Digital Identification Policy

Table of contents

1. Introduction.

1.1 General Description

This policy is elaborated pursuant to Decree No. 70/018 dated May 19, 2018, [1] regulating 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, regarding digital identification trust services and advanced electronic signature under centralized custody, for the purposes of regulating Digital Identification Trust Service Providers.

Trust Service Providers (TSPs) must be regulated in order to ensure secure digital transactions, promoting safe e-commerce and allowing authentic identification of the parties involved.

Digital identification services may have different assurance levels. This policy defines technical specifications, regulations, and procedures to determine the assurance levels of digital identification services.

Assurance levels that provide digital identification with the same legal validity and effects as in-person identification will be defined based on the registration procedure, means for identification and digital authentication process.

This document was prepared according to the regulations in force, NIST guidelines and recommendations for the protection of digital identification in its document SP 800-63 [3], the eIDAS framework for digital identity and trust services for electronic transactions as established in EU Regulation 910/2014 [4] and the experiences of projects such as STORK (Secure idenTity acrOss boRders linKed) [5].

1.2 Name of the document and identification of the Digital Identification Policy

Name: Digital Identification Policy

Version: 1.0

Elaboration date: 08/08/2018

Last update date: 08/08/2018

OID: 2.16.858.10000157.66565.14

Website of publication: http://www.uce.gub.uy/informacion-tecnica/politicas/

1.3 Players

1.3.1 Regulatory Unit

The Regulatory Unit's role is carried out by the UCE (Digital Certification Unit), pursuant to Law No. 18,600 [2]. It is a regulatory role, whereby technical and operational standards to be observed by TSPs, as well as accreditation procedures and requirements shall be defined.

Apart from its regulatory role, the UCE carries out functions such as: accreditation 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 [6] and section 14 of Law No. 18,600 [2].

1.3.2 Trust Service Providers (TSPs)

Any individual or legal entity, public or private, national or foreign, providing one or more trust services.

In this Policy's context, a TSP is a player supplying "digital identity services" to individuals.

Individuals register with the TSP their digital identity that will then be verified by a third party.

1.4 Use of the digital identification service

In addition to the terms of use established by each TSP when delivering their services, this policy establishes authorized uses and restrictions on the use of digital identification services.

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 number: (+598) 2901 2929

1.6 Connection between the Identification 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, [8] Decree No. 70/018 [1]. 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 TSPs and specified in their procedures.

This Policy affects the Information Security Policies and other procedures of the 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:

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

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 repeal 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 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.

Petitioner: Individual whose digital identity must be verified through a digital authentication process.

National infrastructure of digital certification (NIDC): The national infrastructure of digital certification is the set of computer and software devices, cryptographic devices, policies, rules and procedures provided 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.

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.

Identity Provider (IdP): Entity that manages the digital identification means of the person during the process of digital authentication, and that issues assertions based on those digital identification means.

Service Provider (SP): Entity that provides web services to the person and delegates the digital authentication process to an Identity Provider.

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.

Applicant: Individual claiming a digital identity during the digital identity registration process.

User: Any individual digitally registered with a TSP's digital identification service platform.

2. General aspects of the Identification Policy.

2.1 Responsibilities

2.1.1 Responsibilities of the UCE

The UCE shall be responsible for:

a) Certifying TSPs in order to offer the digital identification service of individuals with the same assurance levels as in-person identity.

b) Controlling the admissibility of applications pursuant to section 15 of Decree No. 436/011 [8].

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.

e) Carrying out regular auditing controls of the TSPs. Audits may be carried out upon request of the UCE.

2.1.2 Responsibilities of Trust Service Providers

a) To possess reliable procedures during registration and authentication of individuals for protection of the digital identity thereof.

b) To possess control and traceability procedures regarding use of the digital identity during the last six months.

c) To keep the integration documentation with the digital identification service of the TSP, to be used by third parties validating a digital identity.

d) To provide users with the digital identification service of the TSP, digital identity blocking procedures or related digital identity means.

e) To anticipate procedures for the suspension of a digital identity by the TSP, as defined in section 4.9 of the UCE's Certification Policy for Individuals [7].

f) To sign a terms of use contract with the individuals to be registered with the TSP's identification service.

g) In case any part of the identity registration or validation process is delegated in a third party, notify the UCE said agreements prior to their effective date.

