pixidgroup

Certification Policy - Pixid Root CA

1.3.6.1.4.1.23876.111000

C1 – public

Version	Date	Modifications – Observations
0.1	18/01/2018	Création
0.2	09/2018	Relecture
1.0	09/2018	Final version
1.1	04/2020	Correction numérotation et taille de clé AC Root
1.2	04/2021	Rebranding (no modification except stylesheet)

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

CONTENTS

1. Introduction

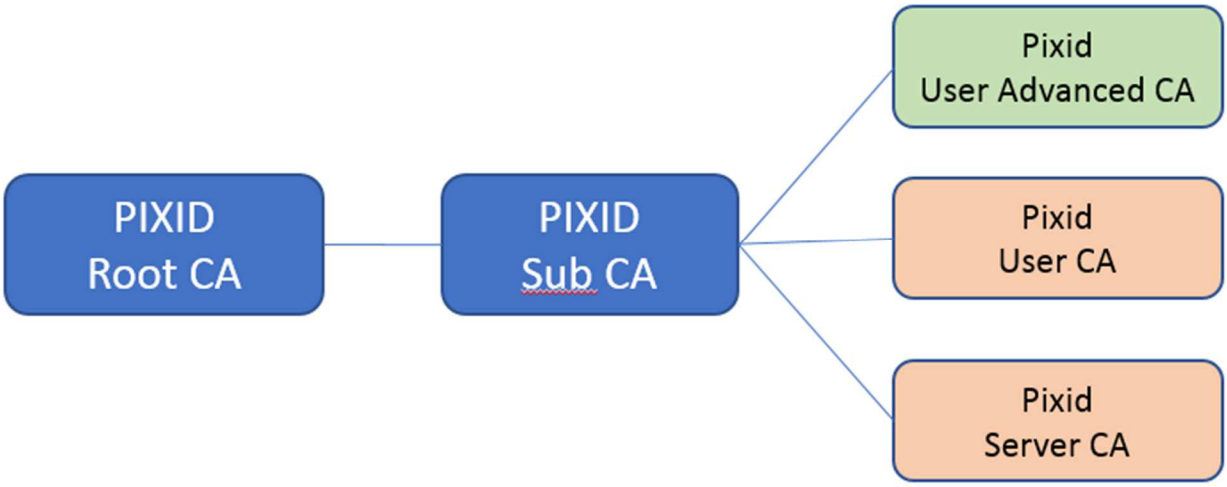
1.1 Overview

1.1.1 Purpose of the Pixid PKI

The purpose of Pixid PKI is to provide authentication, advanced e-signature and e-seals certificates to the users of Pixid solutions and Pixid employees.

1.1.2 Pixid PKI Hierarchy

Pixid, acting as a TSP, is using several Certification Authorities (CA), as shown in the certificates hierarchy, to issue Pixid end-user certificates.



1.1.3 The present document

The present document contains the certificate policy (CP) and practices (CPS) for the CA's of Pixid's hierarchy which do not produce end-users certificates. Throughout this document, the use of the term "CP" refers to the present document, unless otherwise specified.
The CP describes:

- Practices common to **Pixid Root CA** and **Pixid Sub CA**
- Details of the Pixid trustworthy systems and operations

1.2 Document name and identification

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

1.3.6.1.4.1.23876.111000

1.3 Policy administration

1.3.1 Organization administering the CP

The organization administering the CP is Pixid acting as Trusted Service Provider (TSP). The TSP Board is the management body with final authority and responsibility for:

- Specifying and approving the Pixid infrastructure and practices.
- Approving the Pixid Certification Practice Statement(s), Pixid Certificate Policies and Pixid Time Stamping Policies.
- Defining the review process for practices and policies including responsibilities for maintaining the Certification Practice Statements and Certificate Policies.
- Defining the review process that ensures that the Pixid CA's properly implements the above practices.
- Defining the review process that ensures that the Certificate Policies are supported by the Pixid Practice Statement(s).
- Publication to the Subscribers and Relying Parties of the Certificates Policies and Certification Practice Statements and their revisions.

Prior to becoming applicable, modifications to the CP are announced in the repository as available on https://pki.mypixid.io/.
The TSP board can be contacted using the following coordinates:

Pixid contact information	
Contact Person	Patrick FOUBERT
Postal Address	53-55 rue du Capitaine Guynemer - 92400 Courbevoie - France
Telephone number	01.41.16.34.00
E-mail address	contact@pixid.fr
Website	www.pixid.fr

1.3.2 Entity determining suitability between CP and covered CPs

The TSP Board determines suitability between CP and CPs, based on peer review.

