TECHNICAL ANNEX
GoNotice

***

1. EXTERNAL REFERENCES:

Documentation	Detailed links
Policy and Practice Statement	https://qtsp.infocert.it/pdf/ICERT-QERDS-MO-ENG.pdf
User Manual	https://knowledgecenter.infocert.digital/home/guida/manuale-utente-edelivery-gonotice
API Documentation	https://developers.infocert.digital/gonotice/
Support links (FAQs, videos, guides)	https://knowledgecenter.infocert.digital/cerca?searchText=GoNotice&idProdotto=286

2. Service Description – Introduction

Tinexta Infocert, for the purposes of this document, acts as a qualified trust service provider (hereinafter "QTSP") for the Qualified Certified Electronic Delivery Service (hereinafter the "Service" or "QERDS"), in accordance with the provisions of the ICERT-QERDS-MO policy and practice statement (hereinafter also "CPS" or "PS").
For these services, Tinexta Infocert has obtained a conformity assessment carried out by CAB CSQA Certificazioni S.r.l. in accordance with the eIDAS Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, as well as the applicable ETSI standards, including ETSI EN 319 401, ETSI EN 319 521, ETSI EN 319 522-1, ETSI EN 319 522-2, ETSI EN 319 522-3, in accordance with the eIDAS assessment scheme defined by ACCREDIA pursuant to the standards ETSI EN 319 403 and UNI CEI ISO/IEC 17065:2012.

For this service, Tinexta Infocert has obtained accreditation from AgID and is listed, as required by the eIDAS Regulation, on the *Trusted Service List,* which can be consulted at the following link: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls.

GoNotice is an Electronic Registered Delivery Service (ERDS) solution that enables the creation, sending and tracking of certified multi-channel communications (e.g. via email, SMS or WhatsApp, etc.), facilitating secure and certified digital communication processes between sender and recipient.
The electronic certified delivery service, in its qualified form (QERDS), enables the transmission of content whilst providing evidence regarding the handling of the transmitted message and protecting the transmitted content from the risk of loss, theft, damage or unauthorised alterations.
GoNotice, when operating in QERDS mode, is able to provide legally valid proof of the sending, receipt and reading of a message, which is admissible in court proceedings.
The Service is identified by a specific Object Identifier (OID) described in the policy and practice statement.
This Technical Annex forms an integral and substantial part of the service purchase contract (hereinafter the "Agreement") entered into with the Customer.
The General Activation Condition (hereinafter the "GAC"), of which this Technical Annex forms an integral part, applies to any party that activates, uses or relies on the Service, it being understood that, in dealings with the Customer, the provisions of the Agreement also apply.

2.1 Definition of the parties

Customer:
A natural or legal person who is a subscriber for the QERDS and who has the right to suspend or revoke it by means of the service purchase contract (**Agreement**) in return for a fee.

Subject:
A legal person as a subscriber, who must be identified as the QERDS Subject. The Subject is the formal sender (**Sender**) of all communications made whilst using the service. The Subject and the Customer may be the same person.

Subscriber/Authorised Representative:
The legal representative of the Subject or a person delegated by the Subject who will sign the request to activate the Service on behalf of the Subject.

User-Admin:
A user who accesses the GoNotice service using their QERDS credentials and is responsible for registering new users.

User-Sender:
A user who accesses the GoNotice service using their QERDS credentials and is responsible for sending certified communications via the GoNotice service on behalf of the Subject/Sender.

Recipient:
A natural person who receives the communication from the sender following identification.

3. Technical and Regulatory Specifications

3.1 Description and operation of the service

3.1.1 Operational nature of the service

The GoNotice Service is provided according to a 'Store and Notify' operational model, whereby the content of the communication is captured by the system, stored in secure environments and subsequently made available to the recipient via a notification containing the information necessary to access it.
In this model, the communication channels used by the Service serve solely to notify the recipient that the content is available, whilst the content of the communication is not transmitted via these channels but remains managed within the Service's infrastructure.

The Service manages the communication lifecycle through the following main operational stages:

- receipt of the content and verification of the transmission parameters;
- secure storage of the content and any attachments;
- sending the notification to the recipient via one or more selected channels;
- controlled access to the content by the recipient, subject to identification;
- recording and tracking of relevant events in the process;
- generation and association of digital evidence relating to the operations carried out.

