tinexta infocert

# TECHNICAL ANNEX
## QWAC Certificates – Application to Application

Contents


***

## 1. EXTERNAL REFERENCES:

| Documentation | Detailed links |
|---|---|
| **Policy and Practice Statement** | https://qtsp.infocert.it/pdf/ICERT_INDI_MOWS-ENG.pdf |
| **PDS (PKI Disclosure Statement)** | https://qtsp.infocert.it/pdf/ICERT_INDI_PDSWS-ENG.pdf |
| **User Manual** | N/A |
| **API Documentation** | N/A |
| **Support links (FAQs, videos, guides)** | N/A |

## 2. Service Description – Introduction

Tinexta Infocert, for the purposes of this document, acts as a qualified trust service provider (hereinafter "QTSP") for the issuance of qualified certificates for the authentication of "Application to Application" websites (hereinafter the "Service"), in accordance with the provisions of the ICERT-INDI-MOWS policy and practice statement (hereinafter also referred to as the "CPS" or "PS") and the PKI Disclosure Statement (PDS).

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 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, 412-3, 412-4 and 412-5, and ETSI TS 119 495, 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 these services, 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.

Website authentication services enable parties establishing communication over a public network to verify the identity of the entity managing the domain and to establish a secure communication channel.

In the context of communications using the TLS (Transport Layer Security) protocol, this function is performed by certificates commonly known as SSL/TLS certificates, which enable:

- the server to authenticate itself to the client;
- the establishment of an encrypted channel;
- the integrity of the exchanged data to be guaranteed.

Certificates contain key information, including the domain name, the validity period, the public key and the digital signature of the Certification Authority that issued them. In traditional web environments, browsers automatically verify the validity of certificates and alert users to any anomalies or critical issues. Publicly recognised TLS certificates are issued by Certification Authorities in accordance with internationally agreed rules, in particular those defined by the CA/Browser Forum, and are used by browsers and applications to establish trust relationships in communications over public networks.
In the context of this document, the subject of the service consists of qualified website authentication certificates in the 'Application-to-Application' context (Qualified Website Authentication Certificates – QWAC), governed by the eIDAS Regulation (EU) No 910/2014 and subsequent amendments and additions. These certificates are intended for application contexts and are not recognised by the main web browsers and their public trust stores, as they are used solely for the authentication and security of communications between systems.
These certificates represent a specific type of TLS certificate which, in addition to guaranteeing the technical functions of authentication and encryption, attest to the identity of the subject of the certificate on the basis of a qualified verification process carried out by a qualified trust service provider (QTSP) and are therefore subject to more stringent regulatory and compliance requirements than non-qualified TLS certificates.
This Technical Annex forms an integral and substantial part of the service purchase agreement (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 who 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 has entered into a contract (Agreement) for the purchase of the services in return for a fee. The Customer may be the same as the subscriber.

**Subject**
This is the system or website for which the subscriber is requesting the certificate.

**Subscriber**:
A legal entity that is a subscriber to Tinexta Infocert and requests the issuance of a certificate for a Subject. The Subscriber is the natural person with the necessary powers of representation or authorisation to act in the name and on behalf of the legal entity requesting the certificate;

**User/Relying party:**
This is the organisation, system or application that verifies the Subject's digital certificate and relies on the validity of that certificate to establish secure and authenticated communication with the system or website.

tinexta
infocert

# 3. Technical and regulatory specifications

## 3.1 Issuance and use of the service

The service provides for the issue and use of qualified certificates for website authentication (Qualified Website Authentication Certificates – QWAC), as well as the management of their lifecycle.
The certificate is issued following a request from the subscriber, by signing the Activation Request, submitted in accordance with the procedures laid down by Tinexta Infocert, and by submitting the public key certification request (Certificate Signing Request – CSR), containing the identifiers (domains) of the system for which certification is requested.
Following the required checks and a positive outcome, Tinexta Infocert generates the certificate and makes it available to the subscriber.
The service also includes certificate management activities for any revocation, in accordance with the provisions of this document. All information relating to the issue and lifecycle of the certificate is retained for at least 20 years from the certificate's expiry date

### 3.1.1 Certificate and cryptographic keys

A digital certificate is an electronic document, signed by Tinexta Infocert, which certifies the association between the Subject – understood as a system or website – and the corresponding pair of cryptographic keys (public and private), used for the authentication and protection of communications.
The keys are generated and managed under the control and responsibility of the subscriber.
By issuing the certificate, the QTSP guarantees the correct association of the public key with the Subject, in accordance with the applicable regulations and the policy and practice statement.

