PIXID Timestamping Policy

C1 - public

Version	Date	Modifications – Observations
0.1	16/02/2018	Création
0.2	09/2018	Révision
1.0	09/2018	Final version
1.1	04/2021	Rebranding (no modification except stylesheet)

	Committee
Drafted by	PKI Committee
Verified by	Governance Committee
Approved by	Security Committee

CONTENTS

1. Introduction

1.1 Overview

This policy is the Pixid Time-Stamping Policy (TSP) and Time-Stamping Practice Statement (TSPS), which describes the Pixid time-stamping service (TSS), its practices, and the obligations and requirements of Subscribers and Relying Parties.
A Time-Stamp Token (TST) provides evidence of the existence of a hash value at a given date and time. The TST's are generated and digitally signed by the TSA through the use of Time-Stamping Units (TSU's). Pixid may setup several TSU's in order to manage the TSS.
A TST is a signed structure which contains at least the following data:

- the hash value and the hash algorithm of the time-stamped datum
- date and universal time (UTC)
- the identifier of the TSU certificate that has generated the TST
- the identifier of Pixid acting as TSA (within the time-stamp certificate)
- the identifier of the CA that has signed the private keys installed on the TSU's

Within this TSP, day and time of each TST are synchronized with the Coordinated Universal Time (UTC) with an accuracy of less than one second. This TSP applies the standard TST format specified in the ETSI EN 319 422 standard [9].
This TSP is based on [8].

1.2 TSS Description

The Pixid platforms are solutions for web-based management of temporary and flexible employment. Companies (customers), Recruitment agencies (suppliers) and candidates (resources) meet on Pixid platforms and sign contractual agreements.
Pixid's Timestamping Service (TSS) is a Pixid-only service used for the timestamping of advanced electronic signatures produced on Pixid solutions.

1.3 Document name and identification

The TSP can be identified by any party through the following OID:

1.3.6.1.4.1.23876.111005

1.4 Policy administration

See [1].

1.5 TSS Participants

1.5.1 Certification Authorities

The TSU certificates are supplied by a CA. These certificates allow Relying Parties to identify the TSA.
The CA used to issue TSU certificates is "Pixid Server CA".

1.5.2 Time-Stamping Authorities

The TSA is in charge of the application of at least one TSP, by using one or more TSU's.
The TSA is managed by the Approval Board of Pixid
The board approves the TSP and the documents regarding the TSS provided by Pixid.
The board has the final authority and responsibility for:

- specifying and approving the infrastructure and practices of the Pixid TSS
- approving the Pixid TSPS and TSP
- ensuring the perennity of the TSP stated by the TSA in the scope of functional, organizational and technical requirements
- ensuring the perennity of the compliance of the TSU implementation with the TSP
- publishing the TSP and the terms of service and their revisions to Relying Parties

1.5.3 Subscribers

There is no Subscriber in this policy. The TSS is exclusively provided to the Pixid web platforms.

1.5.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a TST generated under this policy by the Pixid TSA.

1.6 Definitions and acronyms

1.6.1 References

[1] [PIXID - 111000 - C1] Certification Policy - Pixid Root CA. Available on Pixid's website (see section 2 of this document)
[2] [PIXID - 111002- C1] Certification Policy - Pixid Server CA. Available on Pixid's website (see section 2 of this document)
[3] General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
[4] Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, July, 23th, 2014.
[5] ETSI EN 319 411-1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, V1.1.1 (2016-02).
[6] ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, V2.1.1 (2016-02).
[7] ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, V2.1.1 (2016-02)
[8] ETSI EN 319 421 V1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps. OID : 0.4.0.2023.1.1
[9] ETSI EN 319 422 – Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp profiles, V1.0.0 (2015-02)
[10] CEN TS 419 261:2015 – Security requirements for trustworthy systems managing certificates and time-stamps, April 2015.

