# Individuals' advanced electronic signature with centralized custody Policy

## Table of Contents

# 1. Introduction

## 1.1. General description

This Policy is elaborated pursuant to Decree No. 70/018 dated March 19, 2018, [1] which regulates sections 31 to 33 of Law No. 18,600 dated September 21, 2009 [2], in the wording given by section 28 of Law No. 19,535 dated September 25, 2017, as regards digital identification trust services and advanced electronic signature with centralized custody, for the purposes of regulating Trust Service Providers (TSPs).

The document determines the management, administrative and technical aspects which shall be considered by Trust Service Providers (TSPs) when providing services of generation and storage of certificates and signatures of individuals.

The purpose of this Policy is to ensure that the electronic signature creation and storage device is reliable, and that signatory has, with a high level of confidence, exclusive access to his or her advanced electronic signature key under centralized custody for individuals.

These services will allow document signing while avoiding the usage of additional devices for signing, such as Tokens or identity card readers. For these purposes, Trust Service Providers will store certificates and private keys for individuals and will provide online signatures with the prior authorization of the holder.

This document was prepared pursuant to the rules and regulations in force, the guidelines for documentation of Policies and Certification Practice Statement set forth in RFC 3647 [3] and the Certification Policy for Individuals [4].

This Policy describes a new way to issue certificates for individuals, along with considerations for use, generation and storage thereof. If any inconsistencies exist between this Policy and the definitions under the Certification Policy for Individuals [4], the latter [4] shall prevail.

## 1.2. Name of the document and identification of the Certification Policy

Name: Individuals' advanced electronic signature with centralized custody Policy.
Version: 1.1.
Elaboration date: June 15, 2018.
Last update date: August 15, 2018.
OID: 2.16.858.10000157.66565.12
Website of publication: http://www.uce.gub.uy/informacion-tecnica/politicas/cp_persona_fisica_centralizada.pdf

## 1.3. INCE's participants

### 1.3.1. Regulatory Unit

The Regulatory Unit role is carried out by the Digital Certification Unit (UCE), pursuant to Law No. 18,600 dated September 21, 2009 [2]. It is a regulatory role, whereby technical and operational standards to be observed by Authorized Credential Service Providers (ACSPs) and TSPs, as well as certification procedures and requirements shall be defined.

Apart from its regulatory role, the UCE carries out functions such as: certification of Credential Service Providers; control and auditing of their activity; training based on general criteria and assessment of good working practices; application of sanctions in case of nonobservance. More detailed information can be found in ACRN's Certification Policy [5] and section 14 of Law No. 18,600 dated September 21, 2009 [2].

### 1.3.2. Subscribers

In the context of this Policy, Subscribers are individuals to whom a TSP has issued one or more certificate for individuals of the National Infrastructure of Digital Certification (NIDC) - PKI Uruguay, through an ACSP. The TSP provides Subscriber the advanced electronic signature service with the certificate for individuals under centralized custody.

Subscribers may use certificates for Individuals for the purposes of authentication, Advanced Electronic signature and encryption.

Subscribers acquire rights and obligations when using certificates for Individuals pursuant to the Certification Policy for Individuals [4].

## 1.4. Use of certificates

Authorized uses and restrictions regarding certificates issued under this Policy are defined in the Certification Policy for Individuals [4].

## 1.5. Certification Policy Management

Management of this Policy shall correspond to the UCE.

For comments or suggestions, the UCE provides the following contact details:
Name: *Unidad de Certificación Electrónica* (Digital Certification Unit)
Email: info@uce.gub.uy
Phone: (+598) 2901 2929

## 1.6. Connection between the Certification Policy and other documents

This Policy is based on Law No. 18,600 [2], in the wording given by section 28 of Law No. 19,535, Decree No. 436/011 dated December 8, 2011 [6], Decree No. 70/018 [1], and the Certification Policy for Individuals [3]. The legislation in force and the specific provisions adopted by the UCE shall always prevail.

All requirements defined in this Policy must be followed by Trust Service Providers (TSPs) and specified in their Certification Practice Statement.

This Policy affects the Information Security Policy and administrative procedures of Trust Service Providers (TSPs).

## 1.7. Approval of the Policy

This policy's approval, as well as the approval of any amendments hereto, shall be the UCE's sole responsibility. UCE shall apply its internal document management procedures in order to guarantee the quality and traceability of the amendments. The amended Policy shall be published as a new version, and record of the date and effected changes shall be kept.