2. Definitions and acronyms

2.1 References

1. The European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
2. European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
3. 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.

4. 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).
5. 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).
6. ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, V2.1.1 (2016-02)
7. CEN TS 419 261:2015 – Security requirements for trustworthy systems managing certificates and time-stamps, April 2015.

2.2 Definition

Advanced Electronic Signature	Refers to Electronic Signature which meets the requirements set out in Article 26 of the EIDAS Regulation 1.
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.
Commitment Type	A signer-selected indication of the exact intent of an electronic signature.
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.
Data To Be Signed (DTBS)	The complete electronic data to be signed (including both Signer's Document and Signature Attributes).
Device	Combination of the key pair, the corresponding certificate and secured user device

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
End Entity	A certificate subject that uses its public key for purposes other than signing certificates
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.
Online Certificate Status Protocol (OCSP) Provider	Online trusted source of certificate status information. The OCSP protocol specifies the syntax for communication between the OSCP server (which contains the certificate status) and the client application (which is informed of that status).
Public RA	Publicly accessible RA to all potential Pixid client
Public Key	Key of an entity's asymmetric key pair that can be made public.
Private RA	RA dedicated to a closed user group
Private Key	Key of an entity's asymmetric key pair that should only be used by that entity.
Qualified certificate for electronic signature **or seal**	Certificate for electronic signatures or seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the EIDAS Regulation 1.
Secure User Device	Device which holds the user's private key and protects this key against compromise and performs signing or decryption functions on behalf of the user.
Signature Attributes	Additional information that is signed together with the Signer's Document.
Signature Creation Data	Refers to unique data, such as codes or private cryptographic keys used by the signatory to create an electronic signature.
Signature Creation Device	Refers to configured software or hardware used to implement the signature creation data.
Signature Policy	Set of technical and procedural requirements for the creation and verification of an electronic signature, under which the signature can be determined to be valid.
Signature Policy Identifier	Object Identifier that unambiguously identifies a Signature Policy.
Signature Verification	Process performed by a verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.
Signature-Verification-Data	Data, such as codes or public cryptographic keys used for the purpose of verifying an electronic signature.

Signature-Verification Device	Configured software or hardware used to implement the signature verification-data.
Signatory	A person who holds a signature creation device and acts either on his own behalf or on behalf of the natural legal person or entity he represents.
Signer	Entity that creates an (electronic) signature.
Subject	Entity to which a Certificate is issued.
Subscriber	Entity that requests and subscribes to a Certificate and for which it is either the Subject or not.
Trusted Third Party (TTP)	Authority trusted (and widely recognised, possibly accredited) by one or more users to provide Trusted Services such as Timestamping, Certification …
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	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.
Validation Data	Additional data, collected by the signer and/or a verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include: certificates, revocation status information, time-stamps or Time-Marks.
Verifier	Entity that validates or verifies an electronic signature. This may be either a relying party or a third party interested in the validity of an electronic signature.
What You See Is What You Sign (WYSIWYS)	Description of the required qualities of the interface able to unambiguously present to the signer the document to be signed according to the content and format.

2.3 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
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
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 Trust Service Provider
TSU Time Stamping Unit
URL Uniform Resource Locator
UTC Coordinated Universal Time

3. Publications and Repository Responsibilities

3.1 Identification of entities operating repositories

The TSP Board is the entity responsible for the operation of online and publically available repository(ies). Pixid is also responsible for the publication of the following documents and information:

- The CP (Certificate Policies)
- The related subscriber contractual agreements (e.g., Purchase Orders, General Terms and Conditions, etc.)
- The Certification Authority Certificates, Certification Paths and related ARLs
- The Certificate Revocation Lists (CRLs)
- The Pixid Time Stamping Policy

The aforementioned documents as well as complementary information are available from the online publicly accessible website as described in section 3.2.

3.2 Publication of Certification Information

The Pixid CP covering the practices used by the CA for Certificates issuance under the applicable CP is available online on https://pki.mypixid.io/. This repository shall also contain any other public documents where Pixid makes certain disclosures about its practices, procedures and the content of certain of its policies, including the CP, and the covered CPs.
The Root CA publishes revocation status information at the following URL: https://pki.mypixid.io/
Note: The status information of any Certificate as delivered by the OCSP server shall be consistent with the information listed in the CRL in force, and vice versa.
The CA maintains the CRL distribution point and the information on this URL until the expiration date of all Certificates containing the CRL distribution point.