1.6.2 Definition

Advanced Electronic Signature	Refers to Electronic Signature which meets the requirements set out in Article 26 of the EIDAS Regulation [4].
Certification Authority (CA)	Authority trusted by one or more users to create and assign certificates. A certification authority may optionally create the users' keys.
Certificate	Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it.
Certificate Identifier	A unique identifier of a Certificate consisting of the name of the CA and of the certificate serial number assigned by the CA.
Certificate Policy (CP)	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement	Statement of the practices which a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
Certificate Validity Period	The time interval during which the CA warrants that it will maintain information about the status of the certificate. (Time interval between start validity date and time and final validity date and time).
Certificate Revocation List (CRL)	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certification Path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Service Provider	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
CRL Distribution Point	A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CA's.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient
Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

Hash Function	Cryptographic function that maps a variable length string of bits to fixed-length strings of bits, satisfying the following two properties: • It is computationally unfeasible to find for a given output an input which maps to this output; • It is computationally unfeasible to find for a given input a second input which maps to the same output.
Key Pair	Public Key and the corresponding Private Key.
Object Identifier (OID)	Sequence of numbers that uniquely and permanently references an object.
Public Key	Key of an entity's asymmetric key pair that can be made public.
Private Key	Key of an entity's asymmetric key pair that should only be used by that entity.
Subscriber	Entity that requests and subscribes to a Certificate and for which it is either the Subject or not.
Time Stamp	Proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.
Time Stamping Authority (TSA)	Authority trusted by one or more users to provide a Time Stamping Service.
Time Stamping Service (TSS)	Service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

1.6.3 Acronyms

AES Advanced Electronic Signature
ARL Authority Revocation List
CA Certification Authority
CP Certificate Policy
CPS Certification Practice Statement
CRL Certificate Revocation List
CSP Certification Service Provider
DSA Digital Signature Algorithm
DRA Delegated Registration Authority
HSM Hardware Security Module
IETF Internet Engineering Task Force
ISO International Organisation for Standardisation
ITU International Telecommunications Union
LCP Lightweight Certificate Policy
LDAP Lightweight Directory Access Protocol
NCP Normalised Certificate Policy
NCP+ Normalised Certificate Policy +
OID Object Identifier
OCSP Online Certificate Status Protocol
OTP One Time Password
PIN Personal Identification Number
PKI Public Key Infrastructure
PKIX Public Key Infrastructure (X.509) (IETF Working Group)
PKCS Public Key Certificates Standard
QES Qualified Electronic Signature
RA Registration Authority
RFC Request for Comments
RSA A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
SCD Signature Creation Device
SSCD Secure Signature Creation Device
TSA Time Stamping Authority

TSP	Time Stamping Policy	URL	Uniform Resource Locator
TSS	Time Stamping Service	UTC	Coordinated Universal Time
TSU	Time Stamping Unit		

2. Publications and Repository Responsibilities

2.1 Identification of entities operating repositories

See [1].

2.2 Repositories

The following information is publicly available at the following URL: https://pki.mypixid.io

- this TSP
- the certificates of the TSU's.

2.3 Time of Frequency of Publication

An update of all relevant Terms & Conditions (including the TSP, the General Terms and Conditions) is published whenever a change occurs.
The TSU certificates are published at most 72 hours after their generation and necessarily prior to their effective use.

2.4 Access Control on Repositories

See [1].

3. General provisions

3.1 TSA obligations

Pixid will supply a TSS in accordance with its TSP and will ensure that the requirements specified in the present TSP are satisfied.
Pixid will ensure the technical issuance of the TST's.

3.2 Relying Party obligations

The Relying Party must verify that the TST's have been correctly signed and that the corresponding TSU certificate is not revoked at the time of verification, by using the CRL's published by the issuing CA.
The Relying Party must also verify that the TST's requests are actually issued by an Pixid TSU. To do so, the Relying Party must verify that the TST includes a reference to an Pixid TSU.
The Relying Party should take into account the TST use limitations described in this TSP and the relying party agreement.

3.3 Obligations for the CA's providing the TSU certificates

The present TSP does not define requirements for the CA providing the TSU certificates; however, the TSU certificates are exclusively issued by Pixid's Server CA [2].

3.4 Timestamping practices

Pixid ensures that it has the reliability needed to provide a TSS and describe how this TSS is implemented. This description ensures that:

- Pixid evaluates business assets and threats to those assets in order to determine the necessary controls and operational procedures
- Pixid has a statement of the practices and procedures used to address all the requirements identified in the present TSP
- The obligations and the implementation requirements to be complied with by the TSA are identified
- Pixid provides Relying Parties with the means to assess conformance to this TSP.
- Pixid implements a relevant organization for the approval of its practices and the verification of conformity between them and this TSP
- Pixid defines a periodic control procedure in order to verify that its practices comply with this TSP

3.5 Conformance with legal requirements

3.5.1 Applicable law

The present document is governed by French and European law.

