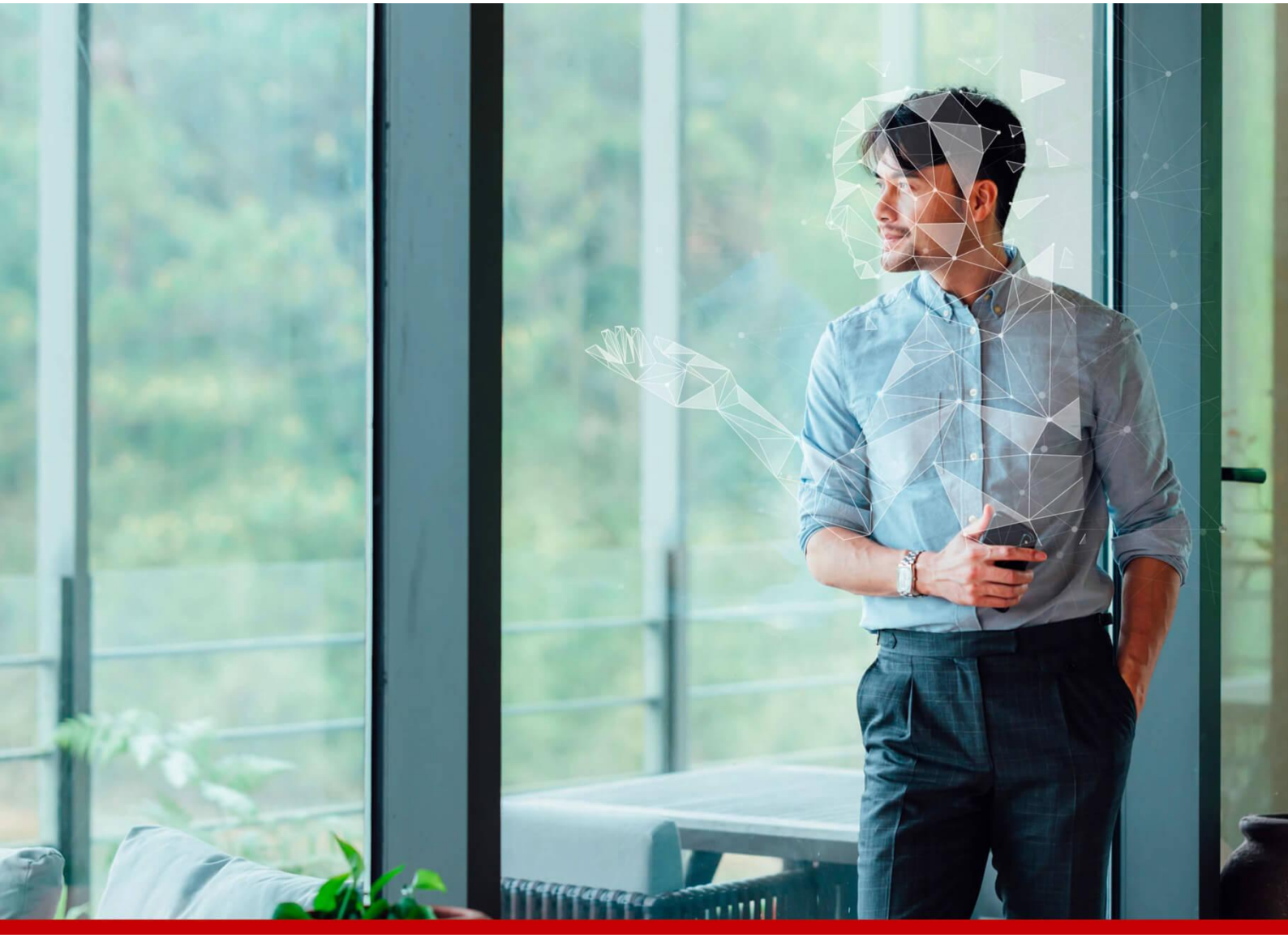


TSA Disclosure Statement

POLICY FOR ELECTRONIC TIMESTAMPING SERVICE

RELEASE 1.0 – 19/03/2026

INDEX

GENERAL INFORMATION **2**

Document Information 2

Version Control 2

1. Disclosure statement **3**

1.1. Introduction 3

1.2. Document name and identification 3

1.3. Contact Information 3

1.3.1. Organization 3

1.3.2. TSU issuing 4

1.3.3. Contact for service deactivation procedures 4

1.4. Electronic time-stamp types and usage 4

1.4.1. Time stamping content 5

1.4.2. Certificates validation 5

1.4.3. Users 5

1.4.4. Issuing authority 5

1.4.5. Users and applicability 6

1.5. Limitations and restrictions on certificate usage 6

1.5.1. Time accuracy 6

1.6. Subscribers obligations 6

1.7. Relying Parties verification obligations 7

1.7.1. Relying parties obligations 7

1.7.2. Verification requirement of the electronic signature corresponding to the qualified electronic timestamping 7

1.7.3. Verification effect 7

1.7.4. Proper use and prohibited activities 8

1.8. Bit4id obligations 8

1.9. Guarranty and limitations of liability 8

1.9.1. Bit4id S.r.l. guarantees for timestamping services 8
1.9.2. Guarantee exclusion 9
2. APPLICABLE AGREEMENTS 10
2.1. Applicable agreements 10
2.2. Certification Practice Statement (CPS) 10
2.3. Privacy Policy 10
2.4. Refund policy 11
2.5. Applicable law and jurisdiction 11
2.6. List of active trust service provider and audit 11
2.7. Final provisions, full agreement and notifications 11

GENERAL INFORMATION

Document Information

Security Classification:	Public
Organization:	Bit4id S.r.l.
Version:	1.0
Last Edition Date:	19/03/2026
Document code:	TSA_Disclosure_Statement_v.1.0_EN

Version Control

Version	Modified parts	Changelog	Date
1.0	Original	File Creation	19/03/2026

1. Disclosure statement

1.1. Introduction

The present TSA Disclosure Statement (hereinafter also referred to as "*Statement*" or "*Policy*"), constitutes an integral part of the contractual terms and conditions of Bit4id S.r.l. (hereinafter "Bit4id"), which operates as a Qualified Trust Service Provider regarding the TSA operations described herein.

The information, prepared in accordance with Annex B of the ETSI EN 319 421 standard, contains essential information to be known in relation to Bit4id's timestamping service.

The qualified timestamping service operates in accordance with RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), and with the ETSI EN 319 421 and ETSI EN 319 422 standards.