### 3.1.2 Identity verification process

The issue of the certificate is subject to verification of the identity of the subscriber, whether a natural or legal person, as well as their relevant powers in relation to the Subject.
Identification and verification activities are carried out by Tinexta Infocert through specifically delegated personnel, on the basis of the documentation provided by the subscriber and through checks carried out on official sources, public registers and databases deemed reliable, in order to verify the declared identity and the existence of powers of representation.
The operational procedures for identification and verification are set out in the ICERT-INDI-MO policy and practice statement.
The necessary checks are also carried out to verify control of the application system and the associated domains for which the certificate is requested. In the case of QWAC PSD2 certificates, the additional specific attributes required by the applicable legislation are also verified.

### 3.1.3 Process for using and verifying the certificate

The certificate is used by the system or application for which it was issued in the context of network communications, in order to enable other systems with which it interacts to verify its identity.
In communications between applications, the system providing the service presents its certificate to the calling system. The latter uses the certificate to verify its validity, origin and status, ensuring that it has been issued by Tinexta Infocert and that it has not expired or been revoked.
In the case of communications secured using the mTLS (Mutual Transport Layer Security) protocol, the calling system also presents its own certificate to the system providing the service, enabling mutual authentication between the parties. Both systems therefore carry out checks on the validity, origin and status of the certificate presented by the other party, in order to verify its reliability and its association with the relevant entity.
A successful outcome of these checks enables the systems involved to mutually confirm the identity of the other party and to establish a secure and authenticated communication between the application

systems.

3.1.4 Validity period and renewal

The certificate is issued with a limited validity period, as specified within the certificate itself.
Tinexta Infocert does not provide for the renewal of the certificate whilst retaining the same public key. Upon expiry, the certificate may be replaced by a new issue, following the generation of a new pair of cryptographic keys and the submission of a new certificate signing request (CSR) for the public key.
The new certificate retains the information relating to the Subject, subject to any updates, and may differ in terms of validity period, identifiers and any other information.

3.1.5 Revocation

Revocation entails the termination of the certificate's validity before its natural expiry date.
Revoked certificates are included in specific revocation lists (CRLs) published by the Certification Authority, and are also made available via online certificate status verification services (OCSP).
Revocation may be requested by the subscriber or ordered by Tinexta Infocert in the cases set out in the policy and practice statement, including, by way of example, the compromise of the private key, inaccuracies in the information contained in the certificate, or the Subject's failure to meet the requirements. Suspension is not provided for certificates issued under this service.

## 3.2 Products and Services

As part of this service, Tinexta Infocert issues qualified certificates for website authentication (Qualified Website Authentication Certificates – QWAC), intended for use in 'Application-to-Application' (A2A) contexts, for the identification of systems and services exposed on the network.
The certificates are issued following validation of the domain and the organisation that controls it, and attest to the association between the Subject – understood as a system or website – and its technical identifiers, such as domain names.
In particular, Tinexta Infocert issues the following types of certificates:

- **QWAC certificates for A2A applications**
  Qualified certificates used for the authentication of systems or websites in the context of network communications.
- **QWAC PSD2 / Open Banking certificates**
  Qualified certificates used within the context of payment services and open banking ecosystems, which include the specific attributes of the payment service provider as required by the applicable legislation.

The certificates are issued in accordance with the aforementioned profiles, identified by specific Object Identifiers (OIDs), which determine their characteristics, including their period of validity. In particular, both types of certificate may have a validity period of up to one year, whilst, in the specific cases provided for PSD2 or open banking services, this may be up to two years.
The technical characteristics of the certificates, including the relevant OIDs, certificate profiles and any qualified attributes, are defined in the ICERT-INDI-MOWS policy and practice statement, to which reference should be made.

## 3.3 Obligations and Responsibilities

### 3.3.1 Obligations of the Subscriber

In addition to the provisions set out in the General Activation Condition (and in the Agreement, where the Customer and the subscriber are the same person), the subscriber is required to:

- to ensure the safekeeping and confidentiality of the Certificate keys and to take all appropriate

organisational and technical measures to prevent harm to third parties.

- to exercise the utmost care in the specification, use, storage and protection of authentication tools, including the private key. The subscriber is also required to ensure that its hardware and software systems comply with the security measures laid down by current legislation. More generally, the subscriber guarantees the security and reliability of the system on which the Certificates are used.
- Before installing the Certificates on their server, to verify the accuracy of the Certificates and all the data contained therein.
- to notify Tinexta Infocert immediately and in writing of any circumstance that might reasonably and prudently give rise to suspicion of a compromise (for example: theft, loss, damage, etc.) of the private key or the Certificates.
- to refrain from using the Certificates or the relevant key in any way after their expiry or revocation,

The subscriber undertakes not to use the Service and the Certificates in connection with domains, systems or applications that involve breaches of the law or the rights of third parties, or that may cause harm to third parties, including, by way of example, cases of unlawful use of IT resources, the dissemination of harmful content or activities contrary to applicable legislation.