3.5.2 Litigation settlement

Not applicable; the TSS is self-operated.

3.5.3 Personal data

The TSS operates in compliance with [3].
Pixid is bound to keep any personal data provided to the TSS confidential, unless its disclosure is allowed by the owner of the data or demanded by regulation or adjudication.

3.6 Amendments

3.6.1 Procedure for amendment

Pixid via its Board is responsible for approval and changes of the policy.
The only changes that the Pixid Board may make to these TSP specifications without notification are minor changes that do not affect the assurance level of this TSP, e.g., editorial or typographical corrections, or changes to the contact details.
Errors, updates, or suggested changes to this document shall be communicated to the contact of the Pixid Board as identified in the present TSP. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.

The Pixid Board shall accept, modify or reject the proposed change after completion of a review phase.

3.6.2 Notification mechanism and period

Proposed changes to the TSP will be disseminated to interested parties by publishing the new document on the Pixid repository.

3.6.3 Circumstances under which OID must be changed

All changes to the TSP, other than editorial or typographical corrections, or changes to the contact details, will be subject to an incremented version of the Object Identifier for the TSP.
Minor changes to this TSP do not require a change in the TSP OID that might be communicated by the CA.
Major changes that may materially change the acceptability of TST's for specific purposes may require corresponding changes to the TSP OID.

4. Operational requirements

4.1 Audit log

Unless otherwise mentioned, Pixid ensures that any appropriate information regarding the TSS operation is kept 7 (seven) years after the corresponding TSU has been decommissioned, mainly in order to provide evidence in case of legal investigation.
Audit logs cover events relating to:

- generation of TST
- administration of the TSS: context management, certificate import, service status
- operation and synchronization of internal clock
- TSU keys life cycle
- TSU certificates life cycle
- any kind of events which might impact the TSU operation.

Each audit record contains precise date and time of the event.
The audit log confidentiality is ensured by an appropriate management of physical, system and network access.

4.2 Private key life cycle management

Pixid ensures that the private signing keys of the TSU are not used after the end of their life cycle.
The TSU automatically destroys the private key when the usage period of the key is reached. TSU keys are not renewed.
Pixid ensures that the number of TSU's in operation at any given time is sufficient to provide a reliable service.

4.3 Clock synchronization

Pixid ensures that:

- its clocks are synchronized with the universal time (UTC) with the declared accuracy of one second
- the calibration of the TSU is maintained so that the clocks shall not be expected to drift outside the declared accuracy
- the TSU clocks are protected against threats related to their environment that could lead to a desynchronisation with respect to UTC time outside the declared accuracy
- a TSU internal clock drift outside the bounds of the declared accuracy is detected
- if the clock of one of the TSU is detected as outside the declared accuracy, then TST's will not be generated any more
- clock synchronization is maintained when a leap second occurs as notified by the appropriate body. The change to take into account the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record of the exact time (within the declared accuracy) is performed when this change occurs.

4.4 Timestamp tokens

Pixid ensures that the TST's are generated securely and include the correct time.

4.5 Content of a TST

In the answer to a request, Pixid provides a TST complying with [9] and containing the following fields:

version	Version 1
policy	OID : 1.3.6.1.4.1.23876.111005
messageImprint	OID of the hash algorithm and the hash value of the data to timestamp. Note : this information is provided in the incoming request.
serialNumber	160 bit random number uniquely identifying the request.
genTime	Time-stamp date in ASN.1 GeneralizedTime format
accuracy	Accuracy of 1 second
ordering	Flag set to FALSE
nonce	Value sent back identically if contained in the request
tsa	DN of the certificate used to sign the TST
extensions	Not used.

4.6 TST signature

The contents of a TST are signed using a 2048 bit RSA private key.

4.7 TSA compromise

In the case of events impacting the security of the TSS and which could impact the generated TST's, Pixid ensures that appropriate information is provided to Relying Parties and Supervisory bodies.
Pixid has taken into account in its Disaster Recovery Plan the potential compromise of its TSS.