For all terms and definitions used within this document, reference can be made to Bit4id's CPS (*Certification Practice Statement*) available at the following address https://www.bit4id.com/documentazione-qtsp or to the definitions provided by the applicable regulations.

1.2. Document name and identification

This document is updated to the version resulting from the "*Version Control*" or "*Documentary Check*" referred to in the "*General Information*" of this Statement.

Bit4id ensures constant verification and constant updating of the document that takes into account any subsequent regulatory updates.

Furthermore, Bit4id undertakes to make this document known and available to interested parties by publishing it on its website where it is always possible to consult the latest approved version.

1.3. Contact Information

1.3.1. Organization

Below are the company data of Bit4id S.r.l. and related contacts:

BIT4ID S.R.L.

Registered office: Via Diocleziano n. 107, 80125 - Napoli

VAT Number (IT): 04741241212

Phone: +39 081 7625600

E-mail: info@bit4id.com

PEC: bit4id-tsp@sicurezzapostale.it

Web Site: https://www.bit4id.com

1.3.2. TSU issuing

The time stamps described in this document are issued by Bit4id S.r.l., as mentioned previously (v.1.3.1. *infra*).

1.3.3. Contact for service deactivation procedures

As a qualified trust service that is not directly linked to the identity of an individual user, the revocation of electronic timestamping certificates falls under the exclusive responsibility of the QTSP, which shall proceed with revocation in the event of a compromise of the key or of the system.

The user may request the deactivation of their service access credentials to prevent unauthorized use, by contacting Bit4id through a communication sent via PEC to the Certifier's address (§1.3.1).

1.4. Electronic time-stamp types and usage

The qualified timestamping service follows the guidelines of the PDS of the TSU Certificate with the following OID:

OID	**Certificate type**
	Time Stamping Service
1.3.6.1.4.1.31898.10.2.1.2.2	Time Stamping Unit certificate (3072 bit)
1.3.6.1.4.1.31898.10.2.2.2.2	Time Stamping Unit certificate (ECC secpt256)

The service provided by Bit4id is compliant with the Best Practices Policy for TimeStamp (BTSP) defined by ETSI 319 421, identified by the OID 0.4.0.2023.1.1.

