eurosign

Signature Policy

Version 1.0 - 20.10.2020

VERSION	DATE	DESCRIPTION	AUTHORS	COMPANY
V. 1.0	20.10.2020	Creation of document	Emmanuel MATHIEU	Eurosign

DOCUMENT STATUS - CLASSIFICATION	REFERENCE
Public distribution	1.3.6.4.1.55276.1.1.1.0

Summary

1. Context and objectives

The EUROSIGN company provides its customers with an electronic signature service that allows anyone who subscribes to the service to electronically sign documents (e.g. contracts, ...) remotely.

This document constitutes the EUROSIGN Signature Policy applicable to documents signed on the EUROSIGN signature service.

The level of signature used in the context of this Signature Policy is as follows "standard" within the meaning of the definition of "electronic signature" stipulated in Article 3 of the European Regulation on electronic identification and trust services for electronic transactions within the internal market and repealing Directive 1999/93/EC (also known as the eIDAS Regulation).

The purpose of the EUROSIGN Signature Policy is to describe:

- The conditions under which these electronic signatures are made, processed, and stored,
- The conditions and the context in which these electronic signatures will be subsequently consultable, usable, verifiable.

This document is intended for:

- Signatories of the documents,
- Recipients and subsequent readers of these signed documents, who will necessarily need to be aware of the conditions under which these electronic signatures will have been made.

2. Signature Policy

2.1 Scope of application

The present Signature Policy applies to electronic transactions produced within the EUROSIGN electronic signature service and does not make any distinction on the context of the signature whether it is performed face-to-face or remotely.

2.2 Identification

This Signature Policy is identified by the OID 1.3.6.1.4.1.55276.1.1.1.0.

This reference, as well as the version number of the Signature Policy used, must be included in the signed data, in order to certify the regime under which each of the signatories produced their electronic signature.

In any subsequent communication, to reference this Signature Policy, the OID will be used together with the fingerprint of this document and the mention of the algorithm used to produce this fingerprint.

2.3 Publication of the document

Before any official publication, the Signature Policy is validated by the EUROSIGN Approval Committee.
This Signature Policy is:

- Available on the signature service and accessible by the signatory at the time of the electronic signature,
- And published on the following URL : https://www.eurosign.com/en/docs/certifications-eurosign/

2.4 Update process

2.4.1 Circumstances making an update necessary

Updating a Signature Policy is a procedure that involves all stakeholders and is subject to a rigorous approach. It is essentially initiated to make major changes, to take into account new needs, new stakeholders, improve the legal framework or fill in gaps.

This policy is reviewed when any major modification is made to the application.

2.4.2 Taking into account the updates

All remarks or requests for information on this Signature Policy should be sent by e-mail to the following address: certification@eurosign.com

These remarks and requests for information are examined by the Approval Committee, which initiates, if necessary, the process of updating this Signature Policy.

An electronic signature is always valid under the Signature Policy that applied at the time of the electronic signature. All versions of the Signature Policies and their respective duration of validity are therefore kept by EUROSIGN and available upon request

2.4.3 Information for stakeholders

When an update has been planned, the information related to this evolution is put online at the publication places specified in chapter 2.3. Regardless of this mode of communication, the stakeholders (see definition in chapter 3.1) can at any time ask EUROSIGN, at the contact point specified in chapter 2.4.2, for more information.

The publication of a new version of the Signature Policy consists of archiving the previous version and putting the following elements online in the directory provided for this purpose:

- Document in PDF format,
- OID of the document,
- Fingerprint of the document,
- Hash algorithm used (SHA-256 condensate for this version),
- Technical signature of the document,
- Signature algorithm used (SHA256WithRSAEncryption algorithm for this version),
- Exact date and time of entry into force.

2.5 Coming into force of the new version and validity period

When a new version of the Signature Policy is put online, it is systematically presented and made available to signatories during electronic transactions following publication.

The exact date and time of the coming into force of the new Signature Policy are specified on the publication site.

The new version of the Signature Policy comes into force as soon as it is published at the place of publication identified in chapter 2.3 and remains valid until a new version is published.

3. Actors and roles

3.1 The actors

3.1.1 Signatories

The signatories of the documents are natural persons who are customers of EUROSIGN's electronic signature service, having the authorization of the entity they represent if necessary to sign documents.

