result of this activity is reported in clause 4.
- Perform an assessment on the result of monitoring and identify concrete proposals on ERDS/REM services provision and models. The result of this activity is reported in clause 5 and the impact on the ERDS framework is reflected in ETSI TR 119 520-1 [i.13].

Guiding principles are ensuring interoperability across diverse ERDS/REM and focus on promoting a seamless adoption of ERDS within existing electronic delivery communities.

1 Scope

The present document aims to study the impact of emerging technologies and models for ERDS/REM provision and assess their impact on the ERDS framework of standards.

The approach followed is to:

- Monitor emerging ERDS/REM technologies and models that have been identified. The result of this activity is reported in clause 4.
- Assess the result of monitoring and identify concrete proposals on ERDS/REM services provision and models. The result of this activity is reported in clause 5 and the impact on the ERDS framework is reflected in ETSI TR 119 520-1 [i.13].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or nonspecific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

[i.3] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act).

[i.4] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.5] Commission Implementing Regulation (EU) 2022/1463 of 5 August 2022 setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council.

[i.6] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents".

[i.7] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.8] ETSI EN 319 532 (all parts): "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services.

[i.9] ETSI GR PDL 014: "Permissioned Distributed Ledger (PDL); Study on non-repudiation techniques".

[i.10] ETSI GR PDL 017: "Permissioned Distributed Ledger (PDL); Application of PDL to Amended Regulation 910/2014 (eIDAS 2) Qualified Trust Services".

NOTE: ETSI GR PDL 017 is being drafted at the time of writing the present document as Work Item "DGR/PDL-0017_eIDAS App".

[i.11] ISO 19626 (all parts): "Processes, data elements and documents in commerce, industry and administration - Trusted communication platforms for electronic documents".

[i.12] CEN/TS 16326:2013: "Postal Services - Hybrid Mail - Functional Specification for postal registered electronic mail".

[i.13] ETSI TR 119 520-1: "Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 1: New (Q)ERDS/(Q)ERDSP standardization rationalized framework as a result of the new components brought by eIDAS2.0".

[i.14] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.15] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

[i.16] Draft Commission Implementing Regulation (EU) laying down common procedures and detailed rules for accessing and processing electronic freight transport information by competent authorities in accordance with Regulation (EU) 2020/1056 of the European Parliament and of the Council.

[i.17] ISO 15000-2: "Electronic business eXtensible Markup Language (ebXML) - Part 2: Applicability Statement (AS) profile of ebXML messaging service".

[i.18] Regulation (EU) No 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.

[i.19] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[i.20] ISO 15000-1: "Electronic business eXtensible Markup Language (ebXML) - Part 1: Messaging service core specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.14], ETSI EN 319 521 [i.4], in ETSI TR 119 520-1 [i.13] and the following apply:

DEP eDelivery: set of technical specifications and standards for electronic message exchange developed by the Commission under the Connecting Europe Facility (CEF) programme and continued under the Digital Europe programme (DEP)

eIDAS 2.0: EU Regulation amending Regulation (EU) No 910/2014 [i.2] as regards establishing a framework for a European Digital Identity

NIS2: Directive (EU) 2022/2555 [i.15] on measures for a high common level of cybersecurity across the Union

Registered Electronic Mail (REM): specific type of electronic registered delivery, which builds on the formats, protocols and mechanisms used in ordinary electronic mail messaging

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 520-1 [i.13] and the following apply:

AS4 Applicability Statement 4

NOTE: It is specified in ISO 15000-2 [i.18].

CEF Connecting Europe Facility programme

NOTE: See https://digital-strategy.ec.europa.eu/en/activities/cef-digital.

DEP Digital Europe Programme

NOTE: See https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

DLT Distributed Ledger Technology
EBSI European Blockchain Services Infrastructure
EIF European Interoperable Framework
ERDS Electronic Registered Delivery Service
OOTS Once-Only Technical System
QERDS Qualified Electronic Registered Delivery Service
TTP Trusted Third Party
TCE Trusted Communication Evidence

4 Gathering information on emerging technologies and new models

4.1 Information sources

The assessment provided in clause 5 is based on the monitoring of emerging technologies and models related to Electronic Registered Delivery Services (ERDS) and Registered Electronic Mail (REM) that are not yet included in the existing ERDS/REM standards framework. This monitoring process included an examination of:

- Standardization activities relevant for ERDS such as the standardization activities by the ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL), ISO Technical Committee on Processes, data elements and documents in commerce, industry and administration (ISO/TC 154) and CEN Technical Committee on Postal services (CEN/TC 331).
- European initiatives requiring electronic delivery or making available electronic related services, components or technologies such as laws and regulations, the eDelivery building block from the Digital Europe Program (DEP eDelivery), Peppol and the European Blockchain Services Initiative (EBSI).

