Qualified Electronic Registered Delivery Service (QERDS)

GoNotice

QERDS PRACTICE STATEMENT

DOCUMENT CODE	ICERT-QERDS-MO
VERSION	1.3
DATE	16/05/2025

tinexta infocert

Table of contents

tinexta infocert

tinexta infocert

1 INTRODUCTION

1.1 Change history

Change	Details
Version/Release n°:	1.3
Version/Release date:	16/05/2025
Description:	Updated company logo Updated Operational Headquarters Updated version of ISO 27001 e 9001 Updated telephone number of InfoCert Updated paragraph 7.1 General revision of stylesheets and formats of the document § 9.1 Clarifications on company insurance coverage § 3.5.1 Clarifications on API credentials release
Reason:	General revisions of the document, accessibility, updates and fixes

Change	Details
Version/Release n°:	1.2
Version/Release date:	10/11/2024
Description:	Updates to paragraphs 3.3.2, 3.5.1, 3.5.2
Reason:	Clarifications

Change	Details
Version/Release n°:	1.1
Version/Release date:	18/10/2024
Description:	• Bug fixes • Document formatting review • Improved structure for document accessibility • Review of definitions and acronyms • Review of regulatory, procedural and technical references • Legal headquarters update • Update of the subjects responsible for approving the Practice Statement • Review and approval of the nomenclature of service roles and specification of their characteristics • Simplifying the description of processes
Reason:	General revision of the document

Change	Details
Version/Release n°:	1.0
Version/Release date:	05/06/2024

Change	Details
Description:	First issue of the document
Reason:	-

1.2 General framework

The present document is the *Practice Statement* of the *Qualified Trust Service Provider* **InfoCert** (**QERDSP**) which describes the "*Qualified Electronic Registered Delivery Service*" (**QERDS**) called **GoNotice**.

GoNotice service is implemented in compliance with **EU Regulation No. 910/2014 eIDAS [1]**.

This document contains the policies and practices followed in the process of identification and provision of GoNotice service, the security measures adopted, the obligations, guarantees and responsibilities, in compliance with the current legal framework on *qualified trust services*.

By publishing this Practice Statement and inserting references to this document in the contracts and in specific links of the user interfaces, users are allowed to evaluate the characteristics and reliability of GoNotice service offered by InfoCert, and therefore the methods of access to the service as well as the link and relationships that exist between the service itself and the *Customer*.

The present Practice Statement also contains the **policies** and **practices** pursued by InfoCert in the control process of the requests, identification of the *Registration responsible* based on the *Contract* (see paragraph §1.3.4) and in the **provision of the service** as per the art. 3, def. 37) and art. 44 of EU Regulation No. 910/2014 eIDAS [1], based on the Consolidated Text of the Digital Administration Code (**Testo Unico del Codice dell'Amministrazione Digitale CAD**) [2]) and the **provisions of AGID** on the procedures for submitting applications for registration in the *Trusted List* as an ERDSP (Electronic Registered Delivery Service Provider), and **in accordance with** the requirements and **security policy** defined in the ETSI EN 319 521 [6] standard.

The **qualified electronic registered delivery service**, specified in the present Practice Statement, is characterized by a series of peculiarities which are fully identified and connected, in the following paragraphs, to the standards and regulations (or specific parts of them) which represent the supporting basis.

The highest-level essential aspects are described below and are then further detailed in the specific sections that follow.

The main feature that distinguishes the **GoNotice** service is that it is defined **in accordance with** the **policies and security requirements** represented by ETSI EN 319 521 [6] standard. In other words, from the most general point of view possible, it represents a service that this standard defines as **Electronic Registered Delivery Service (ERDS)**.

A **GoNotice** flow, from a general point of view and in the absence of ambiguity, can be identified by the so-called "**Store and Notify**" (**S&N** from here on) *style of operation*: the sender's message is submitted to the service to be sent, the service stores it (**store**) in areas dedicated to the sending customer and sends a notification to the recipient (**notify**) with everything necessary for the recipient to access the sender's message.

1.3 Document identification

1.3.1 Name and document identifier

This document is called "InfoCert - Qualified Electronic Registered Delivery Service Provider – **GoNotice** Practice Statement" (*QERDS Practice Statement*) and is characterized by the document code: **ICERT- QERDS-MO**. The version and release level are identifiable in the header of each page.

The *Object Identifiers* (OID) (see definition in paragraph §1.3.4) and the *Uniform Resource Identifiers* (URI), described below, are associated with the document.

InfoCert is identified by **1.3.76.36** *object identifier* (OID).

The root *Uniform Resource Identifier* (URI) identifying the significant objects within the ETSI standards, is **http://uri.etsi.org** (or https://uri.etsi.org).

Significant identifiers for *qualified electronic registered delivery service* and for its related *Practice Statement* are:

Description	OID
qualified-electronic-registered-delivery-service	1.3.76.36.1.1.2000
qualified-electronic-registered-delivery-service-practice-statement	1.3.76.36.1.1.2000.1

Table 1 – Identifiers

1.3.2 Scope and applicability of the document

The purpose of this document is to describe the rules and operating procedures adopted by InfoCert in the management of the **qualified electronic registered delivery service** in accordance with current rules and standards, as outlined in paragraph §1.2.

The present Practice Statement represents also a detailed integration to the information provided to the *Customer* according to the Article 13 of Legislative Decree 196/03 and Article 13 of Regulation (EU) 679/2016 [3].

1.3.3 References

1.3.3.1 Regulatory and technical references

[1] **EU Regulation 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 as amended by Regulation (EU) No 2024/1183 of the European Parliament and of the Council of 11 April 2024 (referred to as EIDAS)

[2] **Legislative Decree 7 March 2005, n.82** (Official Journal no. 112 of 16 May 2005 – S.O. no. 93) – Digital Administration Code (also referred to as CAD) and subsequent amendments.

[3] **Legislative Decree 30 June 2003, n. 196** (Official Journal no. 174 of 29 July 2003) – Privacy Code and subsequent amendments and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data (effective from 25 May 2018).

[4] **Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011**, on consumer rights and related national implementing legislation.

[5] **ETSI EN 319 401** "Electronic Signatures and Infrastructures (ESI): General Policy Requirements for Trust Service Providers".

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

[7] **ETSI EN 319 522** "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services" (specifically the version V1.1.1 of **ETSI EN 319 522-1, 2, 3 parts**).

[8] **Decree of the President of the Council of Ministers 22 February 2013** (Official Journal General Series no.117 of 21-05-2013) – "Technical rules regarding the generation, application and verification of advanced, qualified and digital electronic signatures, according to Articles 20, paragraph 3, 24, paragraph 4, 28, paragraph 3, 32, paragraph 3, letter b), 35, paragraph 2, 36, paragraph 2, and 71".

[9] **ETSI EN 319 403** "Requirements for conformity assessment bodies assessing Trust Service

Providers".

[10] **IETF RFC 6749** "The OAuth 2.0 Authorization Framework"

[11] **IETF RFC 6750** "The OAuth 2.0 Authorization Framework: Bearer Token Usage"

1.3.3.2 Procedural standards

All the operational processes of InfoCert QERDSP described in this *Practice Statement*, like any other activity of InfoCert QERDSP, are carried out in compliance with the Company Quality and Security Plan, in accordance with the standards **UNI EN ISO 9001:2015** and **UNI CEI EN ISO/IEC 27001:2022**.

1.3.3.3 Safety standards

To ensure the security of the *qualified electronic registered delivery service*, InfoCert uses techniques and procedures based on international standards (de jure or de facto) and on specific regulations existing in Italy.

The procedures were drafted and developed based on the following standards:

- **Information Technology Security Evaluation Criteria (ITSEC) v. 1.2**
- **Common Criteria for Information Technology Security Evaluation v 2.2**
- **ISO/IEC 17799** - Information technology -- Security techniques -- Code of practice for information security management
- **UNI CEI EN ISO/IEC 27001:2013** - Information security, cybersecurity and privacy protection - Information security management systems – Requirements UNI CEI ISO/IEC 27001:06 – Information technology – Security techniques – Information security management systems – Requirements.
- **ISO-IEC 27002:05** – Information Technology – Security Techniques – Code of practice for Information Security Management
- **UNI CEI EN ISO/IEC 27017** - Information Technology - Security Techniques - Collection of practices on information security controls for cloud services based on ISO/IEC 27002
- **UNI CEI EN ISO/IEC 27018** - Information Technology - Security Techniques - Collection of practices for the protection of personal data processed in public clouds by data controllers
- **UNI CEI ISO/IEC 29115** - Information Technology - Security Techniques - Framework for Ensuring Entity Authentication

The cryptographic modules (**HSM**) used by InfoCert for the management of the digital keys for the digital signature of contents and evidence (ERDS evidence) are validated and certified according to FIPS 140-2 level 3 and Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL).

1.3.4 Definitions

The definitions used in the present document are listed below. For the terms defined in the above referenced standards, please refer to the definitions therein contained.

Term	Definition
Customer	Natural or legal person who purchases/requests the *qualified electronic registered delivery service* and assumes the right to suspend or revoke it**.**
Owner	Natural or legal person requesting the service, who must be identified as the *Owner* of the *qualified electronic registered delivery service*. The *Owner* is the formal *Sender* of all messages made in the use of the service. In some cases, the *Owner* coincides exactly with the *Customer*.
Registration responsible	Natural person who will be effectively identified as the *Owner* (natural person) or legal representative of the *Owner* or person with legal power of attorney of the *Owner.*
Agent	With the term *Authorized Agent* (or simply *Agent*) means the commercial partner (or intermediary entity or distributor) of InfoCert who carries out activities to support the direct sales network of the GoNotice service through a specific resale contract.
User (Abstract term)	Person or application authorized to access the GoNotice service by authentication.
Admin-User	User who accesses the GoNotice service through the credentials of the *qualified electronic registered delivery service* who deals with registering new users.
Sender-User	User who accesses the GoNotice service through the credentials of the *qualified electronic registered delivery service* who deals with sending *messages* certified by GoNotice service.
Sender (Abstract term)	The *Owner* who sends the *message* to the recipient.
Recipient / Receiver	Natural person who receives the *message* from the sender upon identification.
Identity Provider (IdP)	Provider of the digital identity.
Servizio elettronico di recapito certificato (SERC)	«... un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi

Term	Definition
	dal rischio di perdita, furto, danni o di modifiche non autorizzate;» (as defined in Article 3, def. 36) eIDAS [1]).
Electronic registered delivery service (ERDS)	«... 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;» (as defined in Article 3, def. 36) eIDAS [1]).
Servizio elettronico di recapito certificato qualificato (SERCQ)/ Qualified Electronic Registered Delivery Service (QERDS)	Electronic registered delivery service that meets the following requirements: «(a) they are provided by one or more qualified trust service provider(s); (b) they ensure with a high level of confidence the identification of the sender; (c) they ensure the identification of the addressee before the delivery of the data; (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamps.» (as defined in Article 3, def 37) and Article 44 eIDAS [1]). Unless otherwise specified in this document, "**service**" means *qualified electronic registered delivery service*.
GoNotice service	The *qualified electronic registered delivery service* provided by InfoCert.
Time-stamping authority	*Qualified trust service provider*, acting as a trusted third party, providing the time stamp service {Time-stamping authority}.
Conformity Assessment Body (CAB)	Body which is accredited in accordance with eIDAS Regulation as competent to carry out *conformity assessment* of a *qualified trust service provider* and the qualified trust services it provides. It drives up the CAR (as defined in Article 3, def. 18) eIDAS [1]).
Conformity Assessment Report (CAR)	Report by which the *conformity assessment body* confirms that the *qualified trust service provider* and the trust services themselves comply with the requirements of the Regulation (as defined in Article 21 and 51 eIDAS [1]).
Open ID Connect & OAuth2.0	Interoperable authentication protocol based on the OAuth 2.0 specification framework (IETF RFC 6749 [10] e 6750 [11]). It simplifies the way to verify the identity of users based on authentication performed by an authorization server and allows to obtain user profile information in an interoperable and REST-like way.
Level of Assurance (LoA)	Progressively increasing level of security or assurance of electronic

Term	Definition
	identification schemes based on the provided service. Three levels of assurance are identified (as defined in Article 8 def 2) eIDAS [1]) based on what is defined by ISO/IEC 29115 standard: • level 1- Low (corresponding to LoA2 of ISO-IEC 29115): • level 2 – Medium/Substantial (corresponding al LoA3 of 'ISO-IEC 29115); • level 3 – High (corresponding al LoA4 of 'ISO-IEC 29115). For details refer to ISO standard. The minimum level of assurance allowed for sender authentication and identity verification is level 2.
Contract	The contract for the activation of the GoNotice *qualified electronic registered delivery service* is composed by the Activation Request, the General Contract Conditions, the present Practice Statement and the documents therein referred which together constitute the discipline of the relationships between the parties.
User credentials	Set of data and factors specific to a *User* used to access the *qualified electronic registered delivery service* through a two-factor authentication system.
Person identification data	A set of data that allows to establish the identity of a natural or legal person, or of a natural person representing a legal person (as defined in Article 3 def 1) eIDAS [1]).
Electronic identification	The process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person (as defined in Article 3 def 1) eIDAS [1]).
Time stamp	The time reference data which binds other data in electronic form establishing evidence that the latter data existed at that time (as defined in Article 1 def h) DPCM 22 February 2013)[8].
Electronic identification means	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service (as defined in Article 3 def 2) eIDAS [1]).
One Time Password (OTP)	Password valid only for a single transaction. In the context of the *qualified electronic registered delivery service*, it can be used in the *Two-Factor authentication scheme* to validate the *User Credentials.*
Qualified trust service provider	A *trust service provider* who provides one or more qualified trust services and is granted the qualified status by the supervisory body (as defined in Article 3 def 20) eIDAS [1]).
Request of activation	The request of the *Owner* requesting the activation of the GoNotice *qualified electronic registered delivery service*.
Message	A GoNotice *message* is composed of the data produced by the *Sender* (together to other possible service data) and that are made available to the *Recipient* (see the *user content* and *original message* concepts in the ETSI reference standards)

Term	Definition
Message campaign	GoNotice process that allows a *message* to be sent to one or more recipients in a secure and traceable way using a set of evidence tracks in compliance with the relevant ETSI standards.
Audit Trail	A digitally signed PDF report with a high-level overview and a detailed summary of the events resulting from the *message campaign* and the related delivery outcomes. All XML ERDS evidence files, generated for each significant event of the process, and in accordance with ETSI standards, are also attached.

Table 2 - Definitions

1.3.5 Acronyms and abbreviations

Acronym	Definition
AgID	Agenzia per l'Italia Digitale/ Agency for Digital Italy: Supervisory Authority for Trust Service Providers
CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Codice dell'Amministrazione Digitale / Digital Administration Code (See DL 7 March 2005 [2])
CAR	Conformity Assessment Report
CIE	Carta di Identità Elettronica / Electronic Identity Card
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation (See [1])
ETSI	European Telecommunications Standards Institute
HTTPS	HyperText Transfer Protocol Secure
IP (or IP address)	Numeric address that identifies network entities connected to the network.
ISO	International Organization for Standardization: founded in 1947, ISO is an organization composed of representatives from the national standard organizations
OID	Object Identifier: consists of a sequence of numbers, registered according to the procedure defined in ISO/IEC 6523 standard, which identifies a specific object within the OID tree hierarchy
SPID	Sistema Pubblico di Identità Digitale / Public Digital Identity System
S&N	Store and Notify
S-ERDS	Sender's ERDS
R-ERDS	Recipient's ERDS
UA	ERD User Agent (or **UA/Application**) - system consisting of software and/or hardware components by which senders and recipients participate in the exchange of data with the ERDS

Table 3 – Acronyms and abbreviations

For abbreviations and concepts used in the present document but not reported above, refer to the definitions in the relevant regulatory and technical standards, and in particular to the Clause 3 of each ETSI standard (see paragraph §1.3.3.1).

1.4 Practice Statement

The present Practice Statement, compiled by QERDSP InfoCert in accordance with the general provisions of the reference standards (ETSI EN 319 521 [6]), is provided to the designated supervisory body - which in Italy is AGID - and is part of the qualification documentation of a *qualified electronic registered delivery service* provider.

1.4.1 Notification mechanism and publication period

The Practice Statement is published:

- In electronic format on the QERDSP InfoCert website (indirizzo: http://www.infocert.it/documentation);
- in electronic format in the public list of *qualified trust service providers* (QTSP) supervised by AgID
- As paper document by a request to the *Authorized agent* or to the *contact* for the end users.

1.4.2 Subjects responsible for approving the Practice Statement

This Practice Statement is verified by the Security and Policy Manager, the Privacy Manager, the Certification Service Manager, the Legal Manager, the Regulatory Manager and approved by the Company Management.

1.4.3 Approval Procedures

The drafting and approval of this document subject to the procedures set out in the Company's Quality Management System ISO 9001:2015.

No more than once a year, the *Trust Service Provider* InfoCert shall perform a compliance check of this Practice Statement to its service delivery process.

1.4.4 Review of the Practice Statement

InfoCert reserves the right to make changes to this document for technical reasons or for changes to procedures resulting from laws or regulations, or for optimization of the work cycle.

Each new version of the Practice Statement cancels and replaces previous versions.

Changes that do not have a significant impact on users will result in an increase in the document release number, while changes that have a significant impact on users (such as significant changes to operating procedures) will result in an increase in the document version number. In any case, the manual will be promptly published and made available.

With a frequency not exceeding one year, QERDSP InfoCert performs a compliance check of this Practice Statement to its process for providing the *qualified electronic registered delivery service*.

2 ROLES OF GONOTICE SERVICE

2.1 GoNotice Service Provider

The GoNotice *qualified electronic registered delivery service* allows the transmission of user's content, providing evidence of the processing of the transmitted message, including that it was sent, and protects transmitted messages from the risk of loss, theft, damage or unauthorized modification.

In this document, unless otherwise specified, the term QERDS is used to indicate QERDS Service Provider InfoCert.

The complete data of the organization that performs the function of **QERDS** are as follows:

Company Name	**InfoCert – Joint Stock Company (S.p.A)** **Company subject to the management and coordination of Tinexta S.p.A.**
Registered Office	**Piazzale Flaminio 1/B, 00196 – Roma (RM)**
Operational Headquarters	**Via Gian Domenico Romagnosi 4, 00196 - Roma (RM)** **Via Fernanda Wittgens n. 2, 20123 Milano (MI)** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
Legal representative	**Danilo Cattaneo – as CEO**
Phone number	**0683669635**
VAT Number/Tax Code	**07945211006**
Company Register No.	**Business Register N. 07945211006 -** *N. REA* **RM - 1064345**
Website	**https://www.infocert.it**

2.2 Authorized agent

The service is marketed by InfoCert both through a direct sales network and through partners indicated in this document under the name of **Authorized agent** - as defined in paragraph §1.3.4.

The agent's sole task is to resell the service provided by InfoCert.

2.3 Customer

The present person or legal entity is defined in paragraph §1.3.4.

2.4 Owner

The present person or legal entity is defined in paragraph §1.3.4.

2.5 Registration responsible

The present person or legal entity is defined in paragraph §1.3.4.

2.6 Admin-User e Sender-User

The persons within the *Customer*'s organization responsible for managing the service (Admin-User) and the sending of messages (Admin-User or Sender-User) are defined in paragraph §1.3.4.

2.7 Sender

Owner who sends the *message* to the recipient, as defined in paragraph §1.3.4.

2.8 Recipient

The person receiving the *message* from the sender, as defined in paragraph §1.3.4.

3 IDENTIFICATION AND AUTHENTICATION

3.1 General information on identification procedures

The paragraphs of this section describe the procedures used for the identification of the *Owner* required to activate the GoNotice *qualified electronic registered delivery service*.

The identification procedure implies the *identity verification by recognition* of the *Owner* by InfoCert through one of the methods defined below.

3.2 Identification of the Owner - natural or legal person

The request of the *qualified electronic registered delivery service* for an **Owner consisting of a "natural person"** will be carried out through the procedure described in the next paragraph.

The request of the *qualified electronic registered delivery service* for an **Owner consisting of a "legal entity"** (organization) must be carried out by a natural person, the *Registration responsible*, identified in the same way as the *Owner* consisting of a natural person, in one of the ways described in the next paragraph.

The *Registration responsible* must also present the documentation relating to the legal person and the documentation or power of attorney certifying the title to submit the request on behalf of the legal person.

3.2.1 Identification by qualified electronic signature

To activate the GoNotice service, the *Owner* must complete and digitally sign the service activation request form, which must be filled in with the following information:

- Data of the *Owner* of the *qualified electronic registered delivery service*
- Data of the *Registration responsible* (the data of the Responsible coincides with that of the *Owner*, for an *Owner* consisting in a natural person, and with that of the natural person acting on behalf of the *Owner*, for an *Owner* consisting in a legal person)
- Data of the *person* in charge of carrying out the functions of "Admin-user" (see paragraph §1.3.4)
- Acceptance of the general conditions of the service
- Reference (email address) of the person, in the internal technical structure of the *Customer*'s organization, who will manage the operational phases of the service activation.

3.3 Service verification and activation process

3.3.1 Request verification process

Infocert, through its appropriately trained staff, starts the verification process before to proceed with the activation of the service.