The customer has two levels of identification before starting the signature process:

- **Level 1 identification:** the identity of the signatory is checked on the basis of declarative information.
- **Level 2 identification:** the identity of the signatory is checked on the basis of declarative information and the provision of proof of identity document (national identity card, passport, residence permit).

As part of this Signature Policy, no electronic signature certificate is issued to the signatory.

3.1.2 Eurosign

EUROSIGN develops and operates the signature service used by the signatories.

EUROSIGN and its subcontractors realize, host, and maintain the signature service made available to signatories.

In addition, EUROSIGN:

- Has a seal certificate enabling it to perform a technical seal of documents by affixing an electronic seal for any "standard" electronic signature made by a signatory. This electronic seal protects the integrity of the signed document.
- Uses this seal certificate at the end of each transaction (when all signatories have signed) to make a final seal which is time-stamped to date the document and enable the signatory or a third party to verify the quality of the electronic signature a posteriori.
- Keeps the signed electronic document in secure conditions to guarantee its confidentiality and integrity over time.

3.1.3 Recipient

Recipients of electronically signed documents are the customers themselves, who retain these documents, whose electronic signature evidences their consent to the content of the documents.

3.2 Roles and obligations of the signatory

3.2.1 Signatory’s environment

The signature creation operation must be carried out on a computer equipment (computer, tablet, smartphone) connected to the Internet network.

The signature process does not depend on the client's equipment, therefore, no tools related to signature operations need to be installed on the signatories' computer equipment.

However, the signatory must ensure that this equipment is protected, in particular against fraudulent use of his identity.

It is therefore necessary to protect physical and technical access to this station and the confidential information contained therein.

3.2.2 Signature tool used

Customers need to check the data they are going to sign before putting their electronic signature on it. For this purpose, they use the signature service provided by EUROSIGN and whose various steps of the signature process lead them to:

- Check the elements of the document to be signed,
- Accept the Terms of Use of the service,
- Explicitly accept the signature operation.

3.2.3 Type of certificate used

No electronic certificate is issued to the signatory to perform the signature operation.

The electronic signature performed by the signatory is of "standard" level within the meaning of the definition of "electronic signature" stipulated in Article 3 of the eIDAS Regulation.

However, an electronic seal is carried out by EUROSIGN for any "standard" electronic signature made by a signatory and thus guarantees the integrity of the document.

3.2.4 Certificate media protection

Not applicable. No certificate is issued to the signatory.

3.2.5 Certificate revocation

Not applicable. No certificate is issued to the signatory.

3.3 Roles and obligations of EUROSIGN

3.3.1 Technical environment

The signature service is installed on the EUROSIGN hosting site.

Security measures to protect access to the signature service are implemented, including:

- Monitoring of physical and logical access to the system and protection against intrusions,
- A limitation of access and administration of the service to a minimum of trusted people with the necessary skills.

3.3.2 Signature tool used

EUROSIGN relies on its signature service:

- To affix a seal for each "standard" electronic signature made,
- To affix a final time-stamped seal at the end of the transaction.

3.3.3 Type of certificate used

EUROSIGN uses a qualified sealing certificate issued by the Certinomis Certification Authority in accordance with the Certification Policy identified by the following OID: 1.2.250.1.86.2.3.3.22.1.

3.3.4 Certificate media protection

EUROSIGN complies with the use described in the Certinomis terms of use. As such, the electronic certificate is stored on a cryptographic device which must be qualified at least at FIPS 140-2 Level 2 or CWA 14169 (SSCD), and comply with the requirements of chapter 12.1 of the Certinomis Certification Policy.

3.3.5 Certificate revocation

EUROSIGN undertakes to request the revocation of its sealing certificate in case of loss, theft, compromise or mere suspicion of compromise of its private key and thus comply with the Terms of Use issued by the Authority of Certification Certinomis.

3.3.6 Signature verification data

EUROSIGN performs a quality check of the electronic signature prior to' archiving the signed document.

In order to carry out checks on electronic signatures/seals, EUROSIGN uses the data at its disposal, in particular the public data related to the EUROSIGN certificate, such as revocation lists or the certificate of the Certification Authority that issued its certificate.

All signed documents can be time-stamped at the end of the transaction allowing:

- To ensure the traceability of the date and time information of the signature of these transactions,
- To determine the revocation list to be used to validate this transaction.

If the signature verification stops, the electronic archiving of the document is temporarily suspended but does not impact the validity of the signed and time-stamped document.

EUROSIGN makes sure to implement the procedures and technical devices allowing to automatically launch a new verification of the signed document when the service is available again.

