Política de Identificación Digital

Contenido

1.Introducción 3

1.1. Descripción general 3

1.2. Nombre del documento e identificación de la Política de Identificación Digital 4

1.3. Actores 4

1.3.1. Unidad Reguladora 4

1.3.2. Prestadores de servicios de confianza (PSCo) 4

1.4. Uso del servicio de identificación digital 5

1.5. Administración de la Política de Certificación 5

1.6. Relación entre la Política de Identificación y otros documentos 5

1.7. Procedimiento de Aprobación 5

1.8. Definiciones y abreviaturas 6

2. Aspectos generales de la Política de Identificación 8

2.1 Obligaciones 8

2.1.1 Obligaciones de la UCE 8

2.1.2 Obligaciones de los Prestadores de Servicios de Confianza 9

2.1.3 Obligaciones de las Personas Físicas 9

2.2. Responsabilidades 10

2.3. Tarifas 10

3. Acreditación de Prestadores de Servicios de Confianza 10

4. Niveles de Seguridad en la identidad digital 11

4.1 Procedimiento de registro de identificación digital 13

4.2 Verificación Biométrica 15

4.3 Medios de identificación digital 15

4.4 Autenticación electrónica 17

4.5 Definición de los niveles de identidad digital 18

5. Servicio de confianza de identificación digital. 19

6. Federación de identidades y aserciones. 21

7. Terceros que validan una identidad. 22

8. Controles operativos, de seguridad y técnicos 22

9. Suspensión y revocación de la acreditación de los prestadores de servicios de confianza..... 23

10. Cese de actividades del prestador de servicios de confianza acreditado..... 23

1. Introducción

1.1. Descripción general

A partir del Decreto N° 70/018 de 19 de marzo de 2018 [1], que reglamenta los artículos 31 al 33 de la Ley N° 18.600 de 21 de setiembre de 2009 [2] en la redacción dada por el artículo 28 de la Ley N° 19.535 de 25 de setiembre 2017 respecto a los servicios de confianza de identificación digital y firma electrónica avanzada con custodia centralizada, es elaborada la presente política con el fin de regular a los Prestadores de Servicios de Confianza de Identificación Digital (PSCo).

Su regulación constituye un elemento esencial para garantizar la seguridad de las transacciones electrónicas, promoviendo el comercio electrónico seguro, de modo de permitir la identificación en forma fehaciente de los sujetos intervinientes.

Los servicios de identificación digital podrán contar con diversos niveles de seguridad. Esta política define las especificaciones técnicas, normas y procedimientos para determinar los niveles de seguridad de los servicios de identificación digital.

Considerando el procedimiento de registro, los medios de identificación y el proceso de autenticación electrónica, se definirán los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efecto jurídico que la identificación presencial.

La confección del presente documento se realizó siguiendo el marco normativo vigente, las guías y recomendaciones para proteger la identidad digital del NIST en su publicación SP 800-63 [3], el marco eIDAS relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en su Reglamento 910/2014 [4] y las experiencias de proyectos como STORK (Secure idenTity acrOss boRders linKed) [5].

1.2. Nombre del documento e identificación de la Política de Identificación Digital

Nombre: Política de Identificación Digital.

Versión: 1.0

Fecha de elaboración: 08/08/2018

Fecha de última actualización: 08/08/2018

OID: 2.16.858.10000157.66565.14

Sitio web de publicación: http://www.uce.gub.uy/informacion-tecnica/politicas/

1.3. Actores

1.3.1. Unidad Reguladora

El rol de Unidad Reguladora es desempeñado por la UCE (Unidad de Certificación Electrónica), según lo dispuesto por la Ley N° 18.600 [2], es un rol de regulación, en el cual debe definir los estándares técnicos y operativos que deberán cumplir los PSCo, así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.

Además de su rol regulador, la UCE desempeña funciones de acreditación de Prestadores de Servicios de Certificación; control y auditoría de su actividad; instrucción estableciendo criterios generales y asesoramiento en buenas prácticas de funcionamiento; y sanción en caso de incumplimiento. Puede encontrarse información detallada en la Política de Certificación de la ACRN [6] y en el artículo 14 de la Ley N° 18.600 [2].