The checks carried out to allow activation are the following:

- Verification of the validity of the applicant's signature
- In the event that the *Owner* is a legal entity, InfoCert verifies that the applicant has signing powers
- Possible verification of the power of attorney if the applicant is not the legal representative.

The control, supervision and updating of the procedures necessary for the verification of the signing powers and any checks relating to the power of attorney are carried out by InfoCert under its responsibility.

3.3.2 Service activation

Once the checks are complete, activation proceeds as follows.

InfoCert contacts the technical structure (indicated by the *Owner* in the activation form) to collect information relating to the authentication and authorization system.

The Service *Owner* must indicate the information necessary to enable secure access of at least level 2 (*medium/substantial - LoA3 of ISO-IEC 29115*).

To access the service, InfoCert must appropriately configure, by the Web console, the OAuth 2.0 system dedicated to the *Customer*'s organization, by setting:

- the new *Owner*, with the relevant information
- the *Customer*'s authentication system, as per the specifications of the *Customer*'s technical structure
- the Admin-User, as indicated in the activation form

and inform the *Owner* of the completed configuration.

After activation, the Admin-User will be able to access the GoNotice Web interface (see paragraph §4.3.1) with his/her credentials, defined by the organization within its own authentication system, and appropriately profiled by it. The authentication system must be at least level 2 (*medium/ substantial - LoA3 of ISO-IEC 29115*).

3.4 OAuth 2.0 protocol for authentication

For user authentication (*Admin-User* and *Sender-User*), GoNotice uses OpenID Connect (OIDC). OpenID Connect (OIDC) is an authentication protocol based on OAuth 2.0, a widely adopted standard, that allows applications to authenticate users by verifying identity through an OIDC-compliant Identity Provider (IdP), such as Google, Microsoft Azure, or an enterprise IdP.

By applying strong authentication, with at least level 2 (*medium/substantial - LoA3 of ISO-IEC 29115*) OIDC ensures that sender's accounts adhere to advanced authentication protocols (Multi-Factor Authentication - MFA) for greater security. This is particularly important given the sensitive nature of the messages managed by GoNotice. InfoCert therefore requires that the *Customer*'s organization is equipped with an authentication and authorization service based on OAuth 2.0 protocol (*the most used systems are currently Microsoft Authenticator and Google Authenticator*) and that authentication must be at least level 2 (*medium/substantial - LoA3 of ISO- IEC 29115*).
The responsibility for verifying the identity of the users is therefore delegated to the authentication and authorization service hold by the *Owner*.
InfoCert has the right to not accept authentication systems deemed unsuitable for the use of GoNotice.

3.4.1 Service user profiles

The GoNotice service provides two profiles: The Admin-User and the Sender-User.

3.4.1.1 Admin-User

The person who accesses the GoNotice service through the credentials of the *qualified electronic registered delivery service*, who is responsible for managing the service within the *Customer*'s organization.

In particular, the Admin-User is responsible for registering new users (of the Admin-User and Sender-User type) (see paragraph §1.3.4).

The profile is enabled in the web interface only.

3.4.1.2 Sender-User

User who accesses the GoNotice service through the credentials of the *qualified electronic registered delivery service* and is responsible for sending certified messages (see paragraph §1.3.4) by the profile enabled in the Web interface and in the API.

3.5 Application credentials for API access

In addition to the interactive web interface, the *qualified electronic registered delivery service* provides an API for the sending and verification functions, which can be easily self-integrated by the *Customer*'s applications.

In this scenario, an application of the *Customer* can connect to the service and automatically schedule *message campaigns*, perform checks on the status of deliveries, integrate processes of

the *Customer* requiring certified message deliveries within their services.

For the customer-specific integration, InfoCert issues OAuth 2.0 credentials that the *Customer* can configure into the applications to allow authentication through API.

The API interface provides the functions described in paragraph §4.5.2.

3.5.1 Issuing of API credentials

To get the application credentials, the *Owner*:

- Make a request to InfoCert, indicating an identifier to distinguish the *Customer*'s application/process that will use these credentials
- InfoCert prepares and provides the access credentials in secure mode to the *Owner*.

In the request, it is possible to indicate the duration of the credentials, in any case not more than 15 minutes, that are enough to allow the *Customer* to properly configure the application / process that must use them.

The service, when using the API interface, keeps track in the logs of the operations performed by the applications, through the identification of the credentials used.

The *Owner* must agree with InfoCert the methods of issuing and distributing the credentials on its authentication system which must comply with at least level 2 (*medium/substantial - LoA3 of ISO-IEC 29115*).

3.5.2 Suspending or revoking API credentials

The *Customer* may suspend or revoke the API credentials at any time.

This operation allows to block the access to the service during the authentication phase.

To proceed with the suspension/revocation of the API credentials requested by the *Customer*, InfoCert performs the following steps:

1. Verify the authenticity of the request
2. Suspend/revoke the user and credentials
3. Notify the *Owner* of the removal.

Following suspension/revocation, the access to the service will no longer be permitted.

4 FUNCTIONALITY OF THE SERVICE

4.1 General

The **GoNotice** *qualified electronic registered delivery service*, managed and provided by InfoCert, allows a sender to send qualified certified messages to one or more recipients, according to the in the *Store and Notify* paradigm.

The content of the *message*, which may also contain attachments, is taken over by the service and propagated to the recipient, according to the operating methods described in the present section.

In the transaction of sending the *message* both sender and recipient are identified. All operations performed by the sender and the recipient are tracked and managed by the service in a secure way.

The service does not allow any modification of the original content once submitted.

The following paragraphs describe in detail the operating methods of use of the service.

4.2 How to use the service

The GoNotice *qualified electronic registered delivery service* provides two ways to use the service.

4.2.1 Web interface

In this case, users can use the various features provided by the service by an interactive web interface.

4.2.2 API interface

The GoNotice service can be used by customer-managed processes through a dedicated API (an application interface exposed for the integration of *Customer* applications).

4.3 Access to the service

4.3.1 Acces by Web interface

After the activation, users (*Admin-User* and *Sender-User*) can access to the web interface with their credentials, defined by the *Owner*'s organization within its authentication system, and

appropriately profiled by it.

Access to the GoNotice web interface requires level 2 authentication (*medium/substantial - LoA3 of ISO-IEC 29115*).

Each access requires to re-authenticate to the system.

The recipient (*Receiver*) is also asked to identify to the system, by SPID level 2 authentication system (*medium/substantial - LoA3 of ISO-IEC 29115*) or CIE, to be able to access to the received content.

Once authenticated to the service (see chapter §3), the user can access the Web interface and use all the features of the system until the session expires, or the user explicitly logs out.

4.3.2 Access by API

The access through API is protected by OAuth 2.0 protocol, with credentials issued to the *Owner* (see procedures described in §3.5), which allow the *calling Customer*'s application to be authenticated to the service.

4.3.3 Session and transmission e protocols

Both web and API interfaces use a session mechanism that expires automatically after 1 hour of inactivity.

The access through both Web and API interface uses of HTTPS TLS version 1.2 or 1.3 protocols, ensuring a secure server authentication, a data protection during the sender's sending phase (Web or API interface) and the access to the contents by the *Recipient/Receiver* (Web interface).

4.4 User management

The GoNotice web interface allows the Admin-User to manage the users already present in their Identity Provider (IdP).

Profile management allows to the administrators above to manage and maintain control over access to the system, ensuring that only authorized users can use GoNotice.

Through the Web interface, the Admin-User can register new users (of type *Admin-User* and User- Sender) and assign specific roles and permissions to users within the service.

Specifically, the *Admin-User* is in fact autonomous in being able to:

- enabling and managing of new Admin-Users for service management

- enabling and managing of new Sender-User to prepare and carry out new *message campaigns*.

The Admin-User and Sender-User must be part of the *Customer*'s organization and therefore must be registered in the configured authentication system.

Once the users have been registered, their authentication is delegated to the *Customer*'s authentication system via the OAuth 2.0 protocol.

In case is necessary to revoke the access of one of these users to the GoNotice service, the Admin-User can delete it from the interface. In this way, the user will no longer be able to access GoNotice.

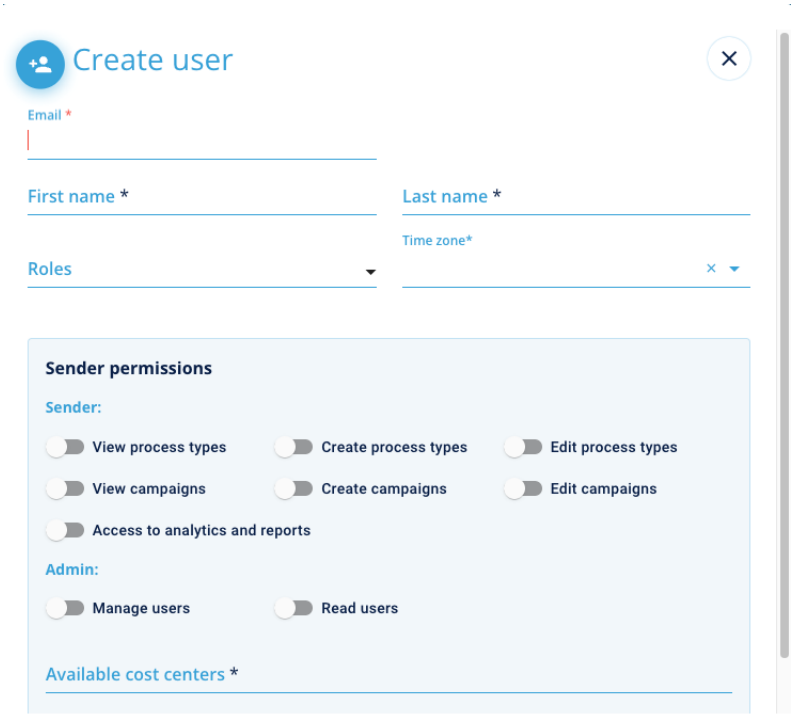

Figure 1- User creation screenshot

To create a new Sender-User, the Admin-User must enter the company email registered on the company's IdP, assign an appropriate role and configure the *cost centre* to which the Sender-User will belong.

The privileges provided for the profiles are the following:

- Admin-User:
  - Manage users: *create/delete and manage users by assigning the cost centre on which*

users have visibility
    - Read users: *view the users registered on the platform*.
- Sender-User:
    - View process types: *view the list of process types already created*
    - Create process types: *create new types of process*
    - Edit process types: *enable sender-user to change process types*
    - View or campaigns: *view the campaigns created*
    - Create campaigns: *create new campaigns*
    - Edit campaigns: *Edit existing campaigns*
    - Access to analytics and reports: *access the Communications Dashboard*

4.5 Sending of messages

To send messages, the *Owner* can choose the method that best suits their needs and preferences:

- through web interface
- through an application API interface

4.5.1 Sending by Web interface

The GoNotice interface provides a platform for configuring and sending messages.