2.1.3 Responsibilities of individuals

In the context of this Digital Identity Policy, users of the digital identification service are individuals, national or foreign citizens, of legal age, who shall have the following responsibilities.

Digital identification service users take on the following responsibilities:

a. To protect the information related to identification and authentication of their digital identity.

b. To request immediate blocking of their identity or digital identification means if their digital identity safety is or appears to be compromised.

2.2 Liability

Those who make use of digital identification services are responsible for demanding that the service has the sufficient safety level for digital identification of persons (see section 4 of this policy).

2.3 Fees

TSPs 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 “Digital identification” service to individuals, providing the same assurance levels as in-person identification.

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 to 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 UCE in this policy.

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 before the UCE may request their registration with the Registry of TSPs to offer the "digital identification" service. In such case, they shall prove compliance with the specific requirements set forth in this policy.

4. Digital identity assurance levels.

In the context of this Policy, the TSP offers a digital identification service to individuals. Broadly, this service consists of digital authentication registers of persons for their verification by third parties.

In the context of the service, each digital identity has an assurance level assigned, which may go from level 0 to level 3, allowing third parties to verify said identity and know the assurance level thereof.

The assurance level of a digital identity is defined according to the security aspects considered in the following elements:

-The registration stage of a digital identity

The process of identifying a person, verifying the person's data, issue or associate one or more digital identification means thereto, and store said association for subsequent use.

-Associated 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 the individual's knowledge, a physical or logical device, or a physical or behavioral feature.

-Digital identity authentication process

Process for identifying a person through a computer system with one or more digital identity means.

-Identity federation

Process that enables transmission of identity information and authentication through a set of network systems.

The assurance level of a digital identity shall be defined according to the strength of said elements.

There follows a detailed explanation of the features that define each digital identity level.

A summary of the features of each digital identity level is hereby presented.

Level 0 (Very Weak)

This is the lowest assurance level and does not ensure any digital identity trust. The presence of the applicant is not required during the digital identity registration stage, and evidence is accepted with no verification whatsoever.

For example, if the applicant provides an email address or an ID number during the identity registration stage, only the formal validity of said data is controlled.

This level is suitable when the consequences of incorrect authentication have a very low or insignificant impact for the third party verifying that identity.

It is suitable for online services that, due to their nature and definition, do not require digital identity trust.

Level 1 (Weak)

As in level 0, the presence of the applicant is not required during the digital identity registration stage. In this level, the data provided by the individual is validated in order to corroborate that said data make up a unique registration in the service platform of the TSP.

Validation can be carried out, for example, using public or private databases, or by requesting the person details that help to obtain certain confidence that the digital identity claimed corresponds with real-life identity.

This level is suitable when the consequences of incorrect authentication have a low impact for the third party verifying that identity.

Level 2 (Moderate)

In this level, the presence of the individual is required during the digital identity registration stage, so as to ensure unequivocally and with a high level of confidence that the digital identity registered belongs to the individual applying for it.

The digital identity means associated to the person during the registration and authentication process are considered strong.

In this level of digital identity, the consequences of incorrect authentication have a high impact for the third party verifying the digital identity.

Level 3 (High)

It is the highest assurance level defined by this policy and the only digital identity level that equals in-person identification.

As with level 2 previously defined, the presence of the individual is required during the digital identity registration stage. The digital identity means associated to the person during the registration and authentication process are considered strong.

During the digital identity registration stage, the biometric data of the applicant are obtained and validated.

Digital authentication uses a Recognized Individual Digital Certificate as a digital identity means.

In this highest digital identity level, equal to in-person identification, the consequences of incorrect authentication have a severe impact for the third party verifying the digital identity. There may be legal consequences which shall depend on the characteristics of the service offered by the third party where the digital identity is used.

4.1 Digital identity registration procedure

Assurance levels for the registration stage are defined according to the assurance levels of the following elements: the person's identification procedure and the issuance and association process of the digital means thereto.

Very low level (RID0)

This level does not require the person's physical presence. Registration can be done online. Evidence is accepted with no verification whatsoever.
For example, if the applicant provides an email address or an identity number during the digital identity registration process, only the formal validity of said data is controlled.