1.3.2. Prestadores de servicios de confianza (PSCo)

Persona física o jurídica, pública o privada, nacional o extranjera, que presta uno o más servicios de confianza.

En el contexto de la presente Política, un PSCo, es actor en la prestación de "Servicios de identificación digital" a personas físicas.

Las personas físicas realizan en el PSCo el registro de su identidad digital que luego será verificada por un tercero.

1.4. Uso del servicio de identificación digital

Los usos habilitados y restricciones para la utilización del servicio de identificación digital, están dados por, la presente política y las condiciones de uso establecidas por cada PSCo en la prestación del servicio.

1.5. Administración de la Política de Certificación

La administración de la presente Política es responsabilidad de la UCE.
Por consultas o sugerencias, la UCE designa al siguiente contacto:

Nombre: Unidad de Certificación Electrónica
Dirección de correo: info@uce.gub.uy
Teléfono: (+598) 2901 2929

1.6. Relación entre la Política de Identificación y otros documentos

La presente Política se basa en la Ley N° 18.600 [2] en la redacción dada por el artículo 28 de la Ley N° 19.535, el Decreto N° 436/011 de 8 de Diciembre de 2011 [8], el Decreto N° 70/018 [1], y prevalece sobre ella la legislación vigente y las disposiciones particulares adoptadas por la UCE.

Los requerimientos definidos en esta Política deben ser instrumentados por los Prestadores de Servicios de Confianza (PSCo) y especificados en sus procedimientos.

Esta Política tiene impacto en las Políticas de Seguridad de la Información y otros procedimientos del Prestador de Servicios de Confianza (PSCo).

1.7. Procedimiento de Aprobación

La aprobación de esta política, así como toda modificación introducida en ella, es responsabilidad exclusiva de la UCE. La UCE aplicará sus procedimientos internos de administración documental para garantizar la calidad y trazabilidad de los cambios realizados. La Política modificada se publicará como una nueva versión, manteniéndose un registro de la fecha y cambios realizados.

1.8. Definiciones y abreviaturas

Las definiciones y abreviaturas generales de la Infraestructura Nacional de Certificación Electrónica (INCE) se encuentran definidas en la Ley N° 18.600 [2]. No obstante, las siguientes definiciones y abreviaturas son utilizadas a lo largo del presente documento, y, por lo tanto, son citadas también aquí.

Autenticación electrónica: el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital.

Autoridad de Registro (AR): en el contexto de la presente política, es responsable del registro y procesamiento de solicitudes de emisión, renovación y revocación de certificados, incluyendo la validación de la identidad de los suscriptores/o de las solicitudes al inicio del proceso.

Certificado Electrónico (CE): documento electrónico firmado electrónicamente que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica.

Certificado Electrónico Reconocido de Persona Física (CERPF): Certificado Electrónico Reconocido cuyo suscriptor es una Persona Física, emitidos en exclusividad por los PSCA y sujetos a los requerimientos de la presente Política de Certificación.

Demandante: Persona Física cuya identidad digital debe verificarse mediante un proceso de Autenticación electrónica.

Infraestructura nacional de certificación electrónica (INCE): la infraestructura nacional de certificación electrónica es el conjunto de equipos y programas informáticos, dispositivos criptográficos, políticas, normas y procedimientos, dispuestos para la generación, almacenamiento y publicación de los certificados reconocidos, así como también para la publicación de información y consulta del estado de vigencia y validez de dichos certificados.

Medio de identificación electrónica o digital: unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante:

a) su conocimiento;
b) un dispositivo físico o lógico;
c) algún rasgo físico o comportamental.

Prestador de Servicios de Certificación Acreditado (PSCA): persona física o jurídica acreditada ante la UCE y responsable de la operación de al menos una Autoridad Certificadora de la INCE.

Prestador de Servicios de Confianza (PSCo): persona física o jurídica, pública o privada, nacional o extranjera, que presta uno o más servicios de confianza.

Proveedor de Identidades (IdP – Identity Provider): entidad que administra los medios de identificación digital de la persona en el proceso de autenticación electrónica y emite aserciones derivadas de esos medios de identificación digital.