Once logged in to the service (see paragraph §4.3), the user (*Admin-User* and *Sender-User*) accesses an interface that provides the tools needed to setup a *message* creation process.

The first phase consists in defining the basic details, such as the title of the *message*, the list of recipients and the content of the message. Here, the sender can personalize the text, add attachments and select the preferred sending channel among the available options, such as email, SMS or WhatsApp.

Once all the necessary parameters have been defined (Figure 2), the sender can preview the *message* to verify that everything is correct and complete.

GoNotice also offers other features, such as scheduling of the delivery to be sent at a specific time in the future and creating pre-built templates to simplify the process of setting up recurring notifications.

After confirming the details, the sender can send the *message*. Once sent, GoNotice closely monitors the status of the *message*, providing real-time updates on deliveries, opens, and recipient interactions. This complete visibility allows the sender to track the effectiveness of the

message.

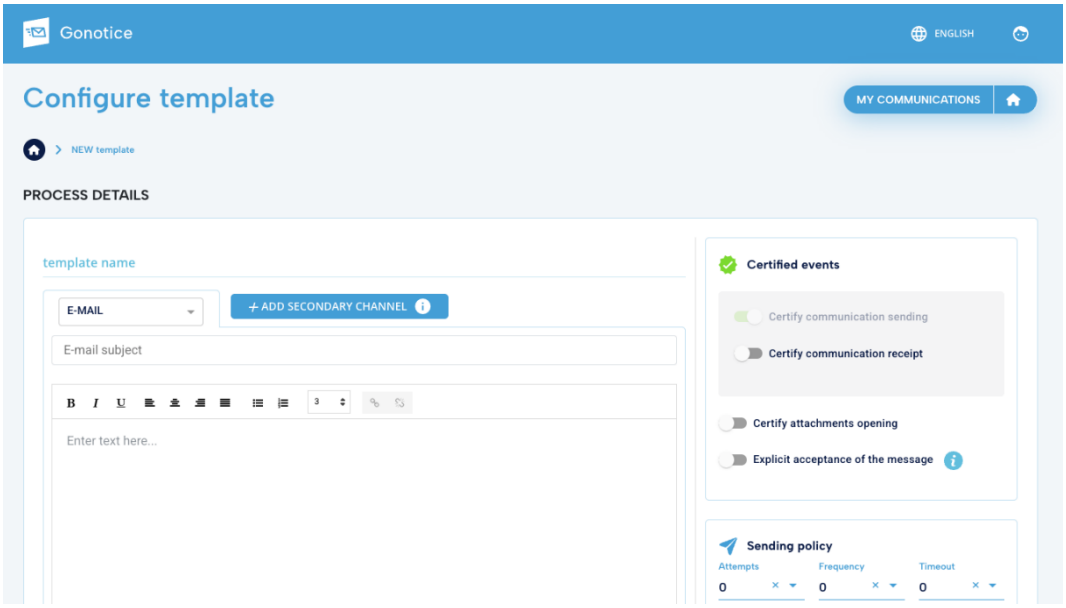

Figure 2 - Process configuration screenshot

4.5.2 API access to the service

GoNotice offers public APIs that allow developers to easily integrate the platform's functionality into their own systems and applications. Access to these APIs is managed via OAuth 2.0 (see paragraph §4.3.2).

OAuth 2.0 provides a number of features that make it ideal for GoNotice API integration. These include secure user credential management, delegation of authorization via access tokens, separation of roles and permissions, and scalability to support large numbers of users and applications.

An online DevPortal is available to further simplify the process of integrating the GoNotice APIs. This platform provides developers with centralized access to detailed documentation, code samples, Swagger specifications, and other resources are available to help them understand and effectively use the GoNotice APIs. Through the DevPortal, developers can access detailed instructions on how to authenticate, make API requests, and utilize all the features the product offers.

4.6 Content management

The GoNotice *qualified electronic registered delivery service* provides that the content of the

submission, with its attachments, is not sent to the recipient through communication channels, but rather:

- the sender's content, to be made available to the recipient, is taken charge by the service and is kept in a protected and secure way within the service
- a unique URL is provided to allow the recipient to access the content through the service
- the URL is forwarded to the recipient through the communication channel chosen by the sender.

The recipient cannot therefore access the content before having completed the service access and identification phases, as required by the QERDS specifications.

4.7 Channels for sending messages

GoNotice offers a variety of channels for sending messages through which the recipient can access the GoNotice interface. The main sending channels offered include email, SMS, and WhatsApp. Each channel has unique characteristics that allow users to choose the one that best suits the type of message and recipient.

InfoCert currently relies on the following providers to send the *message*, through the use of open-source software licenses or APIs made available by the provider as described below:

- **SMS** – Twilio – MIT Open-Source license
- **Email –** Amazon SES (simple email service) - Amazon BOTO – Open-source Apache License 2.0
- **Whatsapp** - REST API

The documentation and usage policies, which include the obligations of the parties in using the service are accessible on the respective websites of the providers.

In addition, GoNotice offers the ability to configure a secondary channel to ensure message delivery even in critical or unexpected situations. This backup channel comes into play if sending through the primary channel encounters difficulties, such as technical problems or unavailability of an external service such as the recipient's mail server. By configuring a secondary channel, users can ensure that the message is still delivered to the recipient, ensuring continuity and reliability in communication.

4.8 Receiving of a message

When GoNotice creates a *message campaign*, it generates initial evidence to track the beginning

of the process. Subsequently, each interaction related to this *message campaign* generates additional evidence, providing a complete trace of the activities performed.

These interactions may include steps as *remote server receiving message*, *recipient opening message*, or *downloading any attachments*. It is important to note that all of these evidence steps are compliant with the standards set by the ETSI (European Telecommunications Standards Institute). Therefore, any feedback received from external systems and the recipient itself will generate additional evidence, helping to provide a detailed and accurate tracking of the entire communication process.

4.9 Evidence

Evidence begins to be generated when the *campaign* is created, and recipients are added. When the *message campaign* is accepted and scheduled, GoNotice creates the SubmissionAcceptance evidence. When the notification is ready to be sent, GoNotice contacts the recipient server or provider and, depending on the service configuration and the outcome of the steps that the *message* takes along its path among the various elements of the system, the relevant set of evidence (NotificationForAcceptance, NotificationAccessTracking, etc...) is generated when the events illustrated in Table 4 and Table 5 occur. If the service is configured to attest attachment viewing, GoNotice generates also the ContentHandover evidence, which confirms that the configured attachments in the *message* were viewed.

All further process events are tracked in line with the provisions of the applicable ETSI standards (see paragraph §1.3.3.1).

4.9.1 Certified events

When a template is configured to send a *message*, the Sender-User has the possibility to choose the type of certification desired for that communication process.

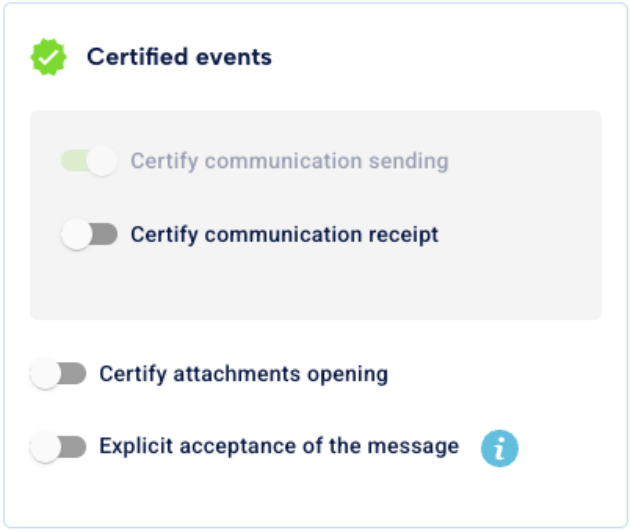

Figure 3 – Configuring certified events

4.9.1.1 Receiving content certification

The certification offered by GoNotice officially attests the receipt of the *message* by the recipient. When enabled, ContentAccessTracking or NotificationAccessTracking evidence is produced depending on the type of message.

4.9.1.2 Opening attachments certification

The *Attachment Opening* certification feature certifies that the recipient has actually opened the files attached to the *message*. This provides concrete and verifiable proof that the attached content has been viewed, adding an additional level of transparency and control. This certification is particularly useful for ensuring traceability and compliance in contexts where it is crucial to know that the recipient has not only received but also opened and viewed the *message*'s attachments. When enabled, this option provides the ContentHandover evidence.

4.9.1.3 Explicit acceptance of the message

The explicit *message acceptance* feature provides clear and verifiable confirmation that the recipient has consciously accepted the *message*. This mechanism requires the recipient to perform a specific action to confirm receipt and acceptance of the message, thus ensuring that the message has not only been received but also accepted with full awareness. When enabled, either ConsignmentAcceptance or ConsignmentRejection evidence is produced, depending on how the recipient interacts with the system.

4.9.2 Evidence supported by GoNotice

The event classification, an excerpt of which is reported in the following tables, is implemented

by GoNotice in full compliance with the relevant ETSI standards (see in particular the Clause 6.2 of the EN 319 522-1 **[7]**).

ETSI evidence	Description
A.1 SubmissionAcceptance	The original message was successfully submitted to the S-ERDS by the Sender. Note: GoNotice service (in the role of S-ERDS) has received the *message* but has not yet sent it. This event indicates that the message part of the *campaign* has entered the system and is ready to be sent.
A.2 SubmissionRejection	The user content that was submitted to the S-ERDS by the Sender-User was not accepted by the S-ERDS
C.1 NotificationForAcceptance	R-ERDS notified the recipient about the availability of a message (without necessarily disclosing its sender, content, etc.) and asked for the recipient's willingness to accept it.
C.2 NotificationForAcceptanceFailure	The recipient could not be notified (or it is clear that it will be impossible to notify the recipient) within a given time period due to technical errors and/or other reasons or no proof of notification within a given period exists. This time period can be determined by legislation, R-ERDS policy rules, or parameters given by the sender or by the S-ERDS.
C.3 ConsignmentAcceptance	The recipient performed an explicit action by indicating to the ERDS which issued the notification the acceptance to receive a user content.
C.4 ConsignmentRejection	The recipient, upon proper identification and authentication, performed an explicit action indicating to the R-ERDS the rejection to receive a user content.
E.1 ContentHandover	The user content successfully crossed the R-ERDS border toward the recipient UA/Application. The related evidence attests that, the user content, at a specific time indicated by the evidence, was delivered to the UA/Application of the recipient upon proper authentication. Note: in this case, as indicated in the paragraph §4.9.1.2, the term *user content* refers to the attachments of the *message* (and not the body).
D.4 ConsignmentNotificationFailure	An attempt to notify the recipient about the availability of the user content failed. The related evidence attests that a notification about the availability of the user content could not be sent to the specified recipient after a certain number of attempts or a timeout. Note: This can happen due to a message delivery timeout when the *message campaign* time limit expires.
F.1 RelayToNonERDS	A user content was successfully forwarded to a non ERDS system for delivery.
F.2 RelayToNonERDSFailure	The attempt to relay a user content to a non ERDS system failed due to

ETSI evidence	Description
	technical errors and/or other reasons.