## 1.8. Definitions and abbreviations

The general definitions and abbreviations of the National Infrastructure of Digital Certification (INCE) are defined in Law No. 18,600 [2]. Nonetheless, the following definitions and abbreviations shall be used herein and are therefore mentioned hereinbelow:

**Authenticator Assurance Level 2 (AAL2):** It represents a specific assurance level for digital authentication, as defined by the National Institute of Standards and Technology (NIST) [7]

Said level provides a high degree of trust, as regards the fact that an applicant for digital authentication holds the digital or electronic identification means which were assigned to applicant during the digital identification registration process.

**Digital authentication:** The process of identifying a person through a computer system using one or more digital identification means.

**Credential Provider Certifying Authority (CAPA):** group of systems, personnel, policies and procedures that the ACSP uses to issue certificates to end users pursuant to certification policies.

**National Root Certifying Authority (NRCA):** set of computer systems, personnel, policies and procedures which, in the INCE's structure through inheritance, constitute the trusted root. It allows to certify other entities in charge of issuing certificates within the INCE.

**Registration Authority (RA):** In the context of this policy, the registration authority is responsible for registration and prosecution of the applications for issuance, renewal, and revocation of certificates, including validation of the application subscriber's identity at the beginning of the process.

**Digital Certificate (DC):** Electronic document, digitally signed, which attests to the relationship between the signatory or certificate holder and the data of creation of the electronic signature.

**Recognized Digital Certificate (RDC):** Digital certificate issued by the NRCA or by an ACSP through one of their CAPAs.

**Recognized Individual Digital Certificate (RIDC):** Recognized Digital Certificate, the subscriber of which is an Individual, issued exclusively by an ACSP and subject to the requirements of this Certification Policy.

**Certification Practice Statement (CPS):** Statement of the practices that a certifying entity employs for managing the certificates that such entity issues (issuance, revocation, renewal, etc.)

**Secure Signature Creation Device or Module (SSCD):** device which protects the subscriber's keys and certificates, used to generate subscriber's electronic signature and which ensures, at a minimum:

a) Data used for signature generation can only be created once and is kept confidential;

b) There is reasonable expectation that data used for signature generation cannot be discovered through inferences, and that the signature is protected against forgery through current available technology, being possibility to detect any subsequent alteration.

c) Data used for signature generation can be safely protected by the signatory against third-party use.

**Federal Information Processing Standard (FIPS) 140 level 3:** computer security standard of the U.S. Government for certification of cryptographic modules. In level 3, it ensures modules are resistant to physical intrusion.

**Advanced electronic signature under centralized custody:** Advanced electronic signature where the signatory's private key is under the custody of an ACSP who makes the signature upon express order of the signatory.

**National Infrastructure of Digital Certification (NIDC):** set of computer equipment and software, cryptographic devices, policies, rules and procedures set for the generation, storage and publication of recognized certificates, as well as for the publication of information and enquiry as to the validity and effect of said certificates.

**Electronic or digital identification means:** Material or immaterial unit that can be processed by a computer system, a part of which is controlled by the system while the other part is exclusively controlled by the individual through:

a) The individual's knowledge;
b) A physical or logical device;
c) A physical or behavioral feature.

**Hardware Security Module (HSM):** cryptographic device based on hardware that generates, stores and protects cryptographic keys.

**Authorized Credential Service Provider (ACSP):** Individual or legal person certified by the UCE and responsible for the operation of at least one of NIDC's Credential Authorities.

**Trust Service Provider (TSP):** Individual or legal person, public or private, national or foreign, that provides one or more trust services.

**Certificate Policy (CP):** a group of policies which indicate the applicability of a certificate to a particular community and/or class of application with common security requirements, and also define the requirements to be observed by any provider in order to work with this kind of certificate. In the context of NIDC, these policies are proposed, approved and maintained by the UCE.

**Digital identity registration:** The process of authenticating a person, proofing the person's data, issue or associate one or more digital identification means thereto, and store said association for subsequent use.

**Trust Services:** Digital services that provide legal security to facts, actions and transactions carried out or registered through digital means, such as:

a) Advanced electronic signature with centralized custody services;
b) Digital identification services;
c) Timestamping services;
d) Other services established by the Digital Certification Unit.