3.3 Time of Frequency of Publication

3.3.1 Frequency of Publication of Revocation information

The Root and Intermediate CA's publish their LRA at least every year.

3.3.2 Frequency of Publication of Terms & Conditions

An update of all relevant Terms & Conditions (including the Pixid CP, the General Terms and Conditions) is published whenever a change occurs.

3.4 Access Control on Repositories

All repositories as listed in 2 are available in public anonymous read-only access. Only trusted staff functions, as specified in section 4 of the present document, have write and change access on these repositories, with strong access control. State-of-the-art security measures protect these repositories.

4. Facility, management, and operational controls

The management, operational, procedural, personnel and physical (non-technical security) controls that are used by Pixid with regards to its Certification Authorities (CA's) and the other PKI Participants other than Subscribers and Relying Parties to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing and archiving seek compliance with the technical standards 4 and 6.
These controls are further described and ruled by the next sub-sections.
Pixid carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is available as an internal document at Pixid.
Pixid provides direction on information security through its TSP Board, responsible for defining the TSP's information security policy and ensuring publication and communication of the policy to all personnel who are impacted by the policy.
Pixid ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose Pixid maintains an inventory of all information assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

4.1 Physical controls

Pixid implements and ensures implementation of physical security controls on all sites and premises, either own, leased or rented, that are used to support its certification and time stamping services. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities, and to avoid compromise or theft of information and information processing facilities.
Detailed descriptions of the secure sites and premises that are used by Pixid to provide certification and time stamping services, as well as Access Control Security Policies are available in Pixid internal documents.

4.1.1 Site location and construction

Several secure premises are used according to the type of component service that is used as part of the provision of Pixid certification and time stamping services. All these premises are protected through numbered zones and locked rooms, cages, safes, and cabinets.

4.1.2 Physical access

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating TSP operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token, and/or biometric readers and access control lists.
Strict access control is enforced to all secure areas. Access to the secure areas is limited to authorized personnel listed on an access list, which is subject to audit and control.

4.1.3 Power and air conditioning

Power and air conditioning operate with a high degree of redundancy in highly secure areas.

4.1.4 Water exposures

Secure areas are protected from any water exposures.

4.1.5 Fire prevention and protection

Secure areas benefit from appropriate prevention and protection measures against fire exposures.

4.1.6 Media storage

Media are stored securely. Backup media are securely stored in a separate location from the original media location. All media storage areas are protected from fire and water exposure and damages according to internal CA risk analysis.

4.1.7 Waste disposal

Waste disposal is securely implemented in order to prevent unauthorized disclosure of sensitive data. Cleaning operations, as well as other types of operations not directly linked to the certification or time stamping (component) services operations, are be strictly monitored and implemented in order to prevent unauthorized actions and/or disclosure of sensitive data.

4.1.8 Off-site backup

Backup media are securely stored in a separate location from the original media location and are protected against fire and water exposure. Pixid implements the necessary measures to ensure a full and automatic recovery of its services in case of a disaster, corrupted servers, software or data. Backup and Disaster recovery sites are located in separate premises sufficiently distant from the primary locations and benefit from equivalent security measures.

4.2 Procedural controls

The TSP for CA activities ensures that CA systems are secure and correctly operated with minimal risk of failure.

4.2.1 Trusted Roles

All members of the personnel staff that involved for the provision of the Pixid certification and time stamping services are either employees of Pixid or authorised and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services.
All members are subject to personnel and management practices that Pixid follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and time stamping related technologies.
All members of the staff operating certificate, key management operations (including (S)SCD devices provisioning), acting as Registration Authorities, security officers, system operators, system administrators, quality control manager and system auditors or any other operations that materially affect such operations, and members of the Pixid TSP Board are considered as serving in a trusted position.
Pixid ensures that:

