Certification Policy – CA Pixid User Advanced

1.3.6.1.4.1.23876.111001.1

C1 - public

Version	Date	Modifications – Observations
0.1	16/02/2018	Création
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

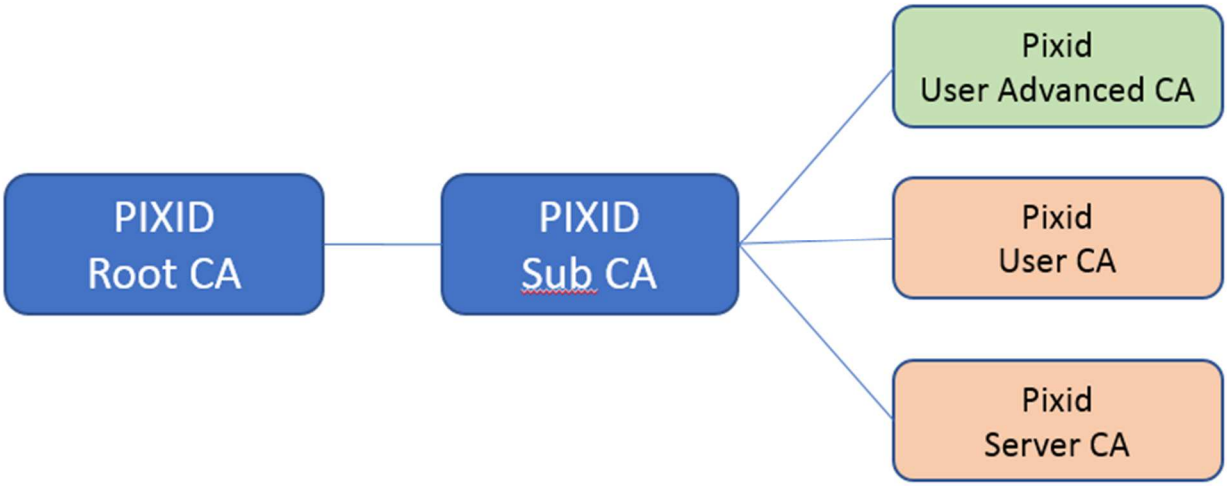
CONTENTS

1. Introduction

1.1 Overview

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.
The Pixid-services and myPixid 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 PKI provides, among others, on-the-fly certification services for the creation of advanced electronic signatures on its platforms.
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.



1.1.2 The present document

The present document contains the certificate policy (CP) and practices (CPS) for Pixid's Users CA ("CA Pixid User Advanced"), which produces end-users certificates. Throughout this document, the use of the term "CP" refers to the present document, unless otherwise specified.
The CP describes the practices of the "User Advanced" CA.

1.2 Document name and identification

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

1.3.6.1.4.1.23876.111001.1

1.3 Policy administration

See 1.

1.4 PKI Participants

The PKI Participants within Pixid PKI are:

- Certification Authorities
- Registration Authorities
- Subscribers
- Relying Parties

The aforementioned parties are collectively called the PKI Participants. All PKI Participants implement practices, procedures and controls conforming to the requirements expressed within this CP.

1.4.1 Certification Authorities

See [o]; the legal person (organization) responsible for these CA's is Pixid.

1.4.2 Registration Authorities

The registration authorities are organized as follows:

Entity	Role	For
Pixid	Registration Authority (RA)	Themselves, Suppliers, Customers and resources
Suppliers	Delegate Registration Authority (DRA)	Themselves, Customers and resources
Customers	Delegate Registration Authority (DRA)	Themselves and resources

1.4.2.1 Registration Authority (RA)

Pixid operates as the RA for suppliers, customers and workers.

1.4.2.2 Delegated Registration Authority (DRA)

All DRA's have to sign a contractual agreement with Pixid. The contract includes the DRA's obligation relating to this policy. Suppliers designate to Pixid at least one administrator, who is responsible for the verification of the identity of signers (customers and resources).

1.4.3 Subscribers

1.4.3.1 Suppliers' employees

Suppliers are temporary employment agencies, whose staff (physical persons) uses the certificates to sign contracts or authenticate themselves on one of the Pixid portals.
Suppliers are represented by one or more administrators (formally designated physical persons), who act as Delegated Registration Authorities.