Table 4 - ETSI evidence supported by GoNotice

In order to implement additional features not explicitly provided for by the ETSI standards, the following events with the relevant evidence are added:

ETSI Evidence	Description
ContentAccessTracking	The user content sent to the recipient has been accessed by the recipient. The related evidence attests that, according to some transaction information collected from the specific consignment mean, the user content sent to the recipient has been accessed by the recipient - properly identified and authenticated - at a specific time as indicated by the evidence. Note: in this case, as indicated in the paragraph §4.9.1.1, the term *user content* refers to the body of the *message* (and not the possible attachments).
NotificationAccessTracking	A notification sent to the recipient has been accessed by the recipient. The related evidence attests that, according to some transaction information collected from the specific notification mean, a notification sent to the recipient has been accessed by the recipient at a specific time as indicated by the evidence. Note: The recipient accesses the notification, sent by GoNotice, containing a link of a specific area of GoNotice system, reserved in a secure and exclusive way for each recipient.
FailoverSubmission	The primary communication channel was not accessible due to a technical error (for example, the email address does not exist, or the server is down). The fallback communication channel is activated. This feature is only applicable when a secondary channel has been configured for delivery.

Table 5 - Evidence created in analogy to that of ETSI standard

4.9.3 Viewing audit summary

Once the submission process is complete, whether this is due to submission policy completion, timeout, or errors, an "audit" button will be enabled.

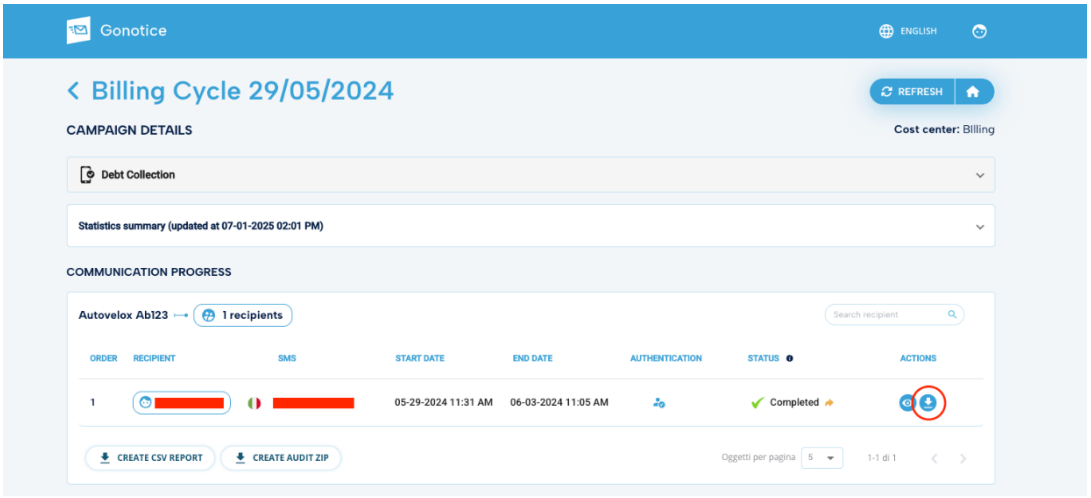

Figure 4 - Communications management dashboard and Audit button

When this button is pressed, a digitally signed report (*Audit Trail*) will be downloaded in PDF format. Within this report, there is a detailed summary of everything that happened during the communication process, providing a clear and understandable overview of the activities and outcomes of the sending operations.

In addition to the summary, the PDF report also includes all the evidence generated during the process, attached in XML format. This evidence set contains precise and detailed information documenting each step of the sending process. Using dedicated software, it is possible to extract and visualize the entire set of evidence for further analysis. This reporting system ensures transparency and traceability, allowing the sender to verify and understand every aspect of the *message* sent via GoNotice.

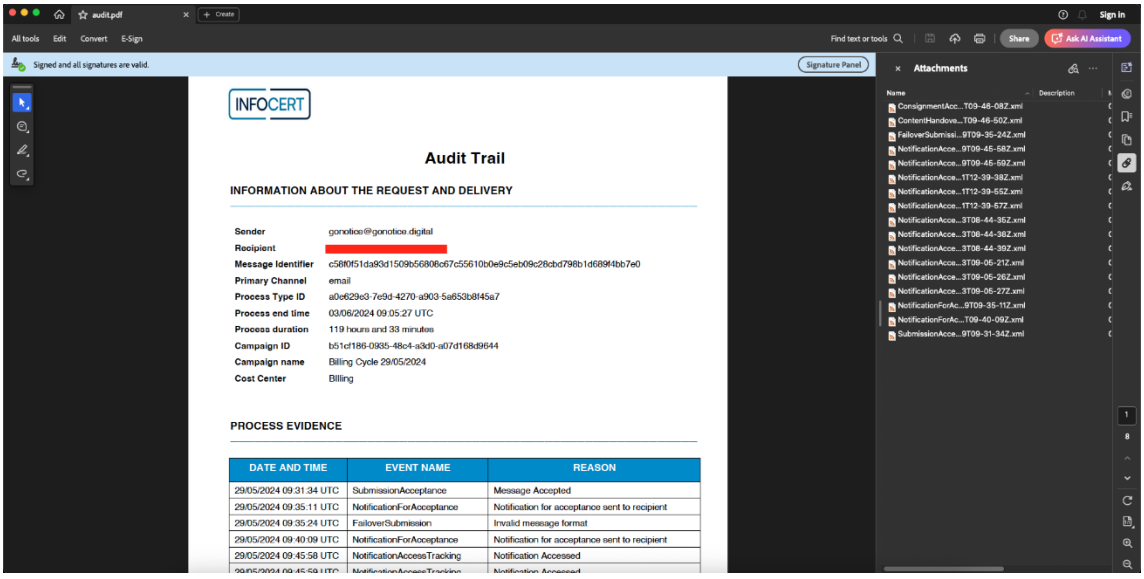

Figure 5 – Audit Trail

4.9.4 Evidence long term preservation

All evidence generated by GoNotice is archived and subject to a retention policy that guarantees its conservation for a period of 20 (twenty) years.

All evidence relating to sender and recipient initial identity verification is archived and subject to a retention policy that guarantees its conservation for a period of 20 (twenty) years.

This means that every interaction, event or activity relating to messages sent through the platform is carefully recorded and kept accessible for a period of time sufficient to satisfy any verification, audit or regulatory compliance needs.

5 SYSTEM USAGE MONITORING

5.1 Access LOG

Access logs are managed by Keycloak software, an open-source identity and access management application. Initially, logs are stored in Keycloak, after which they are transferred to a retention database, where they are stored for at least 2 (two) years.

However, in the case of authentication via the Italian SPID/CIE system, the management of access logs is not managed by Keycloak, but by the eID Gateway, a project created to centralize the access management. Once access is completed, the eID Gateway will take care of retaining access logs for at least 2 (two) years.

5.2 Sending LOG

While using GoNotice, every activity and relevant event is recorded and stored as a log.

These logs are used to track system usage, monitor performance, and identify possible issues. To ensure reliable and long-lasting storage of this data, GoNotice uses Amazon CloudWatch as its logging platform. CloudWatch offers a robust and scalable solution for log management, allowing data to be retained for long periods of time. In particular, logs generated by GoNotice are retained by CloudWatch for at least 2 (two) years, ensuring long-term access to all relevant information about platform usage.

5.3 Service monitoring

To verify the availability of the service, Web probes and Event Management tools have been activated which, in the event of unavailable components, alert system administrators and operators.

Each of these tools, if it detects a malfunction, alerts the relevant persons in charge to carry out the countermeasures foreseen for the type of problem encountered in the service are implemented.

In particular, the probe reports are analysed by the company's Problem Management process (procedure included in the Vision 2000 certified company procedures); the process involves the production of specific outputs.

6 SERVICE LEVELS

6.1 Service availability

Unless otherwise specified in the *General Contract Conditions*, the expected service levels are from 0.00 to 24.00, 7 days a week (minimum availability 99%).

6.2 Third party services

To provide the *qualified electronic registered delivery service*, InfoCert uses third-party services that guarantee high reliability and resilience:

- AWS public cloud for service provision. The architecture includes the use of managed services for containers, storage, backup, etc., with activation of micro services in multiple availability zones of the chosen AWS Regions (the region currently used is *Dublin*).
- Twilio for sending SMS notifications
- AWS SES for sending email notifications
- WhatsApp API for sending notifications
- KeyCloak, as a service for user authentication (IdP OAuth 2.0) and Token
- Kong for exposing service APIs

Immutable backup services are also used for the storage of application data, content and evidence.

6.3 Emergency services

In order to ensure the correct completion of content management and the release of the related evidence (QERDS Evidence set), the following technical and organizational solutions have been prepared.

- **Using Highly Available Systems on the AWS Cloud**, with a microservices architecture active on multiple availability zones, in order to guarantee high reliability of the service
- **Automatic control tools**: automatic tools for checking the system and the various functional components are active in the *qualified electronic registered delivery service*. Based on the problems detected, the automatic tools system provides actions for their resolution or notification to operators to allow their intervention.
- **Disaster Management**: QERDSP InfoCert has adopted the procedures necessary to ensure service continuity even in highly critical situations – see the GoNotice service business continuity document for details.

7 SECURITY MEASURES AND CONTROLS

7.1 General

The specific QERDSP implemented by InfoCert has created a *security system* of the *information system* relating to the *qualified electronic registered delivery service*.

Such *security system* is structured on multiple levels including:

- The use of a public cloud (AWS), which ensures the resilience and security of the services implemented on it.
- A procedural and logistical level, with purely organizational aspects
- A logical level, through the provision of hardware and software technological measures that address the problems and risks associated with this type of service.

This security system is designed to prevent risks arising from system, network and application malfunctions, as well as unauthorized interception or modification of data.

All operational processes of InfoCert QERDSP in the provision of the *qualified electronic registered delivery service* are compliant with the *Company Quality Plan*.

An extract of the InfoCert *security policy* is available upon request to the electronic registered delivery mailbox InfoCert@legalmail.it.

Security policies in InfoCert are reviewed no less than annually and are also updated in the face

of any significant changes. Each review is tracked within the document itself even if no changes were necessary.