Associated digital identity means are not controlled. For example, acceptable password policies are not imposed.

Low level (RID1)

This level does not require the person’s physical presence either. Additionally, in this level, the data provided by the applicant are verified in order to check that said data correspond to a unique register in the service platform of the TSP.

Validation can be carried out, for example, using public or private databases, or by requesting the person details that help to obtain a certain level of confidence regarding the correspondence of digital identity with real-life identity.

The digital identity means is obtained and associated through verification of the evidence submitted by the applicant. For example, the digital identity means “user and password” is generated during the person’s digital registration process, and is activated through a link (which expires after an adequate period, for example, 24 hours) that is sent to the email indicated by the applicant. The applicant must access that link in order to activate the digital identity.

Moderate level (RID2)

The moderate level requires the presence of the individual in order to confirm the identity and associate the digital means to the registered digital identity.

Registration can start online, but an in-person identity validation stage is required, during which association to the digital means that will be later used for the authentication process is carried out.

During the in-person stage of identity validation, a national document identifying the individual shall be required, for example, the national identification document issued by the National Bureau of Civil Identification (DNIC) or the passport. The document and the picture of the person furnished shall be verified.

The digital identity means associated to the person during registration are considered strong.

The association procedure of the digital means to the applicant must be linked to the in-person stage, and may be continued online after said stage. For example, upon the in-person delivery of a QR code, PIN, or password needed for online activation of the digital means.

High level (RID3)

The high level requires the presence of the individual in order to confirm the identity and associate the digital means to the registered digital identity.

Registration can start online, but an in-person identity validation stage is required, during which association to the digital means that will be later used for the authentication process is carried out.

During the in-person stage of identity validation, a national document identifying the individual shall be required. For example, the national identification document issued by the National Bureau of Civil Identification (DNIC) or the passport. The document and the picture of the person furnished shall be verified.

During the registration stage, the biometric verification of the person is carried out in order to ensure non-repudiation. Biometric verification is made through comparison methods and data sources as defined in Section 4.2.

The type of digital identity means associated to the applicant is a Recognized Individual Digital Certificate that may be generated during or before the digital identity registration stage. If the person already has a Recognized Individual Digital Certificate, generated before the registration stage, such person shall prove possession of the digital identity means that contains the certificate. In this case, the new certificate to be issued by the TSP will depend on the validity of the preexistent certificate, during its whole life-cycle.

4.2 Biometric verification

During the digital identity registration stage, a biometric verification of the person is carried out.

A valid biometric verification method uses fingerprints, and the valid data source for biometric comparison is the National Bureau of Civil Identification (DNIC).

Therefore, the biometric verification of a person may be carried out using the Match on Card function of the new electronic identity document (eID) or through a fingerprint validation service connected to the DNIC.

4.3 Digital identity means

During the digital authentication stage, the identity proof furnished by the petitioner of a digital identity shall depend on the assurance of the identification means used and the procedure used to communicate the result of this authentication.

The digital identity means considered by this policy during the authentication stage are the following:

Username / password or PIN: a string of characters memorized and kept in secret by the person. The username may be chosen by the person or generated by the identity provider. For the password or PIN, there are different assurance levels according to the characters. NIST's "Digital Identity Guidelines" 800-63B [9] defines the strength of this type of digital means.

Code list: A code list is usually used in combination with a static password or PIN within an authentication system. Examples are codes derived from coordinate cards. For more information about this digital means, refer to NIST "Digital Identity Guidelines" 800-63B [9], section "Look-Up Secret Verifiers."

One-time password (OTP) token: is a personal hardware device that is capable of producing a single-use password that is valid for one login session and is synchronized with the validation system.

Encryption software device: A cryptographic key stored in a drive, USB flash drive, or other communication means. The authentication is achieved when the possession and control of the key is verified.

Encryption hardware device: a smart card or similar means that contains a cryptographic key protected by hardware. The authentication is achieved when the possession of the device and control of the key is verified.

Recognized Individual Digital Certificate (CERPF): Recognized digital certificate the subscriber of which is an individual. Issued exclusively by the ACSP and subject to the requirements of the UCE's Policy for Individuals.

The digital means defined in this policy are based on NIST's Digital Identity Guidelines 800-63B [9].