4.2 Monitoring of standardization activities

4.2.1 ETSI ISG Permissioned Distributed Ledger (PDL)

ETSI ISG PDL issued a set of specifications and reports that are potentially relevant for ERDS/REM standards in support of ERDS requirements.

ETSI GR PDL 014 [i.9] is a report that elaborates on a number of properties of PDL that can support different types of non-repudiation of transactions, notably: Non-Repudiation of Origin, Non-Repudiation of Emission, Non-Repudiation of Receipt, Non-Repudiation of Submission, Non-Repudiation of Delivery, Non-Repudiation of Transport. PDL does not support directly electronic delivery but can add a level of trust or notarization to electronic delivery or information sharing.

ETSI GR PDL 017 [i.10] is a report focused on possible application of PDL as a qualified electronic ledger and in support for eIDAS 2.0, trust services.

4.2.2 ISO 19626 Trusted communication platforms for electronic documents

ISO 19626-3 [i.11] provides guidelines for developing Trusted Communication Platform for electronic documents (TCP hereinafter) using Distributed Ledger Technology (DLT hereinafter). Its scope is "to present a blockchain-based TCP system architecture (…), and to define details necessary for implementation for components that require blockchain technology application".

ISO 19626-1 [i.11] defines the TCP system architecture as formed by 4 components, namely:

- TTP identity directory. This component "provides registration functions to identify and confirm the trustworthiness of the identity information of communication participants (communication servers and communication clients). It registers and manages their electronic identity information".
- TCP communication server. This component "receives requests from communication clients and transfers electronic documents between originator and addressee(s) in a reliable way".
- TCP communication client. This component "is a client application for a communication entity to request services provided by a communication server".
- TCE repository. This component verifies and archives the TCE delivered by the TCP communication server.

ISO 19626-3 [i.11] analyses the feasibility and suitability of using DLT for the aforementioned 4 components, arriving to the following conclusions:

- Supporting TTP identity directory with DLT is feasible, taking into account that:
  - "the distributed ledger can secure the trustworthiness of registered identity information and share it with the blockchain network through synchronization";
  - whenever there exists sensitive information "it is appropriate to put the sensitive information in a block and/or not share it in the blockchain network";
  - it is expected that this component has "more search requests than registration requests", which needs "to consider the availability of H/W, S/W, network construction, etc.".
- Supporting TCP communication server with DLT is NOT feasible (although it "would work as TCP DLT oracle (…) in processes functionally connected to TTP identity directory DLT nodes and the TCE repository DLT nodes"), taking into account that:
  - the size of transmitted and received documents, which may vary "from several KB to hundreds of MB or tens of GB", while the block size is usually of "1 to 4 MB";
  - the electronic documents are recorded in the DLT, which means that they are "exposed". This implies that "the application of blockchain technology violates the TCP confidentiality requirements".
- Supporting TCP communication client with DLT is, obviously, NOT feasible.
- Supporting TCE repository with DLT is feasible, taking into account that:
  - once the evidence has been created and stored, "it needs to remain immutable until its disposal";
  - the blockchain consensus mechanism eliminates the appearance of potential inconsistencies and subsequent communication disputes;

- DLT reinforces the non-repudiability of TCE.

Moreover, ISO 19626-3 [i.11] specifies that the TCP DLT system "is implemented by applying the private permissioned DLT system", and "that all operations are limited to TCP users and where permissions are required to perform any operation on the system, even reading the transaction records". It also enumerates the major function of DLT nodes, distinguishing those ones provided by:

- Smart contracts. They are in charge of "operating the transaction data flowed in from the DLT interface as an automated processing code". They check "the order or sate of TCP transaction data (…), agree the consensus of the validity of TCP transaction data, and finally create the block data".
- Blockchain functions. The blockchain platform provides "basic functions (…) such as security, transaction processing, and synchronization".
- Distributed ledger. It "registers and manages block data in cryptographically secured data structure".

Finally, ISO 19626-3 [i.11] provides details on the implementations of both the TTP identity directory DLT system, and the TCE repository DLT system.

4.2.3 CEN/TS 16326 Functional Specification for postal registered electronic mail

CEN/TS 16326:2013 [i.12] has been developed by CEN, within TC 331, and is based on ETSI TS 102 640-1 [i.19] that is superseded by ETSI EN 319 532 [i.8] and references ETSI signature formats linked to the legislation in force before the eIDAS Regulation.