7.2 Physical security

Physical security is left to the AWS Cloud service.

The current delivery region is *Dublin*, with active services distributed across three availability zones.

AWS has certifications of compliance under ISO/IEC 27001:2022, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 standards, and its practices are publicly available on the website: The AWS EC2 operational documentation is publicly available on the website: https://docs.aws.amazon.com/.

7.2.1 Data backup

In analogy with what is provided for Certification Authorities, file system backups used by the various platforms present within the CED are also performed regularly for *qualified electronic registered delivery service*.

InfoCert uses the most modern infrastructures for performing backups of disk contents. The execution of snapshots and their archiving is controlled and managed by the products used for backup management.

Backup policies include saving mailboxes on a weekly basis; a daily incremental saving is also provided.

The retention time of any saving is monthly.

7.3 Procedural controls and logical security

7.3.1 Key roles

Key positions are held by professional figures with the necessary experience requirements, professionalism and technical and legal competence, which are continuously verified through annual assessments.

The list of names and the organizational chart of key professional figures was filed with AgID on the occasion of the first accreditation step and is constantly updated to follow the natural evolution of the company organization.

7.3.2 Access to the systems

Access to the systems is permitted only to authorized personnel.

Operators have the right to access the systems with the minimum authorizations necessary to perform their duties.

The systems keep track of accesses and operations performed.

7.3.3 Rules of conduct

The InfoCert Security Policies and related documents illustrate the guidelines and company policy for all services present in the company. These documents aim to create greater awareness and consideration among all staff regarding the confidentiality of information and activities carried out during office hours. Staff are explicitly invited to "maximum confidentiality" regarding all information they come into possession of.

The rules for physical access by employees and external consultants, the rules for using the badge, and the rules for access outside of office hours are given. Part of the documents are dedicated to the security of equipment, systems and IT applications.

The rules regarding the use of the password (confidentiality and the need to change it periodically) and of the PC (use limited to professional use, care and responsibility of the machine, prohibition of using software not released by the appropriate office, rules for remote connection, rules for managing viruses, rules for accessing the Internet and for using e-mail, immediate removal of access if no longer necessary) are given.

The aim of the policies expressed therein is also to minimize the possibility that illegal or unauthorized software may be introduced, even unintentionally, into the internal network.

All non-confidential documents addressed to staff are available on the company intranet.

7.3.4 Recommendations for the owner

The *Owner* must securely store the credentials and authentication tools for the service; must use the service only for the purposes provided for the present Practice Statement and by current national and international laws.

It is advisable to equip workstations with constantly updated antivirus software to ensure greater security for what is sent and received.

7.4 Control of the staff

7.4.1 Qualifications, experience and required authorizations

Once the annual *Human Resources planning* has been carried out, the Function/Organizational Structure Manager identifies the characteristics and skills of the resource to be included (job profile). Subsequently, in agreement with the selection manager, the search and selection process is activated.

7.4.2 Procedures for checking work experience gained

The identified candidates participate in the selection process by undergoing an initial cognitive-motivational interview with the selection manager and a subsequent technical interview with the Function/Organizational Structure manager, aimed at verifying the skills declared by the candidate. Additional verification tools are exercises and tests.

7.4.3 Training requirements

To ensure that no person can individually compromise or alter the overall security of the system or carry out unauthorized activities, it is planned to entrust the operational management of the system to different people, with separate and well-defined tasks. The personnel responsible for designing and providing the *qualified electronic registered delivery service* are InfoCert employees and have been selected based on their experience in designing, implementing and managing IT services, with characteristics of reliability and confidentiality. Training interventions are periodically planned to develop awareness of the assigned tasks. In particular, before the insertion of personnel into the operational activity, training interventions are carried out with the aim of providing all the skills (technical, organizational and procedural) necessary to carry out the assigned tasks.

7.4.4 Training update frequency

At the beginning of each year, an analysis of training needs is carried out in preparation for the definition of training activities to be provided during the year. The analysis is structured as follows:

- Meeting with the Management for the collection of data relating to the training needs necessary for achieve business goals;
- Interview with the Managers for the identification of the specific training needs of their areas;
- Return of collected data to the Company Management for closure and approval of the Plan Formative.

By the month of February, the *Training Plan* thus defined will be shared and made public.

7.4.5 Work shift rotation frequency

Presence on site or in agile working mode (smart working) is distributed over a time slot from 08:00 to 19:00 from Monday to Friday.

The control of production environments during the night and holiday periods is ensured through a rotation plan of availability prepared by the organizational unit manager, on a monthly basis, at least 10 days in advance. Depending on the need, interventions may be conducted remotely (teleintervention) or require access to the offices.

Provided that the necessary technical and professional requirements are met, the Company shall arrange, for the greatest possible number of workers, the *on-call activities*, giving priority to employees who request it.

7.4.6 Sanctions for unauthorized actions

Reference is made to the Italian *CCNL Metalworkers and installation of private industry systems* agreement (National Labor Collective Agreement) for the procedure of imposing sanctions.

7.4.7 Checks on non-employee staff

Access to non-employee personnel is regulated by a specific company policy.

7.4.8 Documentation to be provided by staff

Upon hiring, the employee must provide a copy of a valid identity document, a copy of a valid health card and a passport-sized photo for the badge to access the premises. The employee must then complete and sign the consent to the processing of personal data and the commitment not to disclose confidential information and/or documents. Finally, the employee must read the Code of Ethics and the InfoCert Netiquette.

7.5 Compromission of the service and business continuity

7.5.1 Incident management procedures

InfoCert QERDSP has described the incident management procedures within the ISO 27000 certified SGSI. Each possible incident, as soon as it is detected, is subject to timely analysis, identification of corrective countermeasures and verbalization by the service manager. The verbalization is digitally signed; a copy is also sent to AgID, together with the declaration of the intervention actions aimed at eliminating the causes that may have given rise to the incident, if under the control of InfoCert in compliance with Article 19 of the eIDAS Regulation [1].

7.5.2 Corruption of keys, software or data

To increase resilience in case of problems or compromise of the key used to sign the evidence, InfoCert has prepared two different keys and certificates, with different encryption technologies (RSA 2048 and Elliptic Curves). In case of compromise of one of the keys, it is expected to suspend its use and use only the uncompromised key.

All evidence of the *qualified electronic registered delivery service* is brought into the InfoCert storage system, that is subject to retention ensuring integrity and availability even in the event of compromise of the key used or the service.

The data is managed, within the QERDS service, in a secure manner on redundant storage, managed by the Cloud Provider, with active immutable backups to guarantee maximum security.

The software is managed according to standard procedures according to ISO 9000 quality systems.

7.5.3 Digital signature and timestamp services

The QERDS service uses the qualified electronic signature and the InfoCert time stamping service in the management of contents and evidence, thus ensuring the maximum protection in terms of security and resilience of the service.

7.6 Trust service provider or trusted service termination

InfoCert has provided a termination plan for all scheduled and unscheduled cases, in which it is necessary to interrupt the provision of the QERDS service.

In the event of termination of the QERDS Provider activity, InfoCert will communicate this intention to the Supervisory Authority (AgID) and the certification body (CAB) at least 6 (six) months in advance, indicating, if necessary, the replacement QERDS Provider. With the same advance notice, InfoCert will informs all active *Owners* of *qualified electronic registered delivery service* about the cessation of activities.

In the event that a replacement provider is not indicated, the operating procedures for accessing the information (evidence) still in the care of the QERDSP InfoCert, who is ceasing the activity, will be clearly specified in the aforementioned communication.

Please see the GoNotice *QERDS Termination Plan* document for the *qualified electronic registered delivery service*s available at InfoCert QERDSP.

7.7 Cybersecurity controls

7.7.1 Server-specific security requirements

The operating system of the devices, servers and computers used in the setup, and the management and provision of the *qualified electronic registered delivery service* are made secure (hardened). That is, they are configured in such a way as to minimize the impact of any vulnerabilities by eliminating all the functions that are not needed for the operation and the management of the service itself.

7.7.2 Vulnerability assessments

InfoCert periodically carries out assessments on the System's vulnerabilities (vulnerability assessment) and anti-intrusion tests (penetration test). Based on the results, all countermeasures to secure the applications are implemented.

7.7.3 Security requirements for system administrators

Access by System Administrators, appointed for this purpose in accordance with the provisions of current legislation, occurs through dedicated applications designed to maintain the appropriate level of security and privileges to act on systems, configurations and applications only after individual authentication. Access is tracked, logged and stored for 12 months.

8 CONFORMITY ASSESMENTS AND CONTROLS

To obtain the qualification of *qualified* and *non-qualified trust service provider*, in compliance with the eIDAS Regulation [1], it is necessary to complete the procedure set out in Article 21 of the aforementioned Regulation.

InfoCert has submitted to AgID the specific request to obtain recognition as a *qualified trust service provider* by presenting a report of the *conformity assessment* with the Regulation (*Conformity Assessment Report - CAR*) issued by an *assessment body* authorized by the relevant national body (**CAB**), which in Italy is **ACCREDIA**.

InfoCert provides the service as a *qualified trust service provider* pursuant to eIDAS Regulation (EU) No. 910/2014 [1] of 23 July 2014, on the basis of a *conformity assessment* carried out by the *Conformity Assessment Body* **CSQA Certificazioni S.r.l.**, pursuant to the above Regulation and the ETSI EN 319 401 standard [5], according to the eIDAS [1] evaluation scheme defined by **ACCREDIA** in compliance with the ETSI EN 319_403 [9] and UNI CEI EN ISO/IEC 17065:2012 standards.

8.1 Frequency or circumstances for conformity assessment

The *conformity assessment* is repeated every 2 (two) years, but every year the CAB performs a surveillance audit.

8.2 Identity and qualifications of persons carrying out the controls

The assessment is carried out by:

Company name	**CSQA Certificazioni S.r.l.**
Registered office	**Via S. Gaetano n. 74, 36016 Thiene (VI)**
Phone number	**+39 0445 313011**
Company Register No.	**Business Register no. 02603680246/REA no. 258305**
VAT Number/Tax Code	**02603680246**
Website	**https://www.csqa.it**

8.3 Relationships between InfoCert e CAB

InfoCert and CSQA have no financial interests or business relationships.

There are no ongoing commercial or partnership relationships that could create bias for or against InfoCert in the objective evaluation of CSQA.

8.4 Aspects subject to the assessment

The CAB is required to assess the conformity of the adopted procedures, the organization of the QERDSP InfoCert, the organization of roles, the training of personnel, and the contractual documentation with respect to the Practice Statement, the Regulation and the applicable legislation.

8.5 Actions in case of non-compliance

In the event of non-compliance, the CAB will decide whether to send the report to AgID anyway, or whether to reserve the right to re-perform the audit after the non-compliance has been remedied.