4.4 Digital authentication

Digital authentication is defined as: "*The process of identifying a person through a computer system using one or more digital identity means*."

The trust level offered by the remote authentication process depends on the strength of the authentication method when facing different kinds of attacks and of the digital identity means used during the authentication process.

Based on the digital means defined in section 4.3, different levels of strength are assigned in the table below, from AE0 to AE3, depending on the digital means used during the digital authentication process.

Minimum requirements	Strength of the digital identity electronic means			
	AE0	**AE1**	**AE2**	**AE3**
Username / Password or PIN: chosen by the applicant, but not following password security best practices. May be vulnerable to a brute-force attack or a dictionary attack.	•			
Username / Password or PIN: chosen by the applicant, following password security best practices (NIST 800-63). Not vulnerable to a brute-force attack or a dictionary attack.	•	•		
Multi-factor authentication (Encryption software/hardware devices or OTP or Code list) + Password/PIN following security best practices or biometrics.	•	•	•	
Multi-factor authentication taking into account: Recognized Individual Digital Certificate + password and/or PIN following security best practices.	•	•	•	•

Each of the levels described from A0-A3 takes into account the requirements of all previous levels. For levels AE2 and AE3, it is necessary to include multi-factor authentication based on NIST "Digital identity Guidelines" [9] SP 800-63B, chapter 4.2.

4.5 Definition of digital identity levels

Based on assurance levels during the registration process of a digital identity and the digital authentication process thereof, there follow the assurance levels applicable to digital identity.

		Assurance level in the digital authentication process of a digital identity			
		AE0	**AE1**	**AE2**	**AE3**
Registration procedure for a digital identity	**RID0**	DIGITAL IDENTITY LEVEL 0	DIGITAL IDENTITY LEVEL 0	DIGITAL IDENTITY LEVEL 0	DIGITAL IDENTITY LEVEL 0
	RID1	DIGITAL IDENTITY LEVEL 0	DIGITAL IDENTITY LEVEL 1	DIGITAL IDENTITY LEVEL 1	DIGITAL IDENTITY LEVEL 1
	RID2	DIGITAL IDENTITY LEVEL 0	DIGITAL IDENTITY LEVEL 1	DIGITAL IDENTITY LEVEL 2	DIGITAL IDENTITY LEVEL 2
	RID3	DIGITAL IDENTITY LEVEL 0	DIGITAL IDENTITY LEVEL 1	DIGITAL IDENTITY LEVEL 2	DIGITAL IDENTITY LEVEL 3

The above table describes the different digital identity levels that can be obtained depending on the assurance levels during identity registration and the assurance levels of the authentication process.

The combination of AE (Digital Authentication) and RID (Digital Identity Registration) levels was made taking into account the security paradigm where the assurance level is given by the weakest link; therefore, the lowest value will always be obtained, which results in:

Digital identity level 0: Digital identity level 0 shall exist when the registration level is RID0 and the authentication level is AE0 or higher. It shall also exist when the registration level is RID0 or higher and the authentication level is AE0.

Digital identity level 1: Digital identity level 1 shall exist when the registration level is RID1 and the authentication level is AE1 or higher. It shall also exist when the registration level is RID1 or higher and the authentication level is AE1.

Digital identity level 2: Digital identity level 2 shall exist when the registration level is RID2 and the authentication level is AE2 or higher. It shall also exist when the registration level is RID2 or higher and the authentication level is AE2.

Digital identity level 3 (same as in-person identity): It is the only digital identity level that equals in-person identity. It shall exist when the assurance level in the registration process is RID3 and the authentication level is AE3.

5. Digital identification trust service.

A TSP authorized to provide digital identity service under this policy has, as part of the TSP's systems, a component named Identity Provider (IdP).

The purpose of the Identity Provider is to enable users registered with the identity service of the TSP to have a unique set of digital identity means and authentication point to use third-party services.

In other words, a TSP's IdP provides the authentication service to Service Providers (SP) through a technical and trust integration between both systems.

A TSP's IdP role ends after the digital authentication process and communication of the results of that process to the SP which will as a result verify the digital identity level obtained by the user in the IdP, and will use it to give access to the SP's pertinent services.