Proveedor de Servicios (SP – Service Provider): entidad que provee servicios web a la persona y delega el proceso de autenticación electrónica en un Proveedor de Identidades.

Registro de identificación digital: el proceso de identificar a una persona, verificar sus datos, expedir o asociar uno o más medios de identificación digital a ésta, y almacenar dicha asociación para su posterior utilización.

Servicios de Confianza: son servicios electrónicos que permiten brindar seguridad jurídica a los hechos, actos y negocios realizados o registrados por medios electrónicos, entre ellos:

a) servicios de firma electrónica avanzada con custodia centralizada;
b) servicios de identificación digital;
c) servicios de sellado de tiempo;
d) otros servicios establecidos por la Unidad de Certificación Electrónica.

Servicios de identificación digital: son servicios que realizan registros de autenticación electrónica de personas para su verificación por terceros.

Solicitante: Persona Física reclamando una identidad digital durante el proceso de registro de identificación digital.

Usuario: Persona física registrada digitalmente en una plataforma de servicios de identificación digital de un PSCo.

2. Aspectos generales de la Política de Identificación

2.1Obligaciones

2.1.1 Obligaciones de la UCE

La UCE asume las siguientes obligaciones:

a)Acreditar a los prestadores de servicios de confianza para brindar el servicio de Identificación digital de personas físicas con niveles de seguridad equivalentes a la identificación presencial.

b)Realizar control de admisibilidad de las solicitudes según lo establecido en el artículo 15 del Decreto N° 436/011 [8].

c)Aprobada técnicamente la solicitud de acreditación, se comunicará al solicitante quién dispondrá de 20 días corridos contados a partir del día siguiente a la notificación, para presentar la garantía prevista en el artículo 17 de la Ley N° 18.600 [2] a través de la contratación de un seguro de responsabilidad civil para afrontar el riesgo de la responsabilidad por daños y prejuicios que pudieran ocasionar en la prestación de sus servicios.

d)Otorgar la acreditación al solicitante por el plazo que determine la UCE. Dicha acreditación estará sujeta a las inspecciones y auditorías que requiera.

e)Realizar controles de auditorías periódicas a los PSCo. Las auditorías realizadas pueden ser a demanda de la UCE.

2.1.2 Obligaciones de los Prestadores de Servicios de Confianza

a) Disponer de mecanismos seguros durante el registro y autenticación de personas físicas para la protección de su identificación digital.

b) Contar con mecanismos de control y trazabilidad sobre el uso de la identidad digital en sus últimos seis meses.

c) Disponer de la documentación de integración con el servicio de identificación digital del PSCo, para uso de los terceros que validen una identidad digital.

d) Proveer a los usuarios del servicio de identificación digital del PSCo, mecanismos de bloqueo de la identidad digital o de los medios de identificación digital asociados.

e) Prever mecanismos para la suspensión de una identidad digital por parte del PSCo, definidos en la sección 4.9 de la Política de Certificación de Persona Física de la UCE [7].

f) Firmar un contrato de términos de uso con las personas físicas a registrar en el servicio de identificación del PSCo.

g) En caso de delegar en un tercero elementos del proceso de registro o validación de identidad deberá notificar a la UCE de estos acuerdos, previo a su entrada en vigencia.

2.1.3 Obligaciones de las Personas Físicas

En el contexto de la presente Política de Identificación Digital, los usuarios del servicio de identificación digital son personas físicas, ciudadanos nacionales o extranjeros, mayores de dieciocho años, bajo cuya responsabilidad recaerán las obligaciones citadas en este punto.

Los usuarios del servicio de identidad digital asumen las siguientes obligaciones:

a. Proteger la información relacionada con la identificación y autenticación en su identidad digital.

b. Solicitar el bloqueo inmediato de su identidad o los medios de identificación digital ante compromiso o sospecha de compromiso de la seguridad de su identidad digital.

2.2. Responsabilidades

Es responsabilidad de quienes utilizan servicios de identificación digital requerir, en la prestación de sus servicios, un nivel de seguridad adecuado para la identificación digital de personas (Ver sección 7 de la presente política).

2.3. Tarifas

Los Prestadores de Servicios de Confianza podrán percibir una prestación económica para sus servicios.