- All tasks, roles and responsibilities with respect to the Pixid certification and time stamping services are:
  - Described in job descriptions and made available to the concerned personnel. These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness, and differentiating between general functions and CA specific functions.
  - Allocated to the system of the TSP and/or to the member of the staff according to its trusted role.
- All actions with respect to the Pixid certification and time stamping services can be attributed to the system of the TSP and/or to the member of the staff that has performed the action.
- Personnel exercise administrative and management procedures and processes that are in line with the Pixid information security management procedures (see introduction of section 4 of the CP).
- Trusted or management roles are formally appointed to trusted roles by senior management responsible for security and are not appointed to any person who is known to have a conviction for a serious crime or other offense which affects his/her suitability for the position and/or until necessary checks are completed.
- Appointment to trusted roles is such that the possibility of fraud is minimized.
- Managerial personnel possess expertise in the electronic signature, time stamping technology, mechanisms for calibration or synchronization the TSU clocks with UTC, in risk assessment and information security as well as possess familiarity with security procedures for personnel with security responsibilities.
- CA personnel are formally appointed to trusted roles by senior management responsible for security.

4.2.2 Number of persons required per task

Where dual control is required at least two trusted staff members need their respective and split knowledge in order to be able to proceed with the on-going operation.
For tasks related to critical CA functions such as but not limited to key management and in particular CA key generation, more than two persons are required (see section 5) for extended security and control reasons.

4.2.3 Identification and authentication for each role

Each member of the personnel staff is issued a credential in order to ensure proper identification and authentication prior being allowed to perform any trusted action.

4.2.4 Roles requiring separation of duties

All audit and/or control roles are performed with regards to the separation of duties versus the audited and/or controlled role.

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

Managerial personnel possess expertise and training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.
Pixid ensures that all members of the personnel staff that are involved for the provision of the Pixid certification and time stamping services whether employees of Pixid or authorized and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services are checked regarding qualifications, expert knowledge, experiences and clearance needed and as appropriate to fill trusted roles and to perform the related specific job function.

4.3.2 Background check procedures

Pixid ensures that the relevant checks are performed to prospective personnel by means of status reports issued by a competent authority, third-party statements or signed self-declarations.

4.3.3 Training requirements

Pixid ensures that the relevant trainings are provided to members of the Pixid personnel staff to carry out their specific job functions related to the provision of the Pixid certification and/or time stamping (component) services.

4.3.4 Re-training frequency and requirements

After completion of initial training, training updates are performed to all categories of members of Pixid personnel staff to establish continuity and updates in the knowledge of the personnel and in procedures.

4.3.5 Job rotation frequency and sequence

Not applicable.

4.3.6 Sanction for unauthorized actions

Pixid ensures that relevant sanctions are provided to members of the Pixid personnel staff for policies or procedures violations, unauthorized actions, unauthorized use of authority and unauthorized use of systems

for the purpose of imposing accountability on the TSP personnel, as it may be appropriate under the circumstances. This may include among others revocation of privileges, administrative discipline and/or penal action.

4.3.7 Documentation supplied to personnel

Pixid ensures that the relevant documentation are provided to members of the Pixid personnel staff to carry out their specific job functions related to the provision of the Pixid certification and/or time stamping (component) services.

4.4 Audit logging procedures

4.4.1 Type of events recorded

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. Pixid ensures the following controls are being implemented:

- All events relating to the life-cycle of CA keys are recorded
- The Pixid CA's event logging systems record events related to certificate lifecycle operations including but not limited to:
  - CA key generation
  - Issuance of a certificate
  - Revocation of a certificate
  - Suspension of a certificate
  - Automatic revocation
  - Publication of a CRL.
- All other certification components are equipped with event logging systems that record events related to any operation performed on behalf of the component services.
- Pixid audits all event-logging records. Audit trail records contain:
  - The identification of the operation
  - The date and time of the operation
  - The identification of the Certificate involved in the operation
  - The identity of the transaction requestor.
- In addition, Pixid ensures maintenance of internal logs and audit trails of relevant operational events in the whole infrastructure whatever the component service, including, but not limited to:
  - Start and stop of servers
  - Outages and major problems
  - Physical access of personnel and other persons to sensitive parts of any secure site or area
  - Back-up and restore
  - Report of disaster recovery tests
  - Audit inspections
  - Upgrades and changes to systems, software and infrastructure
  - Security intrusions and attempts at intrusion.

The IT systems ensure that the precise time all events, records and documents listed above are recorded.

4.4.2 Frequency of processing log

Audit logs are processed continuously and/or following any alarm or anomalous event. Audit logs are archived continuously.

4.4.3 Retention period for audit log

Audit log are kept for a minimum of 10 years.

4.4.4 Protection of audit log

The log files are properly protected by an access control mechanism. Only authorized auditors can have access to audit logs.
Appropriate protection against modification and deletion of the audit logs is implemented such that no one may modify or delete audit records except for transfer to long term media for archiving purposes.