ETSI TC ESI is offering support to CEN/TC 331 to align CEN/TS 16326:2013 [i.12] to current ERDS/REM standards and possibly better support hybrid mail in the context of the future ERDS/REM standards framework as result of collaboration activities.

4.3 Monitoring of European initiatives

4.3.1 Policy initiatives relevant for electronic delivery

4.3.1.1 Single Digital Gateway, the once-only technical system

The Commission Implementing Regulation (EU) 2022/1463 [i.5], in the context of the Single Digital Gateway (Regulation (EU) 2018/1724 [i.19]) mandated the establishment of the Once-Only Technical System (OOTS). Within the framework of the OOTS there are two requirements: compliance to electronic registered delivery services and the utilization of DEP eDelivery. Specifically, it is required that eDelivery Access Points form a network of nodes for secure digital data exchange. eDelivery Access Points are defined as communication components that are part of the eDelivery service based on technical specifications and standards, including the AS4 messaging protocol and ancillary services developed under the Connecting Europe Facility Programme and continued as DEP eDelivery, to the extent that these technical specifications and standards overlap with the ISO 15000-2 [i.17] standard.

4.3.1.2 The EIF and the Interoperable Europe Act

The European Interoperable Framework (EIF) was developed in the European Union under the former ISA2 programme to guide European public administrations in achieving interoperability - the ability of diverse systems and organizations to work together. The EIF is an essential part of Regulation (EU) 2024/903 [i.3] laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act).

The EIF is designed to enhance and facilitate digital public services across EU member states, ensuring that these services are interoperable, user-centric, and efficient.

Key Elements of the EIF is its layered approach to interoperability:

- Legal Interoperability: aligning laws and regulations across EU member states to enable seamless digital interactions.

- Organizational Interoperability: ensuring that administrative processes and structures across different entities are compatible and can work together effectively.
- Semantic Interoperability: establishing a common understanding and exchange of data and information.
- Technical Interoperability: enabling systems and technologies to connect and communicate across different IT infrastructures.

The EIF is built on principles like openness, transparency, reusability, technological neutrality, data protection, and user-centricity, ensuring that digital services are accessible, secure, and efficient. It establishes governance mechanisms to manage and guide interoperability efforts, ensuring continuous improvement and adaptation to evolving technologies and needs.

In the context of ERDS, the EIF is relevant and beneficial as a guide for the development and implementation of ERDS, ensuring to model and consider cross-border functionality, standardization and compatibility, legal and organizational alignment, User-Centric Approach and to consider innovation.

In particular technical and semantic interoperability aligns well with the ERDS approach that separates evidence semantic and data formats.

4.3.1.3 The eFTI draft implementing act

The Commission has made available the draft Commission Implementing Regulation setting implementation specifications for Regulation (EU) 2020/1056 [i.16] on electronic Freight Transport Information (eFTI).

This act, if the draft is confirmed, requires the establishment of a cross border network to support accessing and processing of electronic freight transport information by competent authorities.

According to the draft, use of the DEP eDelivery is mandated.

4.3.2 The European projects

4.3.2.1 The Digital Europe Programme

The Digital Europe Programme (DEP) is a EU funding program focused on bringing digital technology to businesses, citizens and public administrations. Among the different initiatives, DET is maintaining the former CEF eDelivery, now one of the Digital Europe building blocks (referred to DEP eDelivery in the present document).

It is based on OASIS ebMS3 and AS4, now adopted by ISO as ISO 15000-1 [i.20] and ISO 15000-2 [i.18].

In this context two initiatives have been identified (currently not part of the "official" DEP eDelivery):

- A REST API Profile complies with the REST API architectural style aiming to support specifically use cases where one party to the data exchange operates in a light context, while the DEP eDelivery AS4 profile implements a solution optimized for general server-to-server communication. An open source pilot implementation of this profile is available.
- A pilot was carried out on a potential approach for connecting DEP eDelivery with the EBSI infrastructure. Two use cases were piloted successfully:
    1) a white list for making it easier to add nodes in an eDelivery network without the need to share the certificates with the other participants;
    2) notarizing the timestamp of eDelivery messages on the blockchain.

4.3.2.2 Peppol

Peppol was a funded European project, now governed by an international association, aiming to enable businesses to communicate electronically with any European public sector entities in the context of procurement process. It established a network, based on AS4. Originally limited to Europe it is now gaining acceptance in many countries outside EU.

4.4 ERDS/REM Emerging technologies

4.4.1 Blockchain & DLT

The use of DLT in the ERDS context is a relatively new and innovative approach. DLT provides a secure and decentralized method for storing and verifying information, which can be used to enhance the security and reliability of ERDS supporting evidence relating to the handling of the transmitted data, proof of sending and receiving the data, protection of transmitted data against the risk of loss, theft, damage or any unauthorized alterations.