3. Acreditación de Prestadores de Servicios de Confianza

En el contexto de la presente Política, los prestadores de servicios de confianza podrán acreditarse para brindar el servicio de "Identificación Digital" de personas físicas con niveles de seguridad equivalentes a la identificación presencial.

Son condiciones indispensables para ser prestador de servicios de confianza acreditado, las siguientes:

a) Ser persona física o jurídica constituida en el país, dar garantía económica y solvencia suficiente para prestar los servicios.

b) Contar con personal calificado con conocimientos y experiencia necesarios para la prestación de los servicios de confianza ofrecidos y con procedimientos de seguridad y de gestión adecuados.

c) Utilizar estándares y herramientas adecuadas según lo establecido por la Unidad de Certificación Electrónica en la presente política.

d) Estar domiciliado en el territorio de la República Oriental del Uruguay, entendiéndose que cumple con este requisito cuando su infraestructura tecnológica y demás recursos materiales y humanos se encuentren situados en territorio uruguayo.

Los prestadores de servicios de certificación acreditados ante la UCE podrán solicitar su inscripción en el Registro de prestadores de servicios de confianza para brindar el servicio de "Identificación digital", en este caso deberán acreditar los requisitos específicos establecidos en la presente política.

4. Niveles de Seguridad en la identidad digital

En el contexto de la presente Política, el Prestador de Servicios de Confianza (PSCo) brinda el servicio de identificación digital de personas físicas. A grandes rasgos el servicio consiste en registros de autenticación electrónica de personas para su verificación por terceros.

En el contexto del servicio, cada identidad digital tiene asignado un nivel de seguridad que puede ir desde el nivel 0 al nivel 3, permitiendo a los terceros que verifiquen esa identidad y conozcan el nivel de seguridad asociado a ella.

El nivel de seguridad de una identidad digital es definido acorde a los aspectos de seguridad considerados en los siguientes elementos:

-**La etapa de Registro de identificación digital**

Proceso de identificar a una persona, verificar sus datos, expedir o asociar uno o más medios de identificación digital a ésta, y almacenar dicha asociación para su posterior utilización

-**Los medios de identificación asociados**

Unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante su conocimiento, un dispositivo físico o lógico, o algún rasgo físico o comportamental.

-**El proceso de autenticación de la identidad digital**

Proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital.

-**La Federación de la identidad.**

Proceso que permite la transmisión de información de identidad y autenticación a través de un conjunto de sistemas en red.

En base a la fortaleza de los elementos mencionados, podemos definir niveles de seguridad para una identidad digital.

En las siguientes secciones del presente punto, se describen en detalle las características que definen a cada nivel de la identidad digital.

A continuación, se presenta un resumen de las características de cada nivel de una identidad digital.

Nivel 0 (Muy Bajo)

Es el nivel de seguridad más bajo y no asegura confianza en absoluto en la identidad digital. No se requiere presencia del solicitante durante la etapa de registro de identificación digital y las evidencias presentadas se aceptan sin ninguna forma de verificación.

Por ejemplo, si el solicitante proporciona una dirección de correo electrónico o número de documento de identidad durante la etapa de registro de identificación digital, el único control que se realiza es que esos datos sean formalmente válidos.

Este nivel es apropiado cuando las consecuencias de una autenticación errónea tienen un impacto muy bajo o insignificante para el tercero que verifica esa identidad.

Se adapta a los servicios en línea que, por su naturaleza y definición, no requieren de confianza en la identidad digital.

Nivel 1 (Bajo)

Al igual que el nivel 0, no se requiere la presencia del solicitante durante la etapa de registro de identificación digital. En este nivel, se realiza una validación a los datos proporcionados por la Persona Física de forma de asegurar que esos datos conforman un registro único en la plataforma de servicios del PSCo.

La validación puede realizarse por ejemplo sobre bases de datos públicas o privadas, o mediante la solicitud a la persona de datos que generen confianza en la correspondencia de su identidad digital con su identidad física.

Este nivel es apropiado cuando las consecuencias de una autenticación errónea tienen un impacto bajo para el tercero que verifica la identidad digital.

