UNIDAD DE CERTIFICACIÓN ELECTRÓNICA

Uruguay: Building a framework for Trust Services

Torre Ejecutiva Sur / Liniers 1324, 3rd floor / +598 29010065 ext 5 / URUGUAY / uce.gub.uy

Authors contact

Jimena Hernández Varela
jimena.hernandez@agesic.gub.uy

Matías Jackson Bertón
matias.jackson@agesic.gub.uy

Jorge Prego Acosta
jorge.prego@agesic.gub.uy

ABSTRACT

This paper explores the path followed by Uruguay in the consolidation of a digital identification framework. The main objective followed by the regulatory entity was to provide legal equivalence between physical presence and digital identification as well as compatibility with international standards. The essay will serve as an input for other countries looking for upgrading their electronic signature framework.

1. CONTEXT

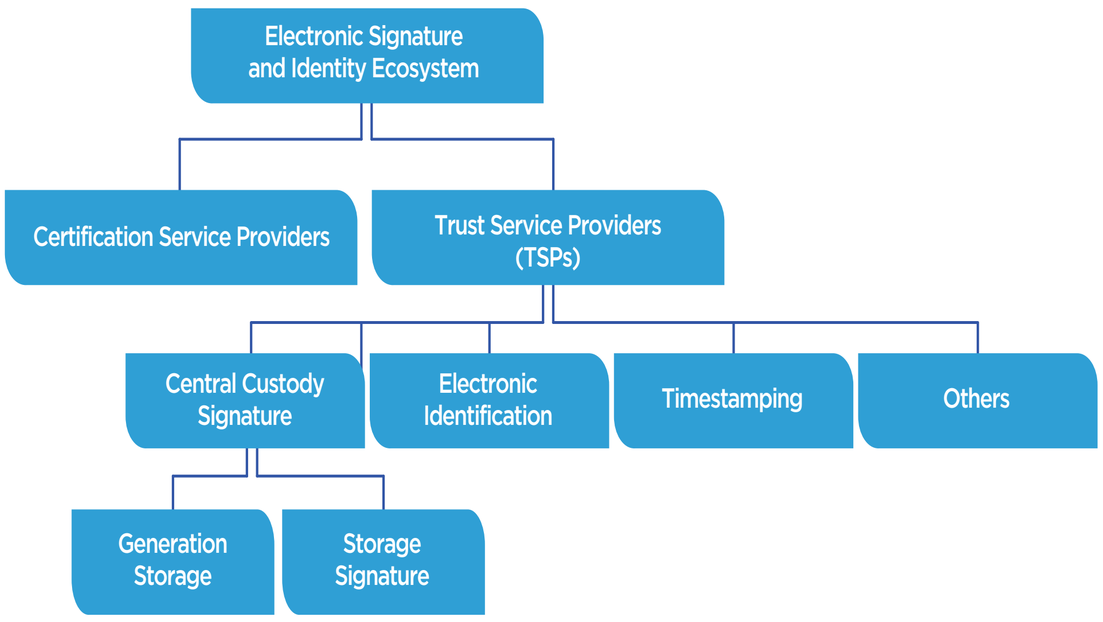
Uruguay is a small country of 3.5 million inhabitants in South America. Size has not prevented it from being first in the region in terms of Digital Development. In the latest years, the country has gone through a strategic path in terms of digital transformation, led by the Agency for Electronic Government and Information Society (AGESIC).

- **Capital: Montevideo**
- **Population: 3,444,006**
- **Area: 176,215 km2**
- **PKI since 2009**
- **D9 Member**

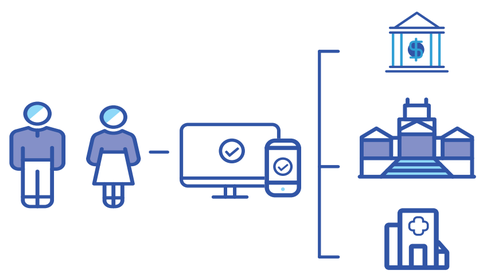
Physical presence or face-to-face recognition has been an impediment for people when they interact with government agencies through electronic means. Many administrative procedures require people to be physically present in front of a public servant and to provide an identification document, such as the National Identification Document or Passport.
In order to leave aside these requirements and to extend the possibilities for introduce digital procedures from beginning to end the Act 19.535 established a legal equivalence between personal and electronic identification. This means that, given the appropriate assurance levels, people will be able to prove electronically that they are who they say they are. This certainty will give them access to more complex and personal services that otherwise would have required them to be physically in one place.

2. TRUST SERVICE PROVIDERS

Trust Service Providers are defined by law as those in charge of providing legal certainty for electronic acts. The Electronic Certification Unit (UCE) has enacted Technical Policies for different kinds of TSPs: Central Custody of Signatures, Digital Identification and Time-stamping.



3. DIGITAL IDENTIFICATION



Not every digital identification mean would give the necessary security to proof the identity of individuals. Assurance levels have to be defined as Electronic Identification a level which occurs by the combination of two dimensions: registration and authentication procedures.
The combination of both, registry and authentication methods, can provide different levels of assurance to validate the digital identity of the person.
Through its technical policy, the UCE has defined four Identification Levels, from Zero to Three, according to the security methods used both when users are registered in the system and when they are authenticated:

- **(i)** Zero Level (Very low): It is the lowest level of security and does not ensure confidence at all in the digital identity The presence of the applicant is not required to record a digital identification and the evidences or data presented are accepted without any verification, except for formal validation;
- **(ii)** First Level (Low): At this level, a validation is made to the data provided by the person in order to ensure that these data correspond to a unique identity record in the TSP platform. Validation can be done, for example, through public or private databases, or by requesting additional data to the person;
- **(iii)** Second Level (Medium): At this level, physical presence of the person is required during the stage of digital identification registration, in order to ensure unambiguously the identity;
- **(iv)** Third Level (High): This is the highest level of Electronic Identification requiring the physical presence of the person during the digital identification registration stage where biometric data of the applicant is captured and validated.

The UCE has defined that this third level provides the necessary certainties that the person is who she or he says, making it equivalent to physical presence. Through this electronic identification, citizens will be able to perform the procedures as if they were 'physically' at the administration office. Digital Identity Levels Matrix.

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

4. INTERNATIONAL STANDARDS

In order to create an interoperable framework the UCE took into account the levels established at international standards and foreign policies, especially the regulation in Europe and United States.
The Table shows the equivalence between these different regulatory frameworks.

eIDas	NIST			Uruguay
	IAL	AAL	FAL	
-	1	1, 2 or 3	1	Very Low
Low	1, 2 or 3	1, 2 or 3	2	Low
Substantial	2 or 3	2 or 3	3	Medium
High	3	3	4	High

5. CONCLUSIONS

With the introduction of electronic identification providers into the ecosystem, the UCE seeks to reduce barriers to the adoption of electronic procedures, getting closer to the final goal of providing an ecosystem that is 100% online.
To encourage more confidence in this new environment, these services are based on international standards which are being used in Europe and the Americas. It is essential to achieve a balance between security and accessibility needs for citizens, in order to generate the necessary confidence to promote the adoption of these new services.
The modifications introduced to the legal framework as well as the matching with international standards is hoped to be a resource for other developing countries trying to adopt new identification means.

ICEGOV 2019 MELBOURNE AUSTRALIA
12th International Conference on Theory and Practice of Electronic Governance
3-5 APRIL 2019
www.icegov.org

PATRON
Australian Government
Digital Transformation Agency

ORGANIZERS
RMIT UNIVERSITY
UNITED NATIONS UNIVERSITY
UNU-EGOV