3.3.7 Protection of means

EUROSIGN ensures the implementation of the necessary means to protect the equipment providing the signature service.

The measures taken concern both:

- The protection of physical and logical access to the equipment to authorized persons only,
- The availability of the service,
- Monitoring and follow-up of the service.

3.3.8 Logs

EUROSIGN ensures the conservation of the relative traces:

- To the circulation of exchanges within networks and computer equipment,
- To the processing of data exchanged.

EUROSIGN ensures that the processing proofs related to the verification of electronic signatures are kept during the entire regulatory period.

3.3.9 Resume in case of service interruption

EUROSIGN ensures the implementation of the necessary means for the resumption of activity in case of service interruption of one of the components necessary for the tasks for which it is responsible.

In particular, it ensures that these means are tested at regular intervals.

3.3.10 User support

Signatories may contact EUROSIGN for any additional information or to report any malfunction at the address indicated in chapter 2.4.2.

3.4 Roles and obligation of recipients

3.4.1 Limitation of EUROSIGN's liabilities

3.4.1.1 Updating the information used

Some data, in particular revocation lists, cannot be updated in real time and it takes several hours (24 at most) before these data are published by the Certification Authority.

Under these conditions, it is possible that an electronic signature may be declared valid if it is made between the moment the certificate has been revoked and the moment its revocation has been published by the Certification Authority and taken into account by EUROSIGN.

EUROSIGN cannot be held responsible for this state of affairs considering this "deposit period" inherent in this type of system.

3.4.1.2 Content of signed documents

Customers are responsible for the content of the information contained in the signed document.

4. Electronic signature and validation

4.1 Characteristics of the signatory's equipment

The signatory's computer equipment (computer, tablet, smartphone) operates in an environment under the client's control.

The signature process is not dependent on the customer's equipment.

The certificate used by EUROSIGN for the customer's signature is a qualified seal certificate.

This certificate is issued by a Certification Authority : Certinomis

4.2 Signed data

Signed data are documents converted to PDF format prior to being signed.

The signature is visually integrated into PDF documents.

4.3 Electronic signature operation

Prior to the electronic signature process, the customer accesses one or more means of authentication according to the enrollment process in force.

Prior to the electronic signature process, the issuer of the document to be signed defines the level of authentication of the signatories expected among the following levels:

- **Level 1 authentication:** the identity of the signatory is checked on the basis of declarative information.

- **Level 2 authentication:** the identity of the signatory is checked on the basis of declarative information and the provision of proof of identity (national identity card, passport, residence permit).

The electronic signature operation can take place in different environments, depending on the equipment available to the signatory.

The following minimum functionalities are provided by the signature service, to allow the signatory to have knowledge and awareness of the action he is about to perform:

Presentation of documents to be signed
The documents to be signed are presented on the screen in sequence. The signatory must voluntarily scroll through all of the document(s) to be signed in order to enter the signature phase.

Presentation of signature attributes to the signatory
The following signature "attributes" are displayed to the signatory to enable him to be aware of the conditions under which his electronic signature will be made and processed:

- Link to the signature policy,
- Link to the Terms of Use,

The signatory must confirm that he has read and understood the Terms of use and the Signature Policy of the EUROSIGN service.

Interaction with the signatory: explicit consent and possibility of stopping the signature process
The signatory has the means to express explicitly (i.e., voluntarily and unambiguously) his or her consent to initiate the process of signature of the selected documents.

The signatory must voluntarily scroll all the document(s) to be signed. He may therefore in no way dispute that this information has been presented to him during the dematerialized transaction.

Authentication
Depending on the level of authentication desired by the issuer of the document to be signed, the customer is authenticated either on the basis of his or her declarative information (Level 1) or by providing proof of his or her identity (Level 2).

A unique authentication by SMS can be performed if it has been specified by the sender. The customer receives then a single-use code on his cell phone whose number has been declared either by himself or by the issuer of the document to be signed.

He is prompted to enter this code on the screen to authenticate and then proceed to the signature step.

Signature

Once signed, the documents are made available to the customer and archived.

4.4 Signatures characteristics

Electronic signatures affixed by customers are PDF signatures. The signature implemented is based on the PaDES standard (ETSI EN 319 412-1).

The certificate used to realize this signature is the EUROSIGN seal certificate.