The subscriber further undertakes not to use the Service and the Certificates for fraudulent or deceptive purposes, including, by way of example, phishing, the distribution of malware, identity theft, etc.

It is prohibited to use the certificate outside the limits and contexts specified in the policy and practice statement and in the supply contracts, and in any event in breach of any usage limits or additional attributes that may be required (key usage, extended key usage, user notice, etc.) as indicated in the certificate.

The subscriber undertakes to request the revocation of the Certificate without delay should the information contained therein no longer be accurate, complete or up to date.

### 3.3.2 Responsibilities of the Subscriber

In addition to the provisions set out in the General Activation Condition (and in the Agreement, where the Customer and the subscriber are the same person), the subscriber is responsible for the accuracy of the data provided for the purposes of issuing the certificate

Should the subscriber, at the time of identification, have concealed their true identity – including through the use of false personal documents – or falsely claimed to be another person, or have acted fraudulently or negligently in such a way as to compromise the identification process and the related findings set out in the Certificate, they shall be held liable for all damages suffered by the Certifier and/or third parties arising from the inaccuracy of the information contained in the Certificate, and shall be obliged to indemnify and hold the Certifier harmless from any claims for damages.

The subscriber is obliged to indemnify, hold harmless and compensate Tinexta Infocert for all damages it may suffer as a direct or indirect consequence of the breach – even partial – of the obligations incumbent upon the subscriber under the General Activation Conditions (and/or in the Agreement, where applicable) and this Technical Annex, as well as any sums that Tinexta Infocert is required to pay to third parties, or to pay by way of an administrative or financial penalty, as a result of the aforementioned breach.

The subscriber is also obliged to indemnify and hold Tinexta Infocert harmless from any liability relating to the use of the Certificates themselves and in the event of complaints, legal proceedings, administrative or judicial actions, losses or damages (including legal costs and fees) arising from the subscriber's unlawful use of the Service.

The Certificates may not under any circumstances be assigned or transferred by the subscriber to third parties (not even following the sale or lease of a business) without the prior written consent of Tinexta Infocert. Furthermore, they may not be transferred or exported to countries outside Italy in breach of the laws or regulations of other jurisdictions.

Once the Certificate has expired or been revoked, or in any case where its use is no longer lawfully authorised, the subscriber is obliged to cease using it immediately and to permanently remove the Certificate from the servers in use.

### 3.3.3 Obligations and responsibilities of the Certification Authority

Tinexta Infocert, in its capacity as a Certification Authority, operates in compliance with applicable legislation, relevant technical standards and the ICERT-INDI-MOWS policy and practice statement.

In particular, Tinexta Infocert shall:

- verify the information provided by the subscriber in accordance with the prescribed procedures, including validation of the domain and the organisation that controls it;
- ensure the correct association between the public key and the Subject, as well as the certificate's compliance with applicable regulatory and technical requirements;
- manage the certificate lifecycle, including the issuance, revocation and publication of status via the relevant services (CRL and OCSP);
- retain, in accordance with the procedures set out in the policy and practice statement, the certificates issued and information relating to lifecycle events, including service logs.

Tinexta Infocert assumes no further obligations beyond those set out in the General Activation Conditions (and/or the Agreement, where applicable), this Technical Annex, the Policy and Practice Statement, and the legislation in force governing trust services.

In particular, Tinexta Infocert accepts no liability in relation to:

- the management, configuration and security of the systems, infrastructure and software used by the subscriber or by third parties;
- the use of the certificate in a manner that does not comply with the intended purposes or the limits of use specified in the certificate itself, in the policy and practice statement or in the applicable legislation;
- compromise of the private key attributable to the subscriber or, in any event, to third parties;
- the malfunction or unavailability of communication networks, IT systems or infrastructure not directly controlled by the Certification Authority.

Tinexta Infocert also assumes no obligation to monitor the content, services or applications made available via the certificate holder.

Without prejudice to the provisions of applicable legislation and except in cases of wilful misconduct or negligence where provided for, the Certification Authority's liability is limited to the cases and within the limits set out in the policy and practice statement and in this document.

## 4. SLA and KPIs

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