4.4.5 Audit log backup procedures

Log files and audit trails are backed up according to internal procedures.

4.4.6 Notification to event-causing subject

If required, Pixid notifies the originator of the audit event.

4.5 Records Archival

4.5.1 Type of records archived

Pixid keeps internal records or ensures the archival, in a trustworthy manner, of the following items:

- All certificates for a period of a minimum of 7 years after the expiration of that certificate
- Audit trails on the issuance of certificates for a period of a minimum of 7 years after issuance of a certificate
- Audit trail of the revocation of a certificate for a period of a minimum of 7 years after revocation of a certificate
- Registration related information for a minimum of 10 years following registration
- CRLs for a minimum of 10 years after publication
- The very last back up of a CA archive for 10 years following the issuance of the last certificate by this CA.

Pixid keeps archives or ensures that archives are kept in a retrievable format.

4.5.2 Retention period for archive

See section 4.5.1.

4.5.3 Protection of archive

Pixid ensures:

- implementation of proper copy mechanisms to prevent data loss or data access loss over time and,
- the confidentiality and integrity of the archive and its physical storage media is maintained during its retention period, and
- Those records concerning certificates are completely and confidentially archived in accordance with the CP.

Archives are accessible to the authorized personnel of Pixid

4.5.4 Archive backup procedures

See section 4.5.3.

4.5.5 Requirements for time-stamping of records

Pixid ensures that the precise time of archiving all events, records and documents listed in section 4.4 and 4.5 is recorded. This is accomplished through accurate NTP synchronization of all systems.

4.5.6 Archive collection system

Archive collection systems are internal to the component service or legal entity operating the component service.

4.5.7 Procedure to obtain and verify archive information

Archives are accessible to the authorized personnel of Pixid Records are retained in electronic or in paper-based format.
When the certificate subject is a natural person, he (or she) may access to related registration records and other information relating to himself (herself); within the constraints of data protection requirements, the Subscriber may similarly access that information.

4.6 Compromise and disaster recovery

4.6.1 Incident and compromise handling procedures

The applicable and appropriate incident and/or compromise reporting and handling procedures, disaster recovery procedures and Business Continuity Plan have been established and are available as a separate internal document.
All incident and/or compromise events are documented and any associated records are archived as described in 4.5.

4.6.2 Computing resources, software, and/or data are corrupted

Pixid establishes the necessary measures to ensure full and highly automated recovery of the Pixid certification and time stamping services in case of a disaster, corrupted servers, software or data.

4.6.3 Entity private key compromise procedures

Compromise of the CA private key(s) or of the associated activation data implies immediate revocation of the certificate of the compromised key(s).
Pixid will additionally take the following measures:

- Notify all PKI Participants
- Notify the French supervisory body (ANSSI)
- Notify the public at large through several channels, including a message on the Pixid repository and web site
- List the certificate of the corrupted CA in CRLs (ARLs),
- Revoke all the certificates signed by the corrupted CA,
- Pixid may generate a new key pair and associated certificate for the CA, and re-issue all issued certificates that were revoked as a consequence of the CA corruption. This process is to be followed only after the following conditions:
    1. assessing the reasons for corruption of the CA private key
    2. revocation of the CA certificate,
    3. having taken all the necessary measures to avoid the cause of revocation in the future,
    4. decision from Pixid TSP Board,

Compromise of private key(s), or of the private keys associated activation data, of other entities (including Subscribers) leads to immediate revocation of the certificates associated to the compromised key(s). These entities are (contractually) bound to notify Pixid with regards to the issuing CA of any (suspicion of) such compromise of their private key(s) or of the associated activation data. See the applicable sections of the CP and of the applicable CP for further details on PKI Participants obligations in that matter.

4.6.4 Business continuity capabilities after a disaster

Pixid establishes the necessary measures to ensure full and highly automated recovery of the Pixid certification and time stamping services in case of a disaster, corrupted servers, software or data. The Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

4.7 CA termination

Pixid ensures that potential disruptions to Subscribers and Relying Parties are minimised as a result of the termination of one of the Pixid CA's services. Pixid guarantees continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

5. Technical security controls

The security measures taken by Pixid with regards to its CA's to protect CA's cryptographic key and activation data, the constraints on repositories, subject CA's, and other PKI Participants, to protect their Private Keys, activation data for their Private Keys, and critical security parameters, ensuring secure key management, and other technical security controls used by Pixid to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, archiving, and other technical security controls on PKI Participants seek compliancy with the technical standards 4 and 6.
These controls are further described and ruled by the following sub-sections.