	OID
itu-t (0) identified-organization (4) etsi (0) time-stamp-policy (2023)	**0.4.0.2023.1.1.**

policy-identifiers (1) baseline-ts-policy (1)	

The electronic timestamping declared as qualified comply with the statements in the Regulation UE 910/2014 (eIDAS) and the TSU certificate is issued according to the ETSI EN 319 422.
Customers receiving this electronic timestamping service must comply with the current legislation and comply with the signed contracts with this Authority, to verify the timestamp signature validity and the validity of the TSU certificate.

1.4.1. Time stamping content

Each time stamp issued by Bit4id contains all the information required by the current regulation, such as:

1. Time stamp serial number;
2. Time stamp signature algorithm;
3. The identifier of the certificate relative to the public key of the TSU;
4. The date and time of the time stamp;
5. The accuracy of the time source compared to UTC (the maximum permitted deviation is one second);
6. The identifier regarding the hash algorithm used to generate the evidence.;
7. The value of the footprint regarding electronic evidence.

1.4.2. Certificates validation

The validation of the state of the certificates is carried out from:

- Access to the OCSP: http://ocsp.bit4idtsp.com
- Download of the CRL:
    - For 3072-bit certificates: http://crl.bit4idtsp.com/tsa-rsa-4096-g1.crl
    - For Elliptic curve certificates: http://crl.bit4idtsp.com/tsa-ecc-256-g1.crl

1.4.3. Users

The Service User is the natural or legal person who, by signing a dedicated contract with Bit4id, has requested and activated an electronic timestamping service.

1.4.4. Issuing authority

The electronic timestamping services are issued by Bit4id.

1.4.5. Users and applicability

The users of the service are the Subscribers (natural or legal persons) who have requested and subscribed to the services offered by Bit4id.

The electronic timestamping service provided by Bit4id's TSA is a qualified trust service in compliance with the indications of the National Supervisory Authority (AgID) and in accordance with current regulations.

1.5. Limitations and restrictions on certificate usage

The use of electronic timestamping services is restricted to customers (natural or legal persons) who have signed a specific agreement with Bit4id for the provision of such services.

Any use other than that specified in the CPS is prohibited.

Certificates issued by Bit4id may not be used in violation of any rights, laws, or regulations.

The purpose of the service is to allow users to demonstrate the existence of an electronic document at a certain date and time through the application of a timestamp to the document.

1.5.1. Time accuracy

The Qualified Timestamping service of Bit4id is based on the use of TSP protocols on HTTP, defined in the regulation RFC 3161 '*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*'.

Bit4id has a trustworthy source of time that allows a level of trust of STRATUM 1, via NTP.

The accuracy of the Qualified Timestamping of Bit4id with respect to UTC is a second.

1.6. Subscribers obligations

The subscriber undertakes to:

- carry out the electronic timestamps requests accordingly to the procedure and the tools provided by Bit4id, in accordance to what is stated in the CPS;
- follow the specific instructions on the TSA Disclosure Statement of Bit4id;
- verify the electronic signatures of the electronic timestamping, including the validity of the used certificate;
- use the electronic timestamping within the limits described in this Policy and in the CPS.

1.7. Relying Parties verification obligations

1.7.1. Relying parties obligations

All those who rely on the information contained in the certificates (R.P., abbreviation for Relying Parties). In accordance with requirement_OVE-6.6-01 of the ETSI EN 319 421 standard, are required to:

- verify that the timestamp has been correctly signed and that the private key used to sign the timestamp has not been compromised up to the time of verification;
- verify the validity status of the certificate, namely whether it has been revoked, by using the current revocation status information.

  The validation must be performed taking into account the status of the certificate at the date and time relevant to the R.P., according to the specific context (e.g., the current date and time, the date and time of signature in cases where this can be demonstrated through a timestamp applied to the document);
- consider any limitations on the use of the certificate;
- take any precautions as prescribed in the agreements or elsewhere.

1.7.2. Verification requirement of the electronic signature corresponding to the qualified electronic timestamping

The verification can be carried out automatically through the verification software provided by Bit4id, accessible at the following address: https://vol.bit4idtsp.com/en, which allows for the verification of timestamps applied to a digitally signed or unsigned document.
The characteristics and the related procedure for using this application are described in Annex A of the Bit4id CPS.

1.7.3. Verification effect

Under the correct verification of the electronic timestamping certificates of compliance with this disclosure text (PDS), the relying parties can trust the provided information.

1.7.4. Proper use and prohibited activities

Relying Parties agree about not using any type of status information of qualified electronic timestamping or any other type that has been supplied by Bit4id, in performing a prohibited transaction by the applicable law of that transaction.