**Digital identification services:** Services that create digital authentication registers of persons for third-party verification.

**Certificate Signing Request (CSR):** in the context of this policy, it is a message issued by an individual under the standard PKCS#10 through which individual requests and provides information to a CAPA for the issuance of a certificate signed by such CAPA.

# 2. General aspects of the Certification Policy

## 2.1. Responsibilities

### 2.1.1. Responsibilities of the UCE

In addition to the obligations defined in NRCA's Certification Policy, the UCE shall be responsible for:

a) Certifying Credential Service Providers who request their registration with the registry of Trust Service Providers and comply with the requirements set forth herein.

b) Controlling the admissibility of applications pursuant to section 15 of Decree No. 436/011 [6].

c) After the certification application is technically approved, applicant shall be notified thereof and shall have 20 calendar days as from the day following such notice to provide the security set forth by section 17 of Law No. 18,600 [2]. Such security shall be obtained through purchase of civil liability insurance for the purposes of assuming the risk of liability for damages which may be caused by the applicant's services.

d) Certifying the applicant for the term determined by the UCE. Said certification shall be subject to the required inspections and audits.

### 2.1.2. Responsibilities of the Authorized Credential Service Providers Registration Authorities

These are defined in the Certification Policy for Individuals [4] under section 2.1.3.

### 2.1.3. Responsibilities of Trust Service Providers

TSPs shall be responsible for:

a) Diligently safeguarding a signatory's private key and providing the means for its generation, protection and destruction pursuant to this policy.

b) Establishing safe procedures to stamp electronic signatures upon request of the signatory pursuant to this policy.

c) Possessing safe procedures for the digital authentication of individuals, observing the technical requirements defined herein.

d) Providing individuals with control and traceability procedures regarding use of their advanced electronic signature private key under custody.

e) Providing a signature service to individuals for the use of the individuals' advanced electronic signature under centralized custody.

f) Possess integration documentation for developers with signature service at no cost.

### 2.1.4. Responsibilities of Certificate Subscribers

In the context of this Certification Policy, subscribers are Individuals, national or foreign citizens, of legal age, who shall have the responsibilities mentioned in this section.

Subscribers of Certificates for Individuals shall have the following responsibilities in addition to the responsibilities set forth by the Certification Policy for Individuals:

a) To protect the data related to identification and authentication for the use of advanced electronic signature under centralized custody.

b) To request immediate revocation of the certificate issued by a TSP if the digital identification means are or appear to be compromised.

### 2.2. Liability

The liability of accredited TSPs shall be governed by the provisions for Credential Service Providers under section 20 of Law N° 18,600 [2]

### 2.3. Fees

TSPs which provide custody of centralized keys, pursuant to this Policy, may receive an economic compensation for their services.

## 3. Accreditation of Trust Service Providers

In the context of this Policy, TSPs may be accredited to offer the “Generation, storage and signature of individuals” service.

In order to be an accredited TSP, it is absolutely necessary:

a) To be an individual or legal entity incorporated in the country, to provide a security and have sufficient solvency for providing the services.

b) To have qualified personnel, with the required knowledge and experience for providing the trust services offered, and with suitable security and management procedures.

c) To follow standards and use suitable tools according to the provisions of the Digital Certification Unit.

d) To be domiciled in the Oriental Republic of Uruguay, a requirement that shall be

considered fulfilled when technological infrastructure and other material and human resources are located in Uruguayan territory.

Credential Service Providers accredited by the UCE may request their registration with the Registry of Trust Service Providers in order to offer the “Generation, storage and signature of individuals” service. In such case, they shall prove compliance with the specific requirements set forth in this Policy.

The accreditation procedure of Generation, Storage and Signature Services Providers shall be conducted pursuant to Law N° 18,600 [2] and Chapter V of Decree N° 436/011 [6].

# 4. Application for an Individual’s advanced electronic signature under centralized custody service certificate.

The terms of a certificate for individuals application are defined under the Certification Policy for Individuals [4] under section 4.1. In the context of this policy, additional terms are defined for application for an individual’s advanced electronic signature under centralized custody certificate.

## 4.1. Registration of Certificate Applications

An application for a certificate for individuals may be initiated in person or remotely (web, mail, etc.) pursuant to the decision of each TSP. In any case, the TSP must document the certificate application and initiate its issuance internal procedures.