5.1 Key pair generation and installation

Key pair generation and installation is considered for the relevant PKI Participants, which are the issuing CA and CA Subscribers.
As CA's are issued under the Pixid Root CA, and located within the Pixid infrastructure, all Pixid CA's, will undergo the same process as described in 5.1.1.

5.1.1 Key pair generation

5.1.1.1 Pixid CA Key pair generation and installation

5.1.1.1.1 Pixid CA Key generation process

Pixid uses a trustworthy process and systems for the generation of its Pixid Root CA and subordinate CA's private keys (and certificates) according to a documented internal procedure.
The secret shares of these private keys are distributed amongst authorised secret-shareholders under the authority of the TSP according to a documented procedure. Pixid ensures that CA's private keys are securely generated, used and protected, using a trustworthy system, and that the necessary measures are taken to prevent their compromise or unauthorised usage.
The CA's Key Ceremony process is witnessed by Pixid TSP representative(s) to ensure confidence in the proper and secure execution of the CA's Key generation procedure.
The CA key pair certificate requests are made available (under standard format) to Pixid and are protected by appropriate measures to prevent unauthorised usage.

5.1.1.1.2 CA Key generation devices and key storage

The generation and storage of CA private keys of the Pixid CA's occurs within a secure cryptographic device meeting appropriate requirements as set forth in section 5.2.1.

5.1.1.1.3 CA Key pair re-generation and re-installation

In case of Pixid CA's key pair re-generation and re-installation, when replacing private keys by new ones, Pixid ensures that exactly the same procedure as for initial key generation is used. Appropriate measures are taken to communicate the end of CA key life cycle and replacement to Subscribers and Relying Parties, also taking into account statements made in the section 5.1.4 of the CP.

At the end of their lifetime, the CA private keys that have been used in the past must be decommissioned and destroyed as well as the active tamper resistant devices and as well as all back-up copies of past private keys in accordance with section 5.2.9.

5.1.2 CA public key delivery to Relying Parties

The Pixid CA's public keys are securely provided to potential Relying Parties in a SSL session from the Pixid repository (see 3.2).

5.1.3 Key sizes

5.1.3.1 Pixid CA Private Key Type

CA	Name	RSA Key size	Hash algorithm
Root CA	Pixid Root CA	4096	SHA512
Subordinate CA	Pixid Sub CA	4096	SHA512
Issuing CA	– CA Pixid User Advanced – CA Pixid Server Advanced – CA Pixid User – CA Pixid Server	4096	SHA256, SHA384 and SHA512

5.1.4 Public key parameters generation and quality checking

Public key RSA exponents are chosen secure. Public Key module generation is done with state of the art parameter generation technology. Parameter generation is implemented using state of the art technology and are regularly re-evaluated regarding new advances in cryptology.

5.1.5 Key usage purposes

5.1.5.1 CA Private Key purposes

Pixid ensures that the CA private signing key(s) are only used for signing certificates, CRLs and OCSP responses. Pixid ensures that the CA private keys are not used within the CA in any way outside the scope of the Pixid PKI domain.

5.1.5.2 Pixid Root CA key usage and purpose

Private key of the Pixid Root CA is used to sign subordinates Pixid CA's, corresponding ARL's. Pixid Root CA is an off-line CA and is never used for signing end-entity certificates.

5.1.5.3 Pixid subordinate CA key usage and purpose

The private key of the Pixid subordinate CA is used to sign Issuing CA's and corresponding ARL's. Pixid subordinate CA is an on-line CA and is never used for signing end-entity certificates.

5.1.5.4 Pixid Issuing CA's key usage and purpose

The private key of the Pixid Issuing CA's is used to sign Certificates issued to end-entities, the corresponding CRLs and OCSP certificates. Unless otherwise specified, Pixid CA's are on-line CA's.