Relying parties will not inspect, interfere or perform any reverse engineering of the technical implementation of public services for electronic timestamping or certification of Bit4id without prior written consent.

The qualified electronic timestamping services provided by Bit4id are not designed for use in unauthorized dangerous situations (that require fail-safe actions), such as nuclear facilities operations, navigation systems, air communications or weapon control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

1.8. Bit4id obligations

Regarding the provision of the qualified electronic timestamping service, Bit4id undertakes:

a) issue, deliver and manage qualified seals, according to the instructions provided by the subscriber, in the cases and for the reasons described in Bit4id CPS at the following link: https://www.bit4id.com/documentazione-qtsp;

b) perform the services with technical media and suitable materials, and with personnel that meet the qualification conditions and experience established in the CPS;

c) comply the quality service levels, in accordance with what is established in the CPS, in the technical, operational and security aspects.

1.9. Guarranty and limitations of liability

1.9.1. Bit4id S.r.l. guarantees for timestamping services

Bit4id guarantees to the Subscribers that the timestamping complies with the requirements established in the Certification Practice Statement (CPS).

Bit4id guarantees that the information within the timestamp is correct.

1.9.2. Guarantee exclusion

Apart from the cases expressly mentioned in this document and in the Operational Manual / CPS of Bit4id, the latter cannot be held liable, in any capacity, towards users, for direct or indirect damages that may arise from them.

2. APPLICABLE AGREEMENTS

2.1. Applicable agreements

Applicable agreements to qualified electronic timestamping are the followings:

- General terms and conditions for digital certification services governing the relationship between Bit4id and the Subscriber/Service User of the certificates available at the following link: https://www.bit4id.com/documentazione-qtsp;
- General conditions of service and Policy included in this document;
- CPS which regulates the provision of certification services (v. par. 2.2. infra);
- any additional Forms and / or contractual documentation expressly referred to in the above documents.

2.2. Certification Practice Statement (CPS)

Bit4id certification services are technically an operationally regulated by the CPS of Bit4id, for its subsequent updates, as well as the additional documents.

The CPS and the operations documentation are changed periodically in the Registry and can be consulted on the website: https://www.bit4id.com/documentazione-qtsp.

2.3. Privacy Policy

Bit4id, with reference to the processing of personal data, complies with current legislation, both national and community, with particular reference to Legislative Decree 196/03, as amended, and Regulation (EU) 2016/679 (hereinafter also referred to as "*GDPR*").

Bit4id cannot disclose or be obliged to disclose confidential information unless a specific request comes from:

a) the person with whom Bit4id has an obligation to keep the information confidential, or
b) a judicial, administrative or any other mandate provided for by current legislation.

Bit4id, in accordance with the provisions of art. 13 of the GDPR, has prepared and adopted a precise Privacy Policy relating to the Processing of Personal Data which describes the treatments carried out by Bit4id, as Data Controller, in relation to the provision of trust services.

The extended Privacy Notice is available for consultation at any time on Bit4id's website at the following address: https://www.bit4id.com/documentazione-qtsp.

2.4. Refund policy

For the refund policy, reference must be made to Bit4id's General Terms of Service, provided at the time of the service request and published on the website https://www.bit4id.com/documentazione-qtsp.

2.5. Applicable law and jurisdiction

Relations with Bit4id are governed exclusively by Italian law.

In the event of disagreement between the parties, they will attempt amicable settlement. To this end, the parties must send a communication to Bit4id through one of the contacts indicated in this document.

For the competent court, reference is made to the Bit4id CPS which here is to be understood as fully referred to and transcribed.

2.6. List of active trust service provider and audit

Below is the link through which it is possible to consult the list of active trust service providers in Italy: https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia

Bit4id, as a Qualified Trust Service Provider (QTSP), is subject to the supervisory activities of the National Supervisory Authority (AgID), pursuant to Article 17 of the eIDAS Regulation.

Bit4id's qualified services, including the TSA, are subject to annual audits conducted by an accredited Conformity Assessment Body (CAB).

The CAB verifies full compliance with technical, organizational, and security requirements, without any relationship with Bit4id that could compromise the impartiality of the inspection activity.

The audit results are transmitted to AgID

2.7. Final provisions, full agreement and notifications

The clauses of this disclosure text are independent of each other, that's why, if any clause is held invalid or unenforceable, the remaining clauses and, the clauses of CPS will still be applicable.

This text contains the full will and all agreements between the parties.

The parties mutually notify the facts by sending an e-mail to the address indicated by the Service User of the contract with Bit4id.