At the end of the transaction, a final sealing can be performed and can be stamped by a Qualified Time Stamping Authority as defined by the eIDAS regulation. The timestamp token will also be contained in the PDF document.

4.5 Usable algorithms for the signature

4.5.1 Condensation algorithm

The supported condensation algorithms are SHA-256.

4.5.2 Encryption algorithm

The encryption algorithm to be used is RSA Encryption.

4.6 Signature verification

Signature verification is possible for the recipients and readers of the signed documents.

Where applicable, it relates to:

- Verification of compliance with the signature standard,
- Verification that the EUROSIGN certificate belongs to a qualified certificate family within the meaning of the eIDAS regulation or certified ETSI 319 411-1 NCP level at least,
- Verification of the EUROSIGN certificate and all certificates of the certification chain:
    - Temporal validity,
    - Status,
    - Cryptographic signature,

- Verification of the integrity of the transmitted data by calculating the fingerprint and comparing it with the received fingerprint,
- Verification of the electronic signature affixed to the file using the EUROSIGN public key contained in the transmitted certificate,
- The verification of the time-stamp data affixed on the last electronic seal carried out by EUROSIGN if applicable,
- Verification that the certificate used at the time of signature was not in a Certificate Revocation List. This concerns the EUROSIGN seal certificate,
- Verification of the referenced Signature Policy identifier.

4.7 Evidence management

In order to keep a trace of each signature validation, EUROSIGN constitutes a signed electronic proof, which lists the elements associated with the signature validation performed :

- Document signed by all customers,
- Seal certificate used by EUROSIGN on behalf of customers,
- Result of the validation,
- Control status of the Certificate Revocation List,
- All the certification chains implemented,
- Audit trail generated by the signature server.

This proof can be remade (by validating the signature of the proof) later in the event of dispute and restores exactly the information used during the validation.

5. Privacy policy

5.1 Classification of information

The following information is considered confidential:

- The private keys of the EUROSIGN seal service and of the components of the EUROSIGN signature service (private keys of Certification Authorities, private keys of Time-Stamping Units)
- The activation data associated with the EUROSIGN private key,
- The personal information of the users entered on the signature platform,
- User identity documents deposited on the signature platform,
- Contracts and other documents handled on the signature platform,
- The evidence and its content,
- The logs of the signature application,
- EUROSIGN's internal evidence management procedures,

- Audit reports on the EUROSIGN signature application and on the various infrastructure components, if any.

Confidential information is protected and therefore not publicly accessible.

5.2 Disclosure of information to a third party

A third party means any organization that is not in EUROSIGN's information processing chain.

The dissemination of information to a third party can only take place if EUROSIGN receives a formal request and accepts the disclosure (in particular in the context of a dispute and if a judge makes a request).

6. Legal provisions

6.1 Applicable law

This signature policy is governed by French law.

6.2 Disputes resolution

All disputes and litigation arising in the interpretation and implementation of this document will be subject to the jurisdiction of the Paris courts.

6.3 Intellectual property of the infrastructure for the creation and validation of signatories

EUROSIGN owns the intellectual property rights of the services implemented within the framework of its signature service.

The signatories have no intellectual property rights on the signed documents.

Any use or reproduction, in whole or in part, of these elements and/or the information they contain, by any process whatsoever, is strictly prohibited and constitutes an infringement punishable under the Intellectual Property Code.

EUROSIGN is the owner of the signature policy.

6.4 Personal data

The personal data within the meaning of Article 4 of the General Data Protection Regulation considered within the framework of the EUROSIGN signature service are:

- Signatory first and last name,
- Signatory's email address,
- Signatory's mobile number,
- Signatory's proof of identity.

The collection and use of personal data by EUROSIGN and all of its components are carried out in strict compliance with the laws and regulations in force on French territory, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as of 25 May 2018 (General Data Protection on Regulation - GDPR) and of the Law No. 78-17 of 6 January 1978 as amended relating to computing, files and freedoms.

In compliance with the above-mentioned provisions, the automated processing of personal data carried out by EUROSIGN has been declared to the National Commission for Computing and Liberties (CNIL).

The signatory is informed that he has the right to access, rectify and oppose data concerning him by writing to EUROSIGN.

The signatories are required to comply with the provisions of the law relating to computers, files and freedoms, the violation of which is subject to criminal penalties.

In particular, they must refrain, with regard to the nominative information to which they have access, from any collection, any misuse and, in general, any act likely to infringe on the privacy or reputation of individuals