Nivel 2 (Medio)

En este nivel se requiere la presencia de la Persona Física durante la etapa de registro de identificación digital, de forma de asegurar sin ambigüedades y con un alto nivel de confianza, que una identidad digital registrada pertenece a la Persona Física que la solicita.

Los medios de identificación digital asociados a la persona durante el registro y el proceso de autenticación, son considerados robustos.

En este nivel de identidad digital, las consecuencias de una autenticación errónea tienen un impacto alto para el tercero que verifica la identidad digital.

Nivel 3 (Alto)

Es el nivel más alto definido por la presente política y único nivel de identidad digital equivalente al presencial.

Al igual que el nivel 2 definido previamente, requiere la presencia de la Persona Física durante la etapa de Registro de identificación digital. El medio de identificación digital asociados a la persona durante el registro es considerado robusto de la misma forma que el proceso de autenticación.

Durante la etapa de registro de identificación digital, se capturan y validan datos biométricos del solicitante.

La autenticación electrónica se realiza utilizando como medio digital de identificación, un Certificado Electrónico Reconocido de Persona Física.

En este nivel de identidad digital más elevado y equivalente al presencial, las consecuencias de una autenticación errónea tienen un impacto severo para el tercero que verifica la identidad digital. Las consecuencias pueden ser legales y dependerán de las características del servicio prestado por el tercero donde se hace uso de la identidad digital.

4.1 Procedimiento de registro de identificación digital

Los niveles de seguridad para la etapa de Registro se definen en función de los niveles de seguridad de los siguientes factores: el procedimiento de identificación de la persona y el proceso de emisión y asociación de los medios digitales a esta.

Nivel Muy bajo (RID0)

Este nivel no requiere presencia física de la persona. El registro puede ser realizado en línea. Las evidencias presentadas se aceptan sin ninguna forma de verificación.
Por ejemplo, si el solicitante proporciona una dirección de correo electrónico o número de documento de identidad durante la etapa de registro de identificación digital, el único control que esos datos sean formalmente válidos.

No se realizan controles sobre el medio de identidad digital asociado, por ejemplo, no se imponen políticas de contraseñas aceptables.

Nivel Bajo (RID1)

Este nivel tampoco requiere presencia física. Adicionalmente al nivel anterior, en este nivel se realiza una validación a los datos proporcionados por el solicitante de forma de asegurar que esos datos conforman un registro único en la plataforma de servicios del PSCo.

La validación puede realizarse por ejemplo sobre bases de datos públicas o privadas, o mediante la solicitud a la persona de datos que generen un cierto grado de confianza en la correspondencia de su identidad digital con su identidad física.

El medio de identificación digital se obtiene y asocia mediante una verificación de la evidencia presentada por parte del solicitante. Por ejemplo, el medio de identificación digital "usuario y contraseña" se genera durante el proceso de registro electrónico por la persona y es activado mediante el envío de un enlace (que caduca luego de un periodo apropiado, por ejemplo 24 horas), a la casilla de correo electrónico indicada por el solicitante. El solicitante debe acceder a dicho enlace para activar su identificación digital.

Nivel Medio (RID2)

El nivel medio requiere de la presencia de la Persona Física para acreditar su identidad y asociar los medios digitales a su identidad digital registrada.

El registro puede comenzar en línea, pero se requiere una instancia presencial de validación de la identidad donde además se realizará la asociación de los medios digitales que luego serán utilizados en el proceso de autenticación.

Para la validación de la identidad en la instancia presencial, se requiere la exhibición de un documento nacional que identifique a la Persona Física, como por ejemplo el documento nacional de identidad emitido por la Dirección Nacional de identificación Civil (DNIC) o pasaporte. Se deberá realizar una validación del documento presentado y comprobación de la foto de la persona.

Los medios de identificación digital asociados a la persona durante el registro son considerados robustos.

El procedimiento de asociación del medio digital al solicitante debe estar ligado a su instancia presencial, pudiendo continuar en línea luego de la instancia presencial. Por ejemplo, mediante la entrega presencial de un código QR, PIN o contraseña necesarios para la activación del medio digital en línea.