For the certificate application procedure or the renewal procedure, applicant shall appear in person to validate his or her identity and documentation, pursuant to section 3.1.2 of the Certification Policy for Individuals [4].

In addition to the methods described under the Individual Policy [4] under section 4.1.2, this Policy defines a new method of key generation for Individuals:

- *Centralized* – the key pair and the CSR are generated by the TSP within its facilities. In this method, the TSP shall generate Applicant’s private key in its cryptographic module (HSM) with centralized custody. The PIN or password that protects the private key will be entered by the Applicant and will be under his or her exclusive control. Storage of the private key generated for Applicant is not allowed in any means other than the device where it was generated. During the private key generation process, digital identification registration shall be carried out, and at least two digital identification means (see section 6.2) shall be associated to the

certificate Applicant. Issuance of the Certificate shall be conducted pursuant to the ACSP issuance procedures.

The TSP shall document the specific procedures carried out to ensure Applicant's private key was generated in its cryptographic module (HSM) under centralized custody, and the Applicant's exclusive control over the PIN or password that protects the use of the generated private key.

The TSP must inform Applicant of the importance of the PIN and the digital identification means for protection of the use of his or her private key, and shall provide guidelines for a safe use.

As part of the certificate application process, Applicant must sign the Terms for Advanced Electronic signature Utilization [8]. This agreement, worded by the TSP, will have a record of Applicant's adherence to this Certification Policy and to other applicable regulations issued by the UCE. If Applicant does not sign this Agreement, the certificate issuance procedure shall not continue.

## 5. Certificate Profile

Certificates for advanced electronic signature under centralized custody are issued with QCCompliance attribute within QcStatement extension in compliance with ITU-T X.509 version 3 standard (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), defined in its latest version under RFC 5280 [10].

This attribute inclusion refers to a statement of the issuer, which states the qualification of the certificate issued, in this case complying with the terms set forth in this Policy.

Within the framework of this Policy, the Certificate for individuals Profile defined in section 7.1 of the Certification Policy for Individuals [4] is modified to include the abovementioned attribute.

| Attributes | Content |
|---|---|
| Version | V3 |
| Serial Number | Number assigned by the issuing CAPA |
| Signature Algorithm | sha256RSA |
| Issuer DN | CAPA's DN as shown in its certificate |
| Valid From / Valid To | 0 to 2 years (from-to) |
| Subscriber DN | CN = Individual's full name<br>C = Country of the identity document submitted<br>serialNumber = Document number and code<br>givenName = Individual's Names separated by a comma<br>surname = Individual's Surnames separated by a comma.<br>(See section 3.1.1.1) |
| Subject Public Key | 2048 or more bits RSA Public Key |

| Extensions | |
|---|---|
| Subject Key Identifier | Subject Public Key attribute 20 bytes hash |
| Authority Key Identifier | Subject Key Identifier Extension Value of the issuing CAPA's certificate |
| Key Usage | DigitalSignature = 1<br>NonRepudiation/contentCommitment = 1<br>KeyEncipherment = 1<br>DataEncipherment = 1<br>KeyAgreement = 0<br>KeyCertSign = 0<br>CRLSign = 0<br>EncipherOnly = 0<br>DecipherOnly = 0 |
| Extended Key Usage | clientAuth, emailProtection |

| | |
|---|---|
| Certificate Policies | **OID: 2.16.858.10000157.66565.12**<br><br>**URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_persona_fisica_centralizada.pdf**<br><br>**OID: OID assigned to ASCP CPS for the issuing CAPA**<br><br>**URI: URL where CPS is published** |
| Basic Constraints | CA = FALSE |
| CRL Distribution Points | URI = Primary URL where CRL is published<br><br>URI = Secondary URL where CRL is published |
| QCStatements | Id-etsi-qcs-QcCompliance<br>Id-etsi-qcs-QcSSCD |

During the certificate generation, the CAPA shall consider inclusion of this attribute, and acknowledge application comes from an accredited TSP which complies with the requirements set forth herein.