5.2 Private key protection

5.2.1 Cryptographic module standards and controls

The TSP uses appropriate secure cryptographic devices to perform CA key management tasks. These cryptographic devices are known as Hardware Security Modules (HSMs).
Hardware and software mechanisms that protect CA private keys are adequately documented. HSMs are prepared, distributed and managed in compliance with the technical standards 647.
HSMs do not leave the secure environment of the CA secured premises. In case HSMs require maintenance or repair that cannot be performed within CA secured premises, they are securely shipped to their manufacturer.
The CA private keys are not present on HSM when it is securely shipped for maintenance or repair outside the CA secure premises. Between usages sessions, HSMs are kept securely within the CA secure premises.
The CA private keys remain under "n of m" multi-personnel control. CA custodians are assigned with the task to activate and deactivate the CA's private keys. CA's keys are then active for defined time periods.
The CA archives its own public keys and related certificates; the CA private key is not escrowed.

5.2.2 Private key (n of m) multi-person control

Protection of CA's private keys are, amongst other appropriate measures, ensured by splitting-up of a strong encryption key over several (M) tamper resistant devices (e.g., smart cards, PED keys) that are protected with multiple passphrases (shares). These tamper resistant devices meet requirements as stated in section 5.2.1.
Private keys of the CA's are not escrowed. Pixid ensures that internal disaster recovery measures are implemented.

5.2.3 Private key escrow

Key escrow is never allowed.

5.2.4 Private key backup

5.2.4.1 Pixid CA Key back-up

Pixid ensures that Pixid CA's' private keys are backed-up, stored and recovered by multiple and appropriately authorized staff serving in trustworthy positions, and witnessed by more than one representative of Pixid. More than one member of the Pixid TSP (Board) makes authorization of key back-up and of assigned personnel in writing.
Pixid CA's' private keys back-up, storage, and recovery procedures are implemented and documented in accordance with the Pixid CP and in auditable internal documents.

5.2.5 Private key archival

Not applicable.

5.2.6 Private key transfer into or from a cryptographic module

Not applicable.

5.2.7 Method of activating the private key

The CA private keys remain under N out of M multi-personnel control. CA custodians are assigned with the task to activate and deactivate the CA's private keys. CA's keys are then active for defined time periods.

5.2.8 Method of deactivating private key

The CA private keys remain under N out of M multi-personnel control. CA custodians are assigned with the task to activate and deactivate the CA's private keys. CA's keys are then active for defined time periods.

5.2.9 Method of destroying private key

At the end of their lifetime the CA private keys are destroyed by trusted CA staff members in the presence of more than one representative of the Pixid, in order to ensure that these private keys cannot ever be retrieved or used ever again.
The CA keys are destroyed through secure in a secure manner as described within documented key destruction internal procedures. Associated records are securely archived within Pixid premises.

5.2.10 Cryptographic module rating

See section 5.2.1.

5.3 Other aspects of key pair management

5.3.1 Public key archival

Pixid archives its own Pixid CA public keys. See section 4.5 for archival conditions.

5.3.2 Subscriber Certificate operational periods and key pair usage periods

Pixid issues Subscriber certificates with validity periods as indicated on such certificates, see applicable CP for further details.

5.4 Activation data

Pixid ensures that activation data associated to Pixid CA's private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of sections 4 and 5.2.

5.5 Computer security controls

Pixid ensures that computer security controls are implemented in compliance with the technical standards 46.

5.6 Life cycle technical controls

Pixid ensures that periodic development control, security management and life cycle security controls are implemented in compliance with the technical standards 46. Detailed descriptions of implemented life cycle technical controls are available as internal document(s).

5.7 Network security controls

Pixid ensures that network security controls (including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with the technical standards 46.
Detailed descriptions of implemented network security controls are available as internal document(s).

6. Compliance audit and other assessments

Not applicable.

7. Other business and legal matters

7.1 Fees

Not applicable.

7.2 Financial responsibility

7.2.1 Insurance coverage

Pixid maintains sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

7.2.2 Other assets

Not applicable.

7.2.3 Insurance or warranty coverage for end-entities

Not applicable.

7.3 Confidentiality of business information

Provisions relating to the treatment of confidential information that PKI Participants may communicate to each other, and in particular relating to the scope of what is considered as information within or not within the scope of confidential information, to the responsibility to protect confidential information, and to disclosure conditions are provided within the CP.

7.4 Protection of personal information

Pixid acting as a TSP operates within the boundaries of the General Data Protection Regulation.

7.5 Intellectual property rights

Subscribers acknowledges and agrees that Pixid and/or its licensors own all intellectual property rights in the Services and the Documentation.

7.6 Representations and warranties

7.6.1 CA representations and warranties

Pixid guarantees that all the requirements set out in the present CP are complied with.