The Service's operating procedures therefore include the centralised management of content, the tracking of process events and the production of the relevant records.

3.1.2 Scope of the service and methods of delivery

The Service enables the Subject, through authorised Users, to create, send and monitor electronic communications, including any attachments, intended for one or more recipients, whilst generating digital records to document the stages of the transmission and access process.
The content of the communication is handled by the Service and stored in a restricted and secure area, without being transmitted directly to the recipients via the notification channels. To this end, the Service generates a unique identifier (e.g. a dedicated URL) for each communication, which enables the recipient to access the content via the Service's infrastructure.
The recipient may access the content only after identification and authentication in accordance with the procedures laid down by the Service. The recipient may then view the content and any attachments, as well as interact with the communication within the limits of the enabled functions (such as, for example, accessing the content, opening attachments or, where applicable, giving explicit acceptance).
For the purposes of this Annex, delivery of the communication is deemed to have been completed at the moment the content is made available to the recipient via the Service, following the recipient's correct identification and their ability to access the content made available.

The Service enables the Data Controller to monitor the status of communications sent and the events associated with them, through tracking and reporting features that provide evidence relating to the main stages of the process.
The procedures for using the Service include:

- access via a web interface, for the manual management of communications;
- access via application programming interfaces (APIs), for integration with the subject's information systems and for the automation of sending and monitoring processes.

The Service can be configured by the subject in relation to the notification channels used, the recipient's access methods and the event tracking options, in accordance with the features made available.

3.1.3 Delivery process and generation of evidence

The Service manages the communication delivery process through a controlled sequence of events, tracked and recorded by the system, in order to ensure the production of digital evidence suitable for documenting the operations carried out and the outcomes of the process.
The delivery process comprises the following main stages:

- acceptance of the communication, with capture of the content and transmission parameters;
- acceptance or, where applicable, rejection of the request, based on the checks carried out by the system;
- preparation and dispatch of the notification to the recipient, containing the information required to access the communication;
- any interaction by the recipient, which may consist of accessing the notification, viewing the content and any attachments, as well as the explicit acceptance of the communication, where applicable;
- conclusion of the process, following the occurrence of the defined events or the expiry of the communication's availability period.

Each stage of the process generates one or more interconnected digital records, which objectively and verifiably document the activities carried out by the Service and the recipient's interactions. These records are associated with the communication and form an integral part of it for evidential purposes.
The records generated by the Service include, by way of example:

- receipt and acceptance of the communication;
- service on the recipient;
- access to the notification or the content;
- delivery of the content to the recipient;
- any explicit actions taken by the recipient (such as acceptance or rejection, where applicable).

The records are produced in accordance with the applicable ETSI standards and are made available in a structured and verifiable format, including through summary reports containing a summary of events and the relevant technical references.

For the purposes of the Service, the availability of the content to the recipient is guaranteed from the moment the notification is correctly sent and the content is made accessible via the Service's infrastructure. The duration of the content's availability and the methods of access are set out in the following paragraphs of this Annex.
The technical procedures for generating, structuring and validating the records, as well as the relevant format specifications, are described in further detail in the ICERT-QERDS-MO policy and practice statement.

Access to the Service is granted to users authorised by the subject via authentication mechanisms based on individual credentials.
The Service provides for the management of various user profiles, including:

- Admin User, with functions for configuring and managing user accounts;
- User–Sender, authorised to send communications.

The digital records generated as part of the Service, relating to communications and events in the delivery process, are retained by Tinexta Infocert for a period of not less than **20 (twenty) years**, in order to ensure their availability for verification, audit and the protection of the parties' rights.

In addition to the records of the delivery process, the Service records and retains **access logs**, as well as **sending and processing logs**, for a period of not less than **2 (two) years**, subject to any longer periods required by applicable legislation or necessary for security, audit or litigation purposes.

The records generated by the Service are associated with a **verifiable time stamp**, which allows the recorded events and operations carried out to be reliably dated.

The time reference used by the Service is consistent with the official time sources adopted by the provider and with the applicable regulatory requirements, and is applied to relevant events in the delivery process, including those relating to sending, notification and the recipient's access to the content.