1.4.3.2 Customers' employees

Customers are companies, organizations, administration, etc., whose staff (physical persons) uses the certificates to sign contracts or authenticate themselves on one of the Pixid portals.
Customers are represented by one or more administrators (formally designated physical persons), who act as Delegated Registration Authorities.

1.4.3.3 Resources

Resources are workers (physical persons) who use the certificates to sign contracts or authenticate themselves on one of the Pixid portals.

1.4.4 Relying Parties

Relying Parties are entities including physical or legal persons who rely on a Certificate and/or a security operation verifiable with reference to a public key listed in a Certificate. Relying Parties shall comply with the Relying Parties obligations and liabilities as stated in the relevant sections of this CP.
Note: Relying Parties are entities that are not necessarily Subscribers.

1.5 Certificates usage

1.5.1 Appropriate certificate usages

Appropriate certificate usages are explicitly described in the certificates themselves, using the *Key Usage* extension. The certificates issued under the present policy are to be used exclusively for electronic signatures or authentication on Pixid platforms.

1.5.2 Prohibited certificate usages

Usage of certificates other than the ones mentioned in the previous paragraph is prohibited. Relying Parties shall use the OID as identified in the certificate to appropriately accept or reject a certificate usage.

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. 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.

1.6.2 Definition

Advanced Electronic Signature	Refers to Electronic Signature which meets the requirements set out in Article 26 of the EIDAS Regulation 2.
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.
Customer	see 1.4.3.2
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 2.
Resource	see 1.4.3.3
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.
Supplier	see 1.4.3.1
Trusted Third Party (TTP)	Authority trusted (and widely recognized, 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.

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 (1.4.2.2)
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 Trust Service Provider
TSU Time Stamping Unit
URL Uniform Resource Locator
UTC Coordinated Universal Time

2. Publications and Repository Responsibilities

2.1 Identification of entities operating repositories

See 1.

2.2 Publication of Certification Information

The Pixid CP covering the practices used by the CA for Certificates issuance under this 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 Pixid User Advanced CA publishes revocation status information at the following URL: **https://pki.mypixid.io/.**
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.

2.3 Time of Frequency of Publication

2.3.1 Frequency of Publication of Revocation information

The Pixid User Advanced CA publishes its CRL at least once every 6 (six) days.

2.3.2 Frequency of Publication of Terms & Conditions

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

2.4 Access Control on Repositories

See 1.

3. Identification and authentication

3.1 Naming

3.1.1 Types of names

Naming and identification rules for physical (private) persons are the same as legal rules applied for naming and identification of physical persons on citizen identity cards, passports or other official documents.
The certificates' distinguished names (DN) are structured as follows:

Country (C)	`FR` (fixed value)
SerialNumber	(random unique value)
GivenName (GN)	Given name of the subject
SurName (SN)	Surname of the subject
Common Name (CN)	GivenName and SurName, separated by a single space

3.1.2 Anonymity or pseudonymity of Subscribers

Not applicable.

3.1.3 Rules for interpreting various name forms

Not applicable.

3.1.4 Uniqueness of names

The full combination of the subject's attributes (Distinguished Name) has to be unique. This is guaranteed by the SerialNumber attribute.

3.1.5 Recognition, authentication, and role of trademarks

No requirement.

3.2 Initial identity validation

3.2.1 Suppliers's members

Suppliers are initially registered by Pixid (acting as the RA) following the signing of the commercial contract between the two parties. One or more administrators are designated by Pixid's client with the following information:

- First and last names
- Date and place of birth
- Reference to a nationally recognized identity document, which provides the previous information (name, date and place of birth)

- Professional email address
- Professional phone number
- SIRET, EU TVA number or national identification number of the supplier, as it appears in the contract with Pixid.

The administrators are DRA for their organization, customers and resources.

3.2.2 Customers's members

Customers could be initially registered by a Supplier (acting as a DRA) or by Pixid (acting as the RA). When the Customer is registered by Pixid, it's following the signing of a commercial contract between the two parties. One or more administrators are designated by Pixid's client with the following information:

- First and last names
- Date and place of birth
- Reference to a nationally recognized identity document, which provides the previous information (name, date and place of birth)
- Professional email address
- Professional phone number
- SIRET, EU TVA number or national identification number of the customer, as it appears in the contract with Pixid.