In addition, if biometric verification was conducted at the registration phase pursuant to section 4.1.2.1 Certification Policy for Individuals Registration with additional biometric verification [4], OID 2.16.858.10000157.66565.13shall be included as follows:

| | |
|---|---|
| Certificate Policies | **OID: 2.16.858.10000157.66565.12**<br><br>**URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_persona_fisica_centralizada.pdf**<br><br>**OID: OID assigned to ASCP CPS for the issuing CAPA**<br><br>**URI: URL where CPS is published**<br><br>**OID: 2.16.858.10000157.66565.13**<br><br>**User Notice: Biometric verification** |

# 6. Advanced electronic signature with centralized custody service

In addition to generation and storage of individuals' private keys, the TSP shall provide the signature service that allows subscribers to use their advanced electronic signature private key under centralized custody.

The signature service offered by the TSP must establish safe mechanisms to stamp electronic signatures only upon signatory's request.

A series of technical considerations for the signature service that allows use of advanced electronic signature private key under centralized custody follows below.

## 6.1. Signature Service

The service shall be developed taking into account international standards for safe development, e.g. OWASP [9].

The TSP shall possess documentation for developers for integration to their signature service. The TSP shall define the terms for its use and/or integration.

Regardless of the signature service implementation, exclusive control of the signatory over his or her advanced electronic signature private key under custody must be ensured at all times.

## 6.2. Subscriber's Authentication

During the certificate application procedure defined under section 4, the digital identification means for digital authentication required by the signature service are associated to Applicant.

The TSP shall ensure an assurance level in the digital authentication procedure equal to or higher than AAL2 defined by the NIST [7], therefore providing a high level of confidence, where the person applying for digital authentication for the use of his or her private key under centralized custody, possesses the digital identification means associated to him or her during the digital identification registration of the certificate application.

Safe digital identification means shall be those defined by the UCE observing the digital identity guidelines document of the NIST [7].

## 7. Private Keys Protection

A TSP must observe the following requirements along with the requirements defined for an ASCP issuing Individual Certifications pursuant to the Certification Policy for Individuals [4].

a) Individual's advanced electronic signature private keys under custody of a TSP shall be generated and stored in cryptographic modules (HSM) which comply with FIPS 140-2 level 3 rules and regulations.

b) The password or PIN to access an individual's advanced electronic signature private key under custody must always be protected by cryptographic modules (HSM) which comply with FIPS 140-2 level 3 rules and regulations and shall be under the exclusive control of the individual.

## 8. Private Key Migration

An Individual's advanced electronic signature private key may not be migrated between different Trust Service Providers, and the storage means may not be modified for the same provider.

## 9. Suspension and revocation of Trust Service Providers accreditation

Suspension and revocation of TSPs accreditation for generation, storage and advanced electronic signature, as well as the effects thereof, shall be governed by the rules of the ACRN's Certification Policy [6] for Credential Service Providers ([5].

## 10. Cessation of activities of accredited Trust Service Providers

Accredited TSPs for generation, storage and advanced electronic signature which cease their activities must communicate said cessation through the Official Gazette and other digital or traditional means they may deem convenient.

In addition, the service provider must continue to offer the service for reception of revocation applications or refer such service, and must continue to update and publish in the updated Registry of revoked certificates until expiration of the last certificate.

# External References

1. Executive Branch, Oriental Republic of Uruguay. Decree N° 70/018 dated March 19, 2018. Regulation of sections 31 to 33 of Law N° 18,600.
2. Legislative Branch, Oriental Republic of Uruguay. Law No. 18,600, dated September 21, 2009. Electronic Documents and Electronic signatures.
3. Chokhani, Ford, Sabett, Wu, RFC 3647 - Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework, 2003.
4. *Unidad de Certificación Electrónica* (Digital Certification Unit), Certification Policy for Individuals, 2015.
5. *Unidad de Certificación Electrónica* (Digital Certification Unit), Certification Policy of the National Root Certifying Authority. 2011.
6. Executive Branch, Oriental Republic of Uruguay. Decree No. 436/011 dated 21 September 2009 – Regulation of Electronic Documents and Electronic signatures
7. SP-800-63B NIST Special Publication, Digital Identity Guidelines - Authentication and Lifecycle Management, 2017.
8. OWASP Project, https://www.owasp.org/.
9. Unidad de Certificación Electrónica (Digital Certification Unit), Terms for Usage of Advanced Electronic Signature. 2012
10. Cooper, Santesson, Farrell, Boeyen, Housley, Polk. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force (IETF), 2008.