7.6.2 Relying Party representations and warranties

The following statements must be considered and complied with by any Relying Party:

- Receive notice and adhere to the conditions of the applicable CP and of the Pixid CP and associated conditions for Relying Parties.
- Decision to rely on a certificate must always be a ***conscious*** one and can only be taken by ***the Relying Party itself based on RFC 5280***.
- Therefore, ***before deciding to rely on a certificate it is needed to be assured of its validity.*** If the Relying Party is not certain that its software performs such checks automatically, the Relying Party has to open the Certificate by clicking on it and checking that the Certificate is ***NOT*** either ***expired*** – by looking at the "valid from ___ to ___" notice; *or* ***suspended or revoked –*** by following the link to the Certificate Revocation List (CRL) and making sure that the certificate is not listed there.
- Never rely on expired or revoked certificates.
- Without prejudice to the warranties provided in the present CP, the Relying Party is wholly accountable for verification of a Certificate before trusting it.
- Without prejudice to the warranties provided in the applicable CP or in the Pixid CP, the Relying Party is wholly accountable for verification of a Certificate before trusting it.
- If a Relying Party relies on a Certificate without following the above rules, Pixid will not accept liability for any consequences.
- The Relying Party is strongly advised not to rely upon the Information contained within their client application in use (browser) as to the usage of the Certificate and to check it against the Certificate Policy if in doubt.

- If a Relying Party becomes aware of or suspects that a Private Key has been compromised it will immediately notify Pixid

7.6.3 Representations and warranties of other participants

Not applicable.

7.7 Disclaimers of warranties

7.7.1 Damages covered and disclaimers

Except as expressly provided elsewhere in the CP and in the applicable legislation, Pixid disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties.
Pixid does not warrant any software.

7.7.2 Loss limitations

To the extent permitted by law, Pixid makes the following exclusions or limitations of liability:

a. In no event shall Pixid be liable for any indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, digital signatures, or other transactions or services (including time stamping services) offered by the CP even if Pixid has been advised of the possibility of such damages.
b. In no event shall Pixid be liable for any direct, indirect, incidental, consequential or any other kind of damages, or for any loss of profits, loss of data, or other indirect, consequential or punitive damages arising from or in connection with the use or the reliance of a suspended, revoked or expired Certificate.
c. By accepting a Certificate, the Subscriber agrees to indemnify and hold Pixid and his agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, that Pixid and its agents and contractors may incur, that are caused by the use or publication of a Certificate and that arises from:
    - Falsehood or misrepresentation of fact by the Subscriber;
    - Failure by the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive Pixid or any person receiving or relying on the Certificate
    - Failure to protect the Subscribers Private Key, to use a trustworthy system, or to otherwise, take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorised use of the Subscriber's Private Key.

7.8 Limitations of liability

The liability of Pixid towards the Subscriber or a Relying Party is limited according to other sections of the CP and to the extent permitted by law.

7.9 Indemnities

Pixid assumes no financial responsibility for improperly used Certificates, CRLs, etc.

7.10 Term and termination

The CP remains in force until notice of the opposite is communicated by Pixid on its repository. Notified changes are appropriately marked by an indicated version.

7.11 Amendments

7.11.1 Procedure for amendment

The Pixid via its TSP Board is responsible for approval and changes of the CP.
The only changes that the Pixid TSP Board may make to these CP specifications without notification are minor changes that do not affect the assurance level of this CP, 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 TSP Board as identified in the CP. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.
The Pixid TSP Board shall accept, modify or reject the proposed change after completion of a review phase.

7.11.2 Notification mechanism and period

Proposed changes to the CP will be disseminated to interested parties by publishing the new document on the Pixid repository. The date of publication and the effective date are indicated on the title page of the CP.

7.11.3 Circumstances under which OID must be changed

All changes to the CP, 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 CP.
Minor changes to this CP do not require a change in the CP OID or the CP pointer qualifier that might be communicated by the CA. Major changes that may materially change the acceptability of Certificates for specific purposes may require corresponding changes to the CP OID or CP pointer qualifier.
Minor changes are indicated by version number that contains a decimal number e.g., version 1.1 for a version with minor changes as opposed to version 2.0 that addresses major changes.

7.12 Governing law and jurisdiction

The CP shall be governed by, and construed in conformity with, the French and European laws.

7.13 Compliance with applicable law

The CP and provision of Pixid PKI Services are compliant to relevant and applicable national and European laws.