InfoCert is committed to resolving all non-conformities in a timely manner, implementing all necessary improvement and adjustment actions.

9 OTHER LEGAL AND BUSINESS ASPECTS

9.1 Insurance coverage

TSP InfoCert has stipulated an insurance contract to cover the risks of the activity and damages caused to third parties, which has a coverage with the following maximum limits:

- 10.000.000 euros for a single incident;
- 10.000.000 euros per year.

9.2 Intellectual property

9.3 Representations and warranties

InfoCert retains responsibility for compliance with the procedures prescribed in its information security policy, even when some functions are delegated to another entity, pursuant to art. 2.4.1. of the Annex to the Commission Implementing Regulation (EU) 2015/1502.

The *Owner* is responsible for the truthfulness of the data communicated in the *Service Activation Request*. If the *Owner*, at the time of identification, has, even through the use of false personal documents, concealed his/her real identity or falsely declared to be another person or, in any case, acted in such a way as to compromise the identification process and the related results indicated in the certificate, he/she will be considered responsible for all damages deriving to InfoCert QERDSP and/or third parties from the inaccuracy of the information contained in the request, with the obligation to guarantee and indemnify InfoCert QERDSP from any requests for compensation for damages.

The *Owner* is responsible for any damages caused to InfoCert QERDSP and/or third parties in the event of a delay on their part in activating the procedures set out in paragraph §3.5.2 of this Practice Statement (revocation and suspension of the service).

9.4 Official contact channels

Please refer to the procedures and contact channels in paragraph §2.1 and in particular to the Person Responsible for the Practice Statement indicated in paragraph §1.4.

APPENDIX A — DIGITAL SIGNATURE CERTIFICATES USED BY QERDS

Electronic Signature Signing Certificate - RSA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 28666201 (0x1b56959)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IT, O=InfoCert S.p.A., OU=Qualified Trust Service Provider/2.5.4.97=VATIT-
07945211006, CN=InfoCert Qualified Electronic Signature CA 3
        Validity
            Not Before: Jun  5 15:05:04 2024 GMT
            Not After : Jun  5 00:00:00 2027 GMT
        Subject: CN=InfoCert QERDS GoNotice/2.5.4.97=NTRIT-07945211006, C=IT, L=ROMA, O=InfoCert
S.p.A./dnQualifier=8d3e3081-f168-492f-983f-ec4155009b87
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:c3:4b:1d:27:c9:4e:cb:39:27:cd:8e:78:4f:
                    d2:21:b6:ee:5c:9e:64:56:e6:66:4c:3e:2f:c1:fb:
                    54:d7:29:e5:26:e3:e4:6e:3b:2c:e1:70:d0:25:6b:
                    1a:c9:f5:94:93:a9:fb:ff:2d:07:32:11:8e:e9:fc:
                    81:2b:89:de:8d:b3:72:56:de:3d:07:c6:84:1e:ce:
                    75:f9:0c:47:d5:65:0b:20:2e:59:6f:4a:d7:b9:d2:
                    a9:1e:4e:e8:af:09:39:cc:4b:e6:c3:e7:d0:40:aa:
                    fa:3e:ab:37:95:e1:6c:54:37:5b:d5:ab:2e:01:d7:
                    36:08:cc:c1:3d:22:49:47:cc:61:99:15:c1:b5:2a:
                    c6:0c:68:f1:02:09:ec:52:9e:9d:5a:a6:d2:c4:18:
                    e0:fd:dc:90:16:a4:5e:4d:b8:38:ee:1a:2e:75:8f:
                    c3:f9:38:be:09:87:ca:64:85:10:15:5b:91:be:b7:
                    cc:9d:24:0b:6c:3b:21:e0:a4:32:3e:24:67:02:06:
                    8f:31:cc:9f:3c:03:06:55:a9:c9:5e:b3:65:37:a2:
                    d8:8a:e3:6f:40:2d:d1:61:ce:92:76:80:cf:3e:5d:
                    13:12:37:80:28:ac:37:6c:e0:5b:e9:67:67:50:69:
                    30:16:90:53:a6:4f:62:a3:0e:7a:34:1d:3d:75:50:
                    cf:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Authority Information Access:
                OCSP - URI:http://ocsp.qc.ca3.InfoCert.it/
                CA Issuers - URI:http://cert.InfoCert.it/ca3/qc/CA.crt

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.InfoCert.it/ca3/qc/CRL39.crl

URI:ldap://ldap.InfoCert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRL39,ou%3
DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList

            X509v3 Certificate Policies:
                Policy: 0.4.0.194112.1.3
                Policy: 1.3.76.36.1.1.46
                  CPS: http://www.firma.InfoCert.it/documentazione/manuali.php

            qcStatements:
```

```
0v0......F..0......F..0......F.....0......F..0......F...0>.....F..0402.,https://www.firma.InfoCert.i
t/pdf/PKI-DS.pdf..en
            X509v3 Key Usage: critical
                Non Repudiation
            X509v3 Authority Key Identifier:
                keyid:9B:3B:1B:18:6A:3E:A2:04:03:F4:D7:99:10:CF:97:11:4C:F1:AA:DE

            X509v3 Subject Key Identifier:
                6E:B3:BF:27:A7:32:26:BC:70:3A:F9:C9:E4:1E:13:4B:05:93:93:80
    Signature Algorithm: sha256WithRSAEncryption
         25:43:00:68:d4:db:06:d4:1d:84:50:83:28:0f:7c:1e:53:c9:
         d8:d0:5e:dd:cb:f0:54:04:5c:03:86:c5:cf:f1:c2:9b:8f:bb:
         02:71:78:63:8a:02:18:85:50:d8:1b:af:82:9e:3f:3d:7d:1c:
         fb:b7:d2:e9:70:18:c4:5f:b5:3b:36:76:17:b3:18:f7:c3:5b:
         c6:50:87:af:92:db:4d:e2:b6:94:4d:99:25:c3:8d:19:f7:12:
         cb:e6:7d:e9:ce:6a:24:68:0d:b2:02:ff:f8:94:32:39:38:84:
         80:d4:c7:8f:be:44:49:03:de:f1:68:e5:7d:0b:15:2f:7f:42:
         ed:6b:d2:37:33:20:ca:6e:8b:75:86:8a:a0:19:f8:7d:09:d7:
         ac:05:1e:18:65:6d:bb:61:13:71:b1:8c:33:4f:ba:b2:96:c3:
         8b:81:07:10:44:a6:1f:70:02:ef:02:1c:8b:43:0f:c7:9e:68:
         13:4b:c8:5d:13:5f:51:3f:51:5d:c4:4d:4b:ce:f7:e0:9f:da:
         f6:dc:1a:ec:04:2f:5c:a0:67:58:5d:6c:34:55:13:3b:49:b7:
         80:8f:b4:2f:83:b1:0a:78:60:1c:b9:31:8f:3d:fd:1f:73:a4:
         19:aa:9f:b8:b6:eb:26:5c:95:3a:31:38:bf:ab:32:48:f3:fa:
         d7:a4:98:9a:07:42:6d:83:d1:56:6b:37:25:6f:08:27:63:c0:
         66:9a:6e:4e:57:7c:11:7c:4c:1b:2e:60:94:b8:ca:9e:49:e1:
         f9:c9:15:63:e3:db:0f:1d:54:80:db:b3:82:7e:df:59:2f:55:
         bf:9d:48:6b:f2:ad:b2:b2:33:96:09:0e:22:46:fb:a3:1f:3e:
         85:48:06:49:e6:c6:59:ae:d3:14:58:b7:a1:a4:3b:99:5f:1d:
         cd:f9:de:71:5a:36:87:97:59:78:73:de:0d:df:03:b9:b2:97:
         4d:b5:3d:d9:bb:02:89:8d:e1:d0:af:4f:37:39:ae:35:8e:55:
         2a:c1:ef:48:67:21:07:fd:48:28:92:ad:73:48:0c:75:80:be:
         73:d2:83:c1:3d:0f:c8:1e:b0:e3:1f:37:6f:a3:8e:db:31:39:
         54:de:66:9b:b7:52:9b:c4:11:e4:2a:31:a8:7a:36:a7:89:d1:
         d1:2a:a2:f8:50:6a:36:25:c4:ad:e8:a6:eb:cd:ad:d5:b8:94:
         de:da:b1:34:12:73:9c:25:a6:ff:98:36:81:e2:91:08:5f:51:
         63:02:6a:f3:2f:34:18:20:05:8d:fd:71:0c:56:f7:da:3e:f2:
         6f:08:44:9b:6a:11:7a:24:29:50:9d:9f:a2:08:92:53:b7:9b:
         97:d5:06:d2:42:b6:9d:a2
```