The administrators are DRA for their organization and resources.

3.2.3 Customers's identity validation by the DRA

When validating a customer's identity, the DRA follows the same procedure as the RA. The customer's administrator is also a DRA for its employees and resources.

3.2.4 Resources's identity validation by the RA

Resources (individual workers) may register themselves on myPixid web site by providing the following information:

- First and last names
- Date and place of birth
- Digital scan of a nationally recognized identity document, which provides the previous information (name, date and place of birth)
- Personal email address
- Personal phone number

3.2.5 Resources's identity validation by the DRA

When validating a resource's identity, the DRA follows the same procedure as the RA.

3.2.6 Method to prove possession of private key

Private keys are managed by the CA on the behalf of the certificate holders.

3.2.7 Authentication of organization identity

Not applicable.

3.2.8 Unverified subscriber information

Not applicable. Certificates do not contain unverified information.

3.2.9 Validation of authority

Not applicable.

3.2.10 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key & update requests

Not applicable.

3.4 Identification and authentication for revocation request

Revocation requests are sent by e-mail. Control of the subscriber's e-mail address, as provided during the initial identity validation, is deemed sufficient for the authentication of the request.

4. Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any users authenticated on myPixid website may request a certificate for himself/herself.

4.1.2 Enrolment process and responsibilities

For provision of services, the CA assumes full responsibility and accountability for acts or omissions of all third party agents it uses to deliver certification services.
Within the context of new Subscriber registration, the RA and DRA responsibility is to verify that the Subscriber is indeed the person (s)he claims to be and to validate the information that is requested to be certified by the CA as well as the information supporting this certification.
The Subscriber will have to proceed to a valid initial identification and authentication as described in section 3.2. The RA or DRA guarantees the accuracy of all information provided to the CA.

4.1.2.1 Suppliers' members enrolment process

Suppliers' signers enroll themselves to their DRA (Supplier's administrator). Following the successful initial identification and authentication as described in section 3.2, they are declared online by the DRA using a secure channel ensuring the authenticity, confidentiality and integrity of the transmitted data.

4.1.2.2 Customers' members enrolment process

Customers' signers enroll themselves to their DRA (Supplier's or Customer's administrator). Following the successful initial identification and authentication as described in section 3.2, they are declared online by the DRA using a secure channel ensuring the authenticity, confidentiality and integrity of the transmitted data.

4.1.2.3 Resources' enrolment process

Resources enroll themselves either directly to the RA (using myPxid website) or to the DRA (Supplier's or Customer's administrator) of the entity they need to contract with. Following the successful initial identification and authentication as described in section 3.2, they are declared online by the DRA using a secure channel ensuring the authenticity, confidentiality and integrity of the transmitted data.

4.1.2.4 PKI Participants responsibilities related to enrolment process

4.1.2.4.1 Subscribers' responsibilities

The Subscriber agrees with and accepts the General Terms and Conditions and the CP. Specifically, the Subscriber hereby gives his/her acceptance to the following responsibilities related to the enrolment process:

- The information submitted during enrolment process by the Subscriber must be valid, up-to-date, accurate, and complete. The Subscriber is responsible for the accuracy of the data provided during enrolment process and the RA or DRA will ensure the correctness and accuracy of the submitted information.
- The Subscriber must agree to the retention (for a period of 7 years from the date of expiry of the last Subscriber Certificate) by the CA, RA and DRA, of all information used for the purposes of registration; in the event that the CA ceases its activities, the Subscriber must also consent for this information to be transmitted to third parties under the same terms and conditions as those laid down in this CP.

4.1.2.4.2 RA and DRA responsibilities

The RA (DRA) guarantees that:

- Subscribers are properly identified and authenticated both with regard to the personal identity of the Subscriber as a natural private person.
- Any application for Certificates submitted to the CA is complete, accurate, valid and duly authorised.
- The RA/DRA informs the Subscriber of the terms and conditions for the use of the Certificate.
- The RA/DRA checks the identity of the Subscriber on the basis of valid identity documents recognised under national law or equivalent measures according to national law. These identity documents must indicate the full name (last name and first names), date and place of birth.