DLT allows multiple parties to maintain and verify a shared ledger maintained in a decentralized manner, which means that it is not controlled by any single party or organization. Instead, it is maintained by a network of nodes that work together to verify and validate the content of the ledger.

The approach used to support integrity and non-repudiation of electronic delivery, as required by eIDAS 2.0 using DLT requires however further standardization activities to ensure the general goal of ensuring basic interoperability between the different DLT and ERDS implementations. moreover, compliance with privacy rules, in particular with the right to be forgotten, can represent a challenge.

4.4.2 REST

Representational State Transfer APIs (RESTful APIs) are a type of web service that follows the REST architectural style, which is a set of principles for designing network-based software systems. RESTful APIs allow two software systems to communicate over the internet by sending and receiving data in a standardized format.

RESTful APIs are based on a client-server architecture, where the client sends a request to the server to perform a certain action, and the server responds with the requested data. The request and response are typically sent using the HTTP protocol, and the data is usually formatted as JSON or XML.

One of the key features of RESTful APIs is that they use a set of standard HTTP methods to perform actions on resources. These methods include Get, Post, Put, Patch and Delete, which are used to retrieve, create, update, and delete resources.

Another important feature of RESTful APIs is that they are stateless, meaning that each request contains all the information necessary for the server to understand and process the request. This allows RESTful APIs to scale easily, as they do not need to store any session or client-specific data.

RESTful APIs are based on the concept of resources, which are entities that can be accessed and manipulated through the API. Each resource is identified by a unique identifier, known as a URI (Uniform Resource Identifier). The URI is used to specify the location of the resource on the server, and the client can use the URI to access and manipulate the resource.

When a client sends a request to a RESTful API, the API processes the request based on the HTTP method used in the request. For example, if the client sends a GET request, the API will retrieve the requested resource and send it back to the client in the response.

RESTful APIs are designed to be language-agnostic and platform-independent, meaning that they can be used with any programming language or platform that supports HTTP. This makes it easy to integrate different software systems, even if they are built using different technologies.

One of the advantages of using RESTful APIs is that they are highly scalable, as they can handle large volumes of requests and can be easily expanded to support additional resources or functionality. Additionally, they are generally considered to be more lightweight and efficient than other types of web services, as they do not require the use of additional protocols or middleware.

Use of RESTful APIs in the context of ERDS can bring benefits to ensure lightweight access AS4 notes or for some ERDS components such as a repository of ERDS evidences.

5 Assessment of emerging technologies and models for ERDS/REM provision

The different models monitored and reported in clause 4.3 have some commonalities:

- focus on European and international interoperability;
- when a specific electronic delivery technology is recommended or mandated, the choice is on AS4 and especially DEP eDelivery.

Moreover, the monitoring did not cover eIDAS 2.0 itself and NIS2 as they are extensively covered in part 1 [i.13] but it is worth to be noted that:

- interoperability is directly addressed by the Baseline concept where different underlying transport are considered in case of the REM and HTTP baseline, but sharing a common and robust model to ensure interoperability;
- standardized support for eIDAS 2.0 trust service framework, especially for the qualified level, and NIS2 requirements is a serious technical goal that cannot be fully achieved by DEP eDelivery alone;
- a modular component based approach has been adopted in the framework with a number of benefits; here it is highlighted that this approach is crucial to reduce the cost of the introduction of new technologies as their impact can in general be confined and does not impact all the components, while a "monolithic" ERDS tends to be less flexible.

An important aspect to consider is the end-user viewpoint of an electronic delivery network. Base DEP eDelivery was already extensively deployed and full compliance with the current framework of ETSI standards requires investments also on end-user applications to adapt them to manage ERDS evidences.

An interesting option to consider is to permit a "detached" mode for ERDS evidence management. In this case the complexity is confined mostly on the ERDS provider side while end users not requiring to manage evidences on every message can just retrieve them when needed from the service provider. It is then envisaged to standardize an Evidence component that can deal with most of the aspects related to evolve a generic electronic delivery or a DEP eDelivery service to an ERDS or QERDS.

It is also important to consider that with the implementation in all Europe of the NIS2 Directive [i.15], Member States are required in article 24(1) to encourage the use of qualified trust services, including QERDS, therefore a robust path to evolve a base electronic delivery or a DEP eDelivery service to a (Q)ERDS is an important element to comply also with NIS2.

A final consideration is about defining checklists, as part of the standardization effort, to better support the component based approach as it supports the audit of each component and, on the other hand, is an important tool for the QERDS provider to assess eventual compliance gaps and address them.

History

Document history		
V1.1.1	April 2024	Publication