```
-----BEGIN CERTIFICATE-----
MIIHhTCCBW2gAwIBAgIEAbVpWTANBgkqhkiG9w0BAQsFADCBpTELMAkGA1UEBhMCSVQxGDAWBgNVBAoMD0luZm9DZXJ0IFMucC5B
LjEpMCcGA1UECwwgUXVhbGlmaWVkIFRydXN0IFNlcnZpY2UgUHJvdmlkZXIxGjAYBgNVBGEMEVZBVElULTA3OTQ1MjExMDA2MTUw
MwYDVQQDDCxJbmZvQ2VydCBRdWFsaWZpZWQgRWxlY3Ryb25pYyBTaWduYXR1cmUgQ0EgMzAeFw0yNDA2MDUxNTA1MDRaFw0yNzA2
MDUwMDAwMDBaMIGjMSAwHgYDVQQDDBdJbmZvQ2VydCBRRVJEUyBHb05vdGljZTEaMBgGA1UEYQwRTlRSSVQtMDc5NDUyMTEwMDYx
CzAJBgNVBAYTAklUMQ0wCwYDVQQHDARST01BMRgwFgYDVQQKDA9JbmZvQ2VydCBTLnAuQS4xLTArBgNVBC4TJDhkM2UzMDgxLWYx
NjgtNDkyZi05ODNmLWVjNDE1NTAwOWI4NzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKvDSx0nyU7LOSfNjnhP0iG2
7lyeZFbmZkw+L8H7VNcp5Sbj5G47LOFw0CVrGsn1lJOp+/8tBzIRjun8gSuJ3o2zclbePQfGhB7OdfkMR9VlCyAuWW9K17nSqR5O
6K8JOcxL5sPn0ECq+j6rN5XhbFQ3W9WrLgHXNgjMwT0iSUfMYZkVwbUqxgxo8QIJ7FKenVqm0sQY4P3ckBakXk24OO4aLnWPw/k4
vgmHymSFEBVbkb63zJ0kC2w7IeCkMj4kZwIGjzHMnzwDBlWpyV6zZTei2Irjb0At0WHOknaAzz5dExI3gCisN2zgW+lnZ1BpMBaQ
U6ZPYqMOejQdPXVQz98CAwEAAaOCArswggK3MAkGA1UdEwQCMAAwbgYIKwYBBQUHAQEEYjBgMCsGCCsGAQUFBzABhh9odHRwOi8v
b2NzcC5xYy5jYTMuaW5mb2NlcnQuaXQvMDEGCCsGAQUFBzAChiVodHRwOi8vY2VydC5pbmZvY2VydC5pdC9jYTMvcWMvQ0EuY3J0
MIH7BgNVHR8EgfMwgfAwge2ggeqggeeGJ2h0dHA6Ly9jcmwuaW5mb2NlcnQuaXQvY2EzL3FjL0NSTDM5LmNybIaBu2xkYXA6Ly9s
ZGFwLmluZm9jZXJ0Lml0L2NuJTNESW5mb0NlcnQlMjBRdWFsaWZpZWQlMjBFbGVjdHJvbmljJTIwU2lnbmF0dXJlJTIwQ0ElMjAz
JTIwQ1JMMzksb3UlM0RRdWFsaWZpZWQlMjBUcnVzdCUyMFNlcnZpY2UlMjBQcm92aWRlcixvJTNESU5GT0NFUlQlMjBTUEEsYyUz
RElUP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwZQYDVR0gBF4wXDAJBgcEAIvsQAEDME8GBitMJAEBLjBFMEMGCCsGAQUFBwIB
FjdodHRwOi8vd3d3LmZpcm1hLmluZm9jZXJ0Lml0L2RvY3VtZW50YXppb25lL21hbnVhbGkucGhwMIGEBggrBgEFBQcBAwR4MHYw
CAYGBACORgEBMAgGBgQAjkYBBDALBgYEAI5GAQMCARQwEwYGBACORgEGMAkGBwQAjkYBBgIwPgYGBACORgEFMDQwMhYsaHR0cHM6
Ly93d3cuZmlybWEuaW5mb2NlcnQuaXQvcGRmL1BLSS1EUy5wZGYTAmVuMA4GA1UdDwEB/wQEAwIGQDAfBgNVHSMEGDAWgBSbOxsY
aj6iBAP015kQz5cRTPGq3jAdBgNVHQ4EFgQUbrO/J6cyJrxwOvnJ5B4TSwWTk4AwDQYJKoZIhvcNAQELBQADggIBACVDAGjU2wbU
HYRQgygPfB5TydjQXt3L8FQEXAOGxc/xwpuPuwJxeGOKAhiFUNgbr4KePz19HPu30ulwGMRftTs2dhezGPfDW8ZQh6+S203itpRN
mSXDjRn3EsvmfenOaiRoDbIC//iUMjk4hIDUx4++REkD3vFo5X0LFS9/Qu1r0jczIMpui3WGiqAZ+H0J16wFHhhlbbthE3GxjDNP
urKWw4uBBxBEph9wAu8CHItDD8eeaBNLyF0TX1E/UV3ETUvO9+Cf2vbcGuwEL1ygZ1hdbDRVEztJt4CPtC+DsQp4YBy5MY89/R9z
```

```
pBmqn7i26yZclToxOL+rMkjz+tekmJoHQm2D0VZrNyVvCCdjwGaabk5XfBF8TBsuYJS4yp5J4fnJFWPj2w8dVIDbs4J+31kvVb+d
SGvyrbKyM5YJDiJG+6MfPoVIBknmxlmu0xRYt6GkO5lfHc353nFaNoeXWXhz3g3fA7myl021Pdm7AomN4dCvTzc5rjWOVSrB70hn
IQf9SCiSrXNIDHWAvnPSg8E9D8gesOMfN2+jjtsxOVTeZpu3UpvEEeQqMah6NqeJ0dEqovhQajYlxK3opuvNrdW4lN7asTQSc5wl
pv+YNoHikQhfUWMCavMvNBggBY39cQxW99o+8m8IRJtqEXokKVCdn6IIklO3m5fVBtJCtp2i
-----END CERTIFICATE-----
```

Electronic Signature Signing Certificate - EC

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1c:72:de:8f:74:2e:09:a0:0e:58:31:d6:38:ff:d4:4e:4f:d2:6a:c6
    Signature Algorithm: ecdsa-with-SHA384
        Issuer:  C=IT,  O=InfoCert  S.p.A.,  OU=Qualified  Trust  Service  Provider/2.5.4.97=VATIT-
07945211006, CN=InfoCert Qualified Electronic Signature EC CA 4
        Validity
            Not Before: Jun  5 14:53:35 2024 GMT
            Not After : Jun  5 00:00:00 2029 GMT
        Subject:  CN=InfoCert  QERDS  GoNotice/2.5.4.97=NTRIT-07945211006,  C=IT,  L=ROMA,  O=InfoCert
S.p.A./dnQualifier=0393f379-5d48-4ce0-8922-307ca4aebd17
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:1a:b1:6d:4d:5f:7b:63:01:00:f8:8f:7e:91:59:
                    7b:9b:b7:71:ae:91:7c:b8:7f:ef:57:89:8f:55:89:
                    56:45:a4:20:af:63:de:64:4a:22:d6:b4:e6:f1:91:
                    1b:5e:39:34:c0:b2:23:5f:c7:e2:0c:89:a7:c1:84:
                    90:50:c2:99:e0
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Certificate Policies:
                Policy: 0.4.0.194112.1.3
                Policy: 1.3.76.36.1.1.46
                  CPS: http://www.firma.InfoCert.it/documentazione/manuali.php
            qcStatements:

0v0......F..0......F.....0......F..0>.....F..0402.,https://www.firma.InfoCert.it/pdf/PKI-
DS.pdf..en0......F..0......F...
            Authority Information Access:
                OCSP - URI:http://ocsp.qcec.ca4.InfoCert.it
                CA Issuers - URI:http://crl.ca4.InfoCert.it/qcec/CA.crt

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.ca4.InfoCert.it/qcec/CRL01.crl
```

```
            X509v3 Key Usage: critical
                Non Repudiation
            X509v3 Authority Key Identifier:
                keyid:8C:DF:7C:B8:F0:94:15:36:0B:7F:DF:81:71:F5:DB:41:5D:3B:FD:FC
            X509v3 Subject Key Identifier:
                E9:89:EE:6B:F7:A7:EA:A2:22:35:B2:D3:9A:6F:7E:87:7F:BA:21:16
    Signature Algorithm: ecdsa-with-SHA384
         30:65:02:30:09:aa:0d:ab:a7:6e:ed:b7:2d:f6:63:64:82:8a:
         e4:15:b2:48:24:e2:a1:0f:a3:e7:7a:5a:5d:fa:56:90:75:8f:
         df:de:a9:3f:96:98:dc:57:8f:7e:de:63:fa:4b:2f:94:02:31:
         00:9f:f6:a3:73:dc:38:bd:9e:7f:e8:9d:fb:32:62:c8:25:6a:
         26:04:03:b6:b3:08:75:17:ca:7d:1e:4f:ef:32:22:5a:df:3a:
         42:55:23:fd:99:be:eb:59:b6:42:22:8f:6e
```

```
-----BEGIN CERTIFICATE-----
MIIEbDCCA/KgAwIBAgIUHHLej3QuCaAOWDHWOP/UTk/SasYwCgYIKoZIzj0EAwMwgagxCzAJBgNVBAYTAklUMRgwFgYDVQQKDA9J
bmZvQ2VydCBTLnAuQS4xKTAnBgNVBAsMIFF1YWxpZmllZCBUcnVzdCBTZXJ2aWNlIFByb3ZpZGVyMRowGAYDVQRhDBFWQVRJVC0w
Nzk0NTIxMTAwNjE4MDYGA1UEAwwvSW5mb0NlcnQgUXVhbGlmaWVkIEVsZWN0cm9uaWMgU2lnbmF0dXJlIEVDIENBIDQwHhcNMjQw
NjA1MTQ1MzM1WhcNMjkwNjA1MDAwMDAwWjCBozEgMB4GA1UEAwwXSW5mb0NlcnQgUUVSRFMgR29Ob3RpY2UxGjAYBgNVBGEMEU5U
UklULTA3OTQ1MjExMDA2MQswCQYDVQQGEwJJVDENMAsGA1UEBwwEUk9NQTEYMBYGA1UECgwPSW5mb0NlcnQgUy5wLkEuMS0wKwYD
VQQuEyQwMzkzZjM3OS01ZDQ4LTRjZTAtODkyMi0zMDdjYTRhZWJkMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQasW1NX3tj
AQD4j36RWXubt3GukXy4f+9XiY9ViVZFpCCvY95kSiLWtObxkRteOTTAsiNfx+IMiafBhJBQwpngo4IB+zCCAfcwCQYDVR0TBAIw
ADBlBgNVHSAEXjBcMAkGBwQAi+xAAQMwTwYGK0wkAQEuMEUwQwYIKwYBBQUHAgEWN2h0dHA6Ly93d3cuZmlybWEuaW5mb2NlcnQu
aXQvZG9jdW1lbnRhemlvbmUvbWFudWFsaS5waHAwgYQGCCsGAQUFBwEDBHgwdjAIBgYEAI5GAQEwCwYGBACORgEDAgEUMAgGBgQA
jkYBBDA+BgYEAI5GAQUwNDAyFixodHRwczovL3d3dy5maXJtYS5pbmZvY2VydC5pdC9wZGYvUEtJLURTLnBkZhMCZW4wEwYGBACO
RgEGMAkGBwQAjkYBBgIwcAYIKwYBBQUHAQEEZDBiMCwGCCsGAQUFBzABhiBodHRwOi8vb2NzcC5xY2VjLmNhNC5pbmZvY2VydC5p
dDAyBggrBgEFBQcwAoYmaHR0cDovL2NybC5jYTQuaW5mb2NlcnQuaXQvcWNlYy9DQS5jcnQwOgYDVR0fBDMwMTAvoC2gK4YpaHR0
cDovL2NybC5jYTQuaW5mb2NlcnQuaXQvcWNlYy9DUkwwMS5jcmwwDgYDVR0PAQH/BAQDAgZAMB8GA1UdIwQYMBaAFIzffLjwlBU2
C3/fgXH120FdO/38MB0GA1UdDgQWBBTpie5r96fqoiI1stOab36Hf7ohFjAKBggqhkjOPQQDAwNoADBlAjAJqg2rp27tty32Y2SC
iuQVskgk4qEPo+d6Wl36VpB1j9/eqT+WmNxXj37eY/pLL5QCMQCf9qNz3Di9nn/onfsyYsglaiYEA7azCHUXyn0eT+8yIlrfOkJV
I/2ZvutZtkIij24=
-----END CERTIFICATE-----
```