The IdP is the technician responsible for the digital authentication process of users registered with the digital identification service of the TSP and is therefore responsible for:

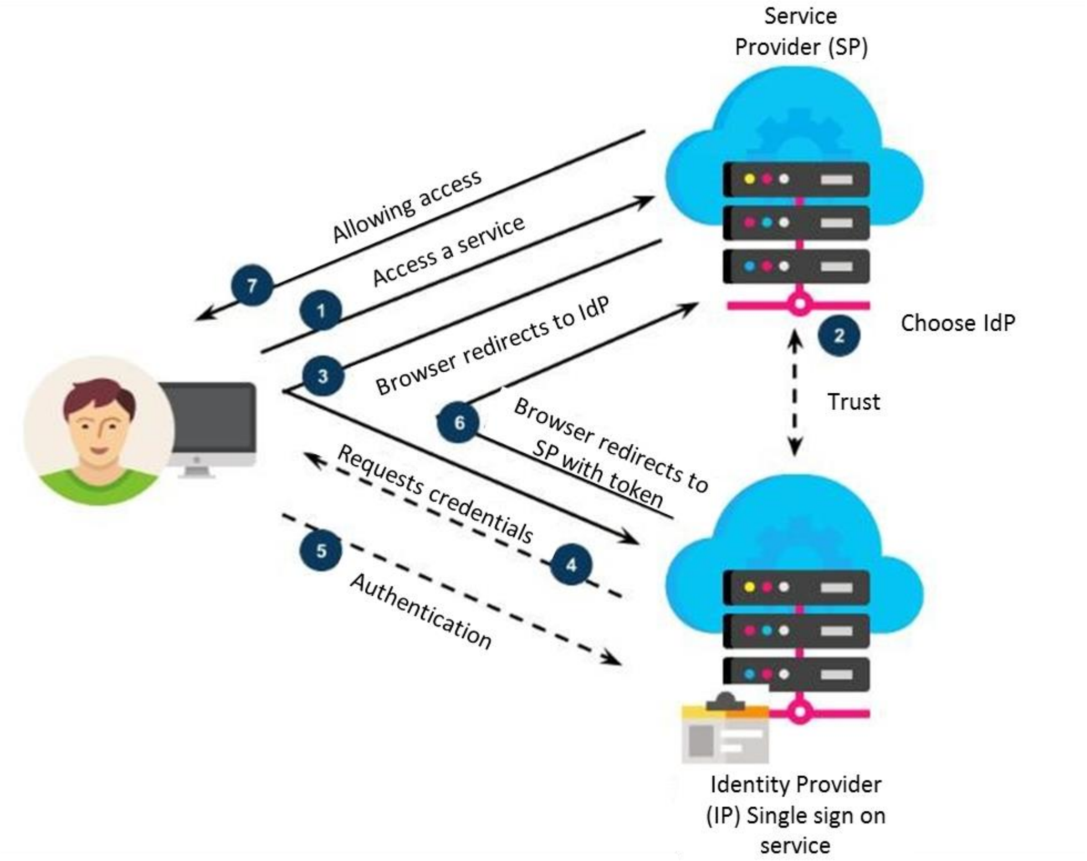
-Requesting the digital means from the User of the digital identity service.

-Accepting or rejecting the authentication of the User of the digital identity service.

-Assigning the corresponding assurance level to the digital identity according to the conditions defined in this policy.

-Communicating the result of the authentication process and thus the digital identity level of the User to the SPs through assertions.

The following diagram shows the authentication process of a User of the SP through an IdP belonging to the TSP’s systems.



1-The User wants to access a service offered by the SP.

2-The SP chooses the TSP’s IdP, to which the digital authentication process of the SP’s users should be entrusted. At this point, the SP may give the User the possibility to choose the TSP.

3-After choosing the TSP, the user is redirected to the IdP (belonging to a TSP) to carry out the digital authentication process and submit the corresponding digital means.

4-The IdP requests the User to provide the digital means for the digital authentication process.

5-The User carries out the digital authentication process in the IdP by submitting the digital means.

6-The IdP redirects the User to the SP, with the authentication result contained in an assertion, including the digital identity level reached by the User in the IdP.

7-The SP authorizes or denies access to the SP's services, verifying the digital identity level obtained by the User in the IdP.

During the authentication process described in the example, there is a trust relationship between the IdP and the SP for the transfer of authentication and identity information of Users.