The RA/DRA ensures the storage of at least one copy of the information provided by the Subscriber during enrolment process, in particular:

- A copy of all information used to check the identity of the Subscriber, including any reference numbers on documentation used for this verification as well as any limitations on its validity.
- This information is retained by the RA/DRA for a period of 7 (seven) years from the date of expiry of the last Certificate linked to the Subscriber's registration.
- The RA/DRA ensures compliance with the requirements relating to the processing of personal data and the protection of privacy with respect to the Subscriber enrolment process.
- The RA/DRA guarantees that these items are managed and stored in such a way as to avoid any repercussions as a result of a loss of confidentiality, integrity as well as availability of this data.

4.2 Certificate application processing

Certificates requests are submitted online by enrolled and authenticated users during a signing process on one of the Pixid Platforms. Users must successfully authenticate themselves using a two-factor authentication means (password and OTP); the request is then approved and sent to the CA.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA authenticates certificate requests and only accept requests sent through a secure channel ensuring authenticity and integrity of the request.

4.3.2 Notification by the CA of the issuance of Certificate

Users are not notified of the certificate issuance. However, the certificates' contents (DN) is displayed to the user during the signing process, and before the application of the signature to the documents.

4.4 Certificate acceptance

The Certificate is deemed to be accepted by the Subscriber if he/she completes the signing process.

4.4.1 Publication of the Certificate by the CA

Certificates are not published by the CA.

4.4.2 Notification of Certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

By signing with the certificate, the Subscriber gives his/her acceptance to the following responsibilities related to the Subscriber private key and Certificate usage:

- In using the Key Pair, the Subscriber must comply with any limitations indicated in the Certificate, this CP, or in applicable contractual agreements.
- The Subscriber must protect its Activation Data at all times against compromise, loss, disclosure, alteration or any otherwise unauthorised use. The Subscriber is the sole user of the Private Key.
- The Subscriber has sole liability for the use of the Private Key.
- The Subscriber must ask the CA to revoke the Certificate as required pursuant to this CP, in particular if:
- The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data has been compromised or for any other reason; and/or,
- The certified data has become inaccurate or has changed in any way (e.g., if the information submitted during the enrolment process as proof of professional status becomes obsolete, in full or in part)
- The Certificate revocation process is then started immediately.
- The Subscriber must inform the CA of any changes to data not included in the Certificate but submitted and registered during the enrolment process.

4.5.2 Relying Party public key and Certificate usage

Relying Parties providing services or directly relying on Certificates issued in accordance with this CP must perform the following and assume the responsibility for having performed the following:

- Successfully perform public key operations as a condition of relying on a Certificate, compliant with RFC 5280.
- Validate a Certificate by using the CA's Certificate Revocation Lists (CRLs) OCSP or web based Certificate status services in accordance with the Certificate path validation procedure
- Un-trust a Certificate if it has expired has been suspended or is revoked.
- Rely on a Certificate only for appropriate applications (and context) as set forth in this CP, taking into account all the limitations on the use of the Certificate specified in the Certificate, the applicable contractual documents and this CP.
- Take all other precautions with regard to the use of the Certificate as set out in this CP or elsewhere, and rely on a Certificate as may be reasonable under the circumstances.

4.6 Certificate renewal

Not applicable.

4.7 Certificate re-key

Not applicable.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation

4.9.1 Circumstances for revocation

The Subscriber and, when applicable, the organisation for which the Subscriber (or Subject when Subject and Subscriber are different entities) is certified (as stated in the Certificate), must ask the CA to revoke the Certificate in the following cases:

- The Private Key of the Subscriber is lost, stolen or potentially compromised; or,
- The Subscriber no longer has "sole" control of the Private Key because the Private Key Activation Data has been compromised or for any other reason; or,
- The certified data has become inaccurate or has changed in any way (e.g., if the information submitted during the enrolment process as proof of professional status becomes obsolete, in full or in part).

The RA/DRA will request the revocation of a Certificate after having received notice by the Subscriber, or when applicable, by the Subscriber's organisation.

4.9.2 Who can request revocation

Revocation can be requested by the Subscriber, by the Subscriber's organization, and by the RA/DRA.