4.7.1 Disaster Recovery Plan

The Disaster Recovery Plan addresses the compromise of TSU private signing key, either actual or suspected, or the loss of calibration of a TSU clock, which might impact the issued TST's.
Pixid constantly updates its Disaster Recovery Plan in order to cover and to ensure the best possible service against the following threats:

- private key compromise
- network failures
- unavailability of personnel
- problems pertaining to clock calibration
- failure of hardware components

4.7.2 Communication

In case of a compromise, real or suspected, or the loss of calibration of a TSU, that could impact generated TST's, Pixid will provide Relying Parties and Supervisory bodies with a description of the incident.

4.7.3 Interruption of TST generation

In case of a compromise, real or suspected, or the loss of calibration of a TSU, that could impact generated TST's, Pixid takes all necessary measures to ensure that this TSU does not generate any further TST's until steps are taken to restore the situation.

4.7.4 ANSSI alert

In case of a compromise, real or suspected, of its TSS, Pixid will notify directly and without delay the ANSSI, as the French Supervisory Body.

4.8 End of activity

Procedures to handle the end of activity are defined by Pixid. Pixid ensures that all the information necessary to verify the correctness of TST's will be provided, even after the termination of its TSS.
Prior to the termination of its TSS, the following procedures will be performed:

- Pixid will transfer obligations to a reliable body for maintaining event logs and audit archives necessary to demonstrate its correct operation for a reasonable period
- Pixid will maintain its obligations to make available its public keys or certificates to relying parties for a reasonable period
- the TSU private keys will be destroyed so that they cannot be retrieved, according to the procedure described in section.

Pixid takes all necessary measures to cover the costs to fulfill these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself.

5. Facility, management, and operational controls

See [1].

6. Technical security controls

See [1] for generic security controls. The current section only refers to the management of TSU's.

6.1 Time accuracy

TSU clocks are locally monitored by reference time servers. These servers are autonomous and are synchronized with UTC(k) reference servers. Pixid ensures that the TST's generated by its TSS have an accuracy with respect to UTC time of less than one second.

6.2 Private key protection

6.2.1 Cryptographic module standards and controls

The TSU's HSM follow the same requirements, standards and controls as the ones used for the CA. See [1].
TSU private keys are never exported outside of these modules. The keys are stored within only one hardware security module environment. The keys are generated only for the TSS.
The TSU's use 2048 bit RSA private keys.

6.2.2 Private key escrow

Key escrow is never allowed.

6.2.3 Private key backup

Not applicable to TSU's keys.

6.2.4 Private key archival

Not applicable to TSU's keys.

6.2.5 Private key transfer into or from a cryptographic module

Not applicable to TSU's keys.

6.2.6 Method of activating the private key

TSU's keys are automatically activated.

6.2.7 Method of deactivating private key

TSU's keys cannot be deactivated.

6.2.8 Method of destroying private key

Pixid ensures that TSU private keys are destroyed at the end of their life cycle.

6.2.9 Cryptographic module rating

See section 6.2.1.

6.3 Certification of TSU keys

A TSU certificate request is transmitted to the CA, in accordance with the rules defined in the corresponding Certificate Policy.
The TSA abides by its obligations defined in the Certificate Policy of the CA.
The TSA verifies, when importing a certificate in a TSU, that it comes from the intended CA.
Each TSU owns a unique active key at a given time.
Pixid ensures that cryptographic keys are loaded in the HSM prior any TST issuing.

6.4 Mandatory algorithms

The Pixid TSA:

- accepts hash values generated by Subscribers and using hash algorithms in compliance with regulatory requirements. The accepted hash algorithms are the following:
  - SHA-256
  - SHA-384
  - SHA-512
- issues TST's signed with algorithms and key lengths in compliance with regulatory requirements. The TSU key pair is a 2048 bit RSA key. The signature algorithm uses a hash function belonging to the SHA-2 family.

6.5 TST verification

Pixid ensures that Relying Parties can obtain information needed to verify the digital signature of TST's.

6.6 Validity period of TSU certificates

The Validity period of a TSU certificate is defined by the CA.

6.7 Computer security controls

See [1].

6.8 Life cycle technical controls

See [1].

6.9 Network security controls

See [1].

7. TST Profile

See 4.5.

8. Compliance audit and other assessments

See [1].