3.1.4 Methods of access to and use of the Service

Access to the Service is permitted exclusively to Users authorised by the Data Controller, in accordance with the roles and authorisation levels defined within the Service.
The Service can be accessed in the following ways:

- a web interface, which allows Users to manually create, configure, send and monitor communications;
- application programming interfaces (APIs), which enable the Service to be integrated into the subject's information systems and allow for the automation of processes relating to the sending and management of communications.

Access to the Service is granted through User authentication using appropriate credentials and security mechanisms, in accordance with the procedures set out by the Service.

Users operate within the scope of the functions assigned to them, including, by way of example:

- configuration of communications and the relevant sending parameters;
- management of recipient lists;
- sending of communications;
- checking the status of communications and associated records.

The Data Controller is responsible for managing user accounts and the associated authorisation levels, as well as for the use of the Service by authorised Users.

3.1.5 Access to content by the Recipient

Following the sending of the communication, the Recipient receives a notification via one of the selected channels, containing the information necessary to access the content made available by the Service.
Access to the content takes place exclusively via the Service's infrastructure, using the unique identifier associated with the communication and subject to completion of the required identification and authentication procedures.
Depending on the Service's configuration (ERDS or QERDS), access to the content may require the use of enhanced authentication mechanisms, such as, for example:

- authentication via digital identity systems, possibly at a high level;
- the use of one-time passwords (OTPs) or other verification factors.

Once authenticated, the recipient may:

- view the content of the communication;
- access any attachments;
- carry out any actions provided for by the Service (such as, where configured, accepting or rejecting the communication).

The content of the message is made available to the recipient for the period specified by the sender, starting from the time the delivery confirmation is received. Once the pre-set period has elapsed, the content will no longer be accessible via the platform.

3.2 How to use the Service

3.2.1 Activation of the Service

In order to activate the Service, the subscriber must complete a form requesting activation of the Service (**Activation Request**), which will constitute acceptance of the General Terms and Conditions, this Technical Annex and the Privacy Policy, collectively referred to as **the "Contract"**.

For the purposes of activation, the Data Controller, through the subscriber/Data Processor, shall provide the information necessary for the identification and configuration of the Service, including details relating to authorised users and the required usage parameters.

Tinexta Infocert shall verify the information received and, if the outcome is positive, shall proceed with:

- the configuration of the environment dedicated to the subject (tenant);
- enabling the Data Subject (Sender) and the Admin User;
- setting up the procedures for accessing the Service, including authentication and authorisation features.

In the case of use via application programming interfaces (APIs), activation also includes the provision of the credentials necessary for integrating the Service into the subject's systems, in accordance with the prescribed procedures.

The Service is deemed to be active from the date of notification of activation by Tinexta Infocert or from the moment the subject is able to access and use the Service.

3.2.2 Methods of implementation and integration of the Service

The Service is provided via the cloud and may be used by the subject in various ways, depending on their operational and organisational requirements.
In particular, the Service can be accessed:

- via **a web interface**, without the need for integration with external systems, for the manual management of communications;
- via **application integration (API)**, which enables the subject to incorporate the Service's functionalities into their own information systems and automate the processes of sending, monitoring and managing communications.

In the case of integration via API, the Data Controller is responsible for the correct technical implementation of the interfaces, as well as for managing the application flows that interact with the Service, including the security of its own systems and access credentials.
Any advanced configuration, customisation or complex integration activities may require specific technical interventions and vary in duration; these remain the responsibility of the Data Controller or are to be agreed between the Parties within the framework of the Agreement.
The Data Controller remains responsible for the correct integration and use of the Service, without prejudice to the provisions regarding the obligations and liabilities of the Parties.

3.2.3 Duration of the Service

Unless otherwise provided for in the contract, the Service is provided for the duration specified in the Agreement, commencing on the activation date, and is renewable in accordance with the terms set out therein.
During the term of the contractual relationship, the Data Subject may use the Service within the limits of the functionalities made available and in accordance with the technical and operational conditions set out therein.

The Service is subject to specific **operational and usage limits**, which may relate, by way of example, to:

- the maximum size of content that can be transmitted;
- the maximum number of communications that can be handled within a given time period;
- the procedures for using the application interfaces and available features.