Nivel Alto (RID3)

El nivel Alto requiere de presencia de la Persona Física para acreditar su identidad y asociar los medios digitales a su identidad digital registrada.

El registro puede comenzar en línea, pero se requiere una instancia presencial de validación de la identidad donde además se realizará la asociación de los medios digitales que luego serán utilizados en el proceso de autenticación.

Para la validación de la instancia presencial, se requiere la exhibición de un documento nacional que identifique a la Persona Física, como por ejemplo el documento nacional de identidad emitido por la Dirección Nacional de identificación Civil (DNIC) o pasaporte. Se deberá realizar una validación del documento presentado y comprobación de la foto de la persona.

De forma adicional al nivel anterior, durante la etapa de registro se realiza la verificación biométrica de la persona con el propósito de no repudio de su identidad. La verificación biométrica de la persona se realiza utilizando métodos y fuentes de datos para la comparación definidos en la Sección 4.2.

El tipo de medio de identificación digital asociado al solicitante, es un Certificado Electrónico Reconocido de Persona Física que puede ser generado durante o antes de la etapa de registro de identificación digital. En caso de que la persona ya cuente con un Certificado Electrónico Reconocido de Persona Física y por lo tanto generado antes de la etapa de registro, deberá demostrar posesión del medio de identificación digital que contiene al certificado. En este escenario la vida del nuevo certificado a emitir por el PSCo deberá quedar condicionado a la validez del certificado pre existente, durante todo su ciclo de vida.

4.2 Verificación Biométrica

Durante la etapa de registro de identificación digital se lleva a cabo una verificación biométrica de la persona.

El método de verificación biométrica válido es el que utiliza la huella dactilar y la fuente válida de datos para comparación biométrica es la Dirección Nacional de Identificación Civil (DNIC).

Por lo tanto, la verificación biométrica de la persona puede realizarse utilizado la funcionalidad de Match on Card del nuevo documento electrónico de identidad (eID) o mediante un servicio de validación de huellas conectado con la Dirección Nacional de Identificación Civil (DNIC).

4.3 Medios de identificación digital

En la etapa de autenticación electrónica, la prueba de identidad proporcionada por el demandante de una identidad digital depende de la fortaleza de los medios de

identificación utilizados y el mecanismo utilizado para comunicar el resultado de esa autenticación.

Los medios de identificación digital considerados por esta política durante la etapa de autenticación son los siguientes:

Nombre de usuario / Contraseña o PIN: es una cadena de caracteres memorizada y mantenida en secreto por la persona. El nombre de usuario puede ser elegido por la persona o generado por el proveedor de identidad. Para la contraseña o PIN hay distintos niveles de fortaleza según la conformación de sus caracteres. El documento "Digital identity Guidelines" 800-63B [9] del NIST define la fortaleza de este tipo de medios digitales.

Lista de códigos: Una lista de códigos a menudo se usa en combinación con una contraseña estática o PIN dentro del sistema de autenticación. Un ejemplo son los códigos derivados de las tarjetas de coordenadas. Para más detalles sobre este medio digital, tomar como referencia el documento "Digital identity Guidilenes" 800-63B [9] del NIST en la sección "Look-Up Secret Verifiers".

Dispositivo de contraseña de un solo uso (OTP-One Time Password): es un dispositivo de hardware personal que genera una contraseña de "una sola vez" que es válida para una única sesión de autenticación y que esta sincronizado con el sistema de validación.

Dispositivo Criptográfico de Software: clave criptográfica almacenada en un disco, dispositivo USB u otro medio de comunicación. La autenticación se logra probando la posesión y el control de la clave.

Dispositivo Criptográfico de Hardware: es una tarjeta inteligente o medio similar que contiene una clave criptográfica protegida por hardware. La autenticación se logra probando la posesión del dispositivo y el control de la clave.

Certificado Electrónico Reconocido de Persona Física (CERPF): Certificado Electrónico Reconocido cuyo suscriptor es una Persona Física, emitidos en exclusividad por los PSCA y sujetos a los requerimientos de la Política de Persona Física de la UCE.

Los medios digitales definidos en la presente política toman como referencia el documento Digital identity Guidilenes del NIST 800-63B [9].