In the following point, the technical and security considerations for the transfer of information, named federation, are described.

6. Identity federation and assertion.

Federation implies the transfer of a person's attributes to a third party which is not involved in a transaction, through assertions.

An assertion used for authentication is a set of attribute values or attribute references associated to an authenticated user that are transferred to the IdP or SP in a federated identity system. Assertions contain a variety of information, for example: asseveration metadata, attribute values and attribute references about the user.

In the case of a level 3 digital identity that equals in-person identity, the TSP must take into account the following considerations for the implementation of the TSP's federation in the component IdP.

-Implement the federation strategy using SAML 2.0 or OpenID Connect.

-Assertions must be signed by the IdP and ciphered through asymmetric cryptography and public key from the SP or symmetric cryptography and shared key.

The considerations are based on level "FAL 2" defined by NIST in "Digital Identity Guidelines" [9] SP 800-63C for identity federation.

7. Third parties validating an identity.

Pursuant to section 7 of Decree No. 70/018 [1], those who use digital identification services are responsible for demanding, when providing their services, an adequate assurance level for the digital identification of persons.

This means that the SP that integrates the services of an authorized TSP is responsible for requesting the adequate digital identity level for the operation or functionality, depending on the SP's business.

For example:

If the service to be used by users in the SP requires a level 3 digital identity guarantee, the SP must demand the user to be authenticated in the TSP's IdP with a digital identity level 3.

8. Operational, security and technical controls.

A TSP that wishes to be authorized to provide digital identity services for individuals must comply with standards and adequate requirements in Information Security.

For the definition of standards and adequate security requirements, the Cibersecurity Framework published by AGESIC [10], applied to systems associated to the TSP's identification service, will be followed.

Security certifications, such as ISO 27001, may be taken into account as long as their application to the systems associated to the TSP's identification service is proved.

Additionally, the TSP must prove compliance with the conditions established for the assurance levels of a digital identity with a level equivalent to in-person identity, required for:

-The digital identity registration procedure (section 4.1),

-The association of digital identity means (section 4.3),

-The digital authentication process (section 4.4),

-Identity federation (section 6).

Compliance with the aforementioned terms must be reflected on the current procedures of the TSP.

9. Suspension and revocation of TSPs accreditations.

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.

10. Cessation of activities of accredited TSPs.

Accredited TSPs which cease their activities must communicate said cessation through the Official Gazette and another digital or traditional means that they may deem convenient.

External references

1. **Executive Branch, Oriental Republic of Uruguay.** Decree No. 70/018 – Regulation of sections 31 to 33 of Law No. 18,600 dated September 21, 2009. https://medios.presidencia.gub.uy/legal/2018/decretos/03/cons_min_625.pdf

2. **Legislative Branch, Oriental Republic of Uruguay.** Law No. 18,600, dated September 21, 2009, about Electronic Documents and Digital Signatures. https://legislativo.parlamento.gub.uy/temporales/leytemp8634393.htm

3. **SP-800-63 NIST Special Publication,** Digital Identity Guidelines - Authentication and Lifecycle Management, 2017. https://pages.nist.gov/800-63-3/

4. **Regulation (EU) No. 910/2014,** European Parliament, dated July 23, 2014. https://www.boe.es/doue/2014/257/L00073-00114.pdf

5. **STORK 2.0 Security Identity Across Borders Linked**, https://www.eid-stork2.eu/

6. ***Unidad de Certificación Electrónica* (Digital Certification Unit),** Certification Policy of the National Root Certifying Authority . http://uce.gub.uy/informacion-tecnica/politicas/

7. ***Unidad de Certificación Electrónica* (Digital Certification Unit),** Certification Policy for Individuals (newest version). http://uce.gub.uy/informacion-tecnica/politicas/

8. **Executive Branch, Oriental Republic of Uruguay.** Decree No. 436/011 dated December 8, 2011 – Regulation of Electronic Documents and Digital Signatures. http://archivo.presidencia.gub.uy/sci/decretos/2011/12/cons_min_420.pdf

9. **SP-800-63B NIST Special Publication,** Digital Identity Guidelines - Authentication and Lifecycle Management, 2017. https://pages.nist.gov/800-63-3/

10. **Cibersecurity Framework v 4.0,** https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad-v40.html