These limits are defined to ensure the proper functioning of the Service, the security of the infrastructure and the overall quality of service provision, and are governed by the policy and practice statement.
It is understood that use of the Service beyond the aforementioned limits or in a manner inconsistent with the prescribed procedures may result in restrictions on the provision of the Service, as well as the application of the measures set out in the Agreement and the Contract.

Upon termination of the contractual relationship, for whatever reason, the subject loses the right to use the Service, the account is deactivated and the records are retained for 20 years.

3.2.4 Availability of content and s of records

The content of communications is made available to the recipient for a specific period determined by the Service and the Data Controller's settings, during which it may be accessed following authentication; once this period has elapsed, the content may no longer be accessible, without prejudice to the validity of the records generated or the effects of delivery, even in the event of non-access.

The Service generates and retains digital records relating to the stages of the process (sending, notification, access and interactions), guaranteeing their integrity and authenticity and making them available to the subject in the form of reports (audit trails); these records may also be used by third parties to verify the transmission process, provided that they check their authenticity, integrity and suitability for the purpose, taking into account the limitations of the Service. They certify solely the recorded events and not the content or accuracy of the information transmitted, whilst the technical methods of generation and verification are set out in the Service's technical documentation.

3.3 Obligations and responsibilities

3.3.1 Obligations of the Data Controller and the Subscriber

The Data Controller and the subscriber undertake to use the Service in accordance with applicable legislation, the General Activation Conditions, this Technical Annex and the instructions provided by Tinexta Infocert, as well as in accordance with the provisions of the Agreement.
In particular, the subject undertakes to:

- use the Service exclusively for lawful purposes and in compliance with applicable regulatory provisions;
- ensure the accuracy, completeness and lawfulness of the content of communications sent via the Service;

- ensure that recipients are correctly identified and that there is an appropriate legal basis for sending the communications, and provide the relevant documentation upon request by the competent authority or Tinexta Infocert within the limits of the law;
- configure the Service in a manner consistent with their operational requirements and in accordance with the available functionalities;
- manage access credentials and authentication systems with due care, preventing unauthorised access.

The subscriber is responsible for the configuration and use of the Service within the context of its own processes and is required to monitor the correct use of the Service by users, having shared the accepted contractual terms with them.

3.3.2 Obligations of the Recipient

The Recipient, when interacting with the Service, undertakes to:

- use the channels for accessing content in accordance with the procedures laid down by the Service;
- correctly complete the identification and authentication procedures required to access communications;
- not to misuse the access tools made available (such as links, credentials, temporary codes or other authentication tools);
- not to transfer to third parties or allow unauthorised persons to use the access tools and credentials received

The Recipient is responsible for:

- the accuracy of the information provided for identification purposes;
- safeguarding the access tools received;
- for the use of the information contained in the communication once the content has been made available.

It is understood that failure to access the content or to interact with the communication within the specified time limits does not prevent the generation and validity of the Service's records, within the limits of applicable legislation.

3.3.3 Obligations of Tinexta Infocert

Tinexta Infocert undertakes to:

- provide the Service in accordance with applicable legislation and relevant technical standards;
- ensure the proper functioning of the components of the Service under its control;

- adopt appropriate technical and organisational measures to ensure the security, integrity and confidentiality of the data processed;
- generate, manage and retain electronic records relating to communications;
- make suitable tools available to the subject for checking the status of communications and associated records.

3.3.4 Limitations of liability

Without prejudice to the provisions of the General Activation Conditions, Tinexta Infocert shall not be liable:

- for the content of communications sent by the subject;
- for the accuracy, lawfulness or completeness of the information transmitted;
- for the recipient's failure to receive or view the notification for reasons not attributable to the Service (such as the unavailability of communication channels or failure to view the notification);
- for the improper use of the Service by the Subject, authorised users or the recipient;
- for malfunctions arising from systems or infrastructure not under its control.

The Service guarantees solely the correct management of the delivery process and the generation of the relevant records within the limits of the characteristics and procedures described in this Annex.

4. SLA and KPIs

In terms of service delivery, the monthly service availability figures are set out in detail in the relevant policy and practice statement.

1