4.9.3 Procedure for revocation request

Certificate revocation requests must be sent by e-mail at the following URL: revocation@mypixid.eu
Applications and reports relating to a revocation are processed on receipt and are authenticated as described in 3.4.

4.9.4 Time within which CA must process the revocation request

The investigation of the Certificate revocation request shall begin within twenty-four (24) hours of receipt.

4.9.5 Revocation checking requirement for Relying Parties

Relying Parties must use online resources that the CA makes available through its repository to check the status of a Certificate before relying on it.

4.9.6 CRL issuance frequency

See [2.3.1].

4.9.7 On-line revocation/status checking availability

Not applicable.

4.9.8 Special requirements regarding key compromise

Not applicable.

4.10 Certificate status services

See [2.3.1].

4.11 End of subscription

Subscription termination is subject to appropriate clause within the Subscriber Agreement (e.g., in the General Terms and Conditions). End of subscription is materialised by the expiration or the revocation of any Certificate belonging to the Subscriber.

4.12 Key escrow and recovery

Not applicable.

5. Facility, management, and operational controls

See 1.

6. Technical security controls

See 1 for CA Key Pair and Certificate management. The current section only refers to Subscribers' Key Pair and Certificates.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The generation and storage of Subscribers' private keys occurs within a secure cryptographic device.

6.1.2 Key sizes

Subscribers' Private Key Type

	RSA Key size	Hash algorithm
Subscriber	2048	SHA256

6.1.3 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.

6.1.4 Key usage purposes

See [1.5].

6.2 Private key protection

6.2.1 Cryptographic module standards and controls

The Subscribers' HSM follow the same requirements, standards and controls as the ones used for the CA. See 1.

6.2.2 Private key escrow

Key escrow is never allowed.

6.2.3 Private key backup

Not applicable to Subscribers' keys.

6.2.4 Private key archival

Not applicable to Subscribers' keys.

6.2.5 Private key transfer into or from a cryptographic module

Not applicable to Subscribers' keys.

6.2.6 Method of activating the private key

A Subscriber's private key can only be activated by its owner, using bi-factor authentication. Technical and organizational security measures ensure that, during its lifespan, a Subscriber's private key cannot be used by a third-party.

6.2.7 Method of deactivating private key

Subscribers' keys cannot be deactivated.

6.2.8 Method of destroying private key

Subscribers' keys are automatically destroyed (erased from the HSM) as soon as possible and after 45 minutes maximum.

6.2.9 Cryptographic module rating

See section [6.2.1].

6.3 Other aspects of key pair management

6.3.1 Public key archival

Not applicable to Subscribers' keys.

6.3.2 Subscriber Certificate operational periods and key pair usage periods

Subscriber certificates' validity period is 45 minutes. For key pair usage period, see 6.2.8.

6.4 Activation data

Activation data is randomly generated whenever the Subscriber needs to sign a document on the myPixid platform (OTP).

6.5 Computer security controls

See 1.

6.6 Life cycle technical controls

See 1.

6.7 Network security controls

See 1.

7. Compliance audit and other assessments

See 1.

8. Other business and legal matters

See 1 for general business and legal matters. The current section only refers to the business and legal matters specifically pertaining to the Pixid User Advanced CA.

8.1 Fees

Save the access to the CRL and OCSP services, which is public and free, the cost of the CA's services are outside the scope of the present policy.

8.2 Financial responsibility

8.2.1 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.

8.2.2 Other assets

Not applicable.

8.2.3 Insurance or warranty coverage for end-entities

Not applicable.

8.3 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.

8.4 Protection of personal information

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

8.5 Intellectual property rights

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

8.6 Representations and warranties

8.6.1 CA representations and warranties

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

8.6.2 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 this 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 this 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.

8.6.3 Representations and warranties of other participants

Not applicable.

8.7 Disclaimers of warranties

8.7.1 Damages covered and disclaimers

Except as expressly provided elsewhere in the CP and in the applicable legislation, Pixid S.A.S 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.

8.7.2 Loss limitations

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

- 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.

- 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.
- 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 unauthorized use of the Subscriber's Private Key.

8.8 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.

8.9 Indemnities

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

8.10 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.

8.11 Amendments

8.11.1 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.

8.11.2 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.

8.11.3 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.

8.12 Governing law and jurisdiction

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

8.13 Compliance with applicable law

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