4.4 Autenticación electrónica

Se define la autenticación electrónica como: *"el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital"*

El nivel de confianza que ofrece el proceso de autenticación remota depende de la solidez del mecanismo de autenticación frente a diferentes tipos de ataques y del medio de identificación digital utilizado durante el proceso de autenticación.

En base a los medios digitales definidos en la sección 4.3, asignamos en la siguiente tabla los diferentes niveles de fortaleza desde AE0 a AE3 dependiendo del medio digital utilizado durante el proceso de autenticación electrónica.

Requerimientos mínimos	**Fortaleza del medio digital de identificación electrónica**			
	AE0	**AE1**	**AE2**	**AE3**
Nombre de usuario / Contraseña o PIN: elegido por el solicitante, pero no conforme a las buenas prácticas de fortaleza de contraseñas. Puede ser vulnerable a ataques de fuerza bruta o diccionario.	•			
Nombre de usuario / Contraseña o PIN: elegido por el solicitante y conforme con las buenas prácticas de fortaleza de contraseñas (NIST 800-63). No vulnerable a ataques de fuerza bruta o diccionario.	•	•		
Múltiples factores de Autenticación contemplando: (Dispositivos Criptográficos en Software/Hardware o OTP o lista de códigos) + Contraseña/PIN conforme con las buenas prácticas de fortaleza o biometría.	•	•	•	
Múltiples factores de autenticación contemplando: Certificados electrónicos reconocidos de Persona Física + Contraseña y/o PIN conforme con las buenas prácticas de fortaleza.	•	•	•	•

Cada uno de los niveles descritos desde A0-A3 contempla los requerimientos de todos los niveles anteriores. Para los niveles AE2 y AE3 es necesario incluir multi-factores de autenticación tomando como referencia las guías del NIST en su documento "Digital identity Guidelines" [9] SP 800-63B, Capítulo 4.2.

4.5 Definición de los niveles de identidad digital

En base a los niveles de seguridad durante el proceso de registro de identificación digital y el proceso de autenticación electrónica de una identidad digital, se definen en el siguiente cuadro los niveles de seguridad para una identidad digital.

		Nivel de seguridad en el proceso de autenticación electrónica de una identidad digital			
		AE0	**AE1**	**AE2**	**AE3**
Procedimiento de registro de identificación digital	**RID0**	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 0
	RID1	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 1
	RID2	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 2	NIVEL DE IDENTIDAD DIGITAL 2
	RID3	NIVEL DE IDENTIDAD DIGITAL 0	NIVEL DE IDENTIDAD DIGITAL 1	NIVEL DE IDENTIDAD DIGITAL 2	NIVEL DE IDENTIDAD DIGITAL 3

La tabla anterior describe los diferentes niveles de identidad digital que se pueden alcanzar dependiendo de los niveles de seguridad en el registro de identificación y los niveles de seguridad en el proceso de autenticación.

La combinación de los niveles AE (Autenticación Electrónica) y RID (Registro de Identificación digital) se realizó teniendo en cuenta el paradigma de seguridad en el que el nivel de seguridad está dado por el eslabón más débil, por lo tanto, siempre se obtendrá el valor más bajo, por lo que resulta:

Nivel de identidad digital 0: Se configura cuando el nivel de registro es RID0 y el nivel de autenticación es AE0 o superior. También se configura cuando el nivel de registro es RID0 o superior y el nivel de autenticación AE0.

Nivel de identidad digital 1: Se configura cuando el nivel de registro es RID1 y el nivel de autenticación es AE1 o superior. También se configura cuando el nivel de registro es RID1 o superior y el nivel de autenticación AE1.

Nivel de identidad digital 2: Se configura cuando el nivel de registro es RID2 y el nivel de autenticación es AE2 o superior. También se configura cuando el nivel de registro es RID2 o superior y el nivel de autenticación AE2.

Nivel de identidad digital 3 (Equivalente a presencial): Es el único nivel de identidad digital equivalente al presencial. Se configura cuando el nivel de seguridad en el procedimiento de registro es RID3 y el nivel de autenticación es AE3.

5. Servicio de confianza de identificación digital.

Un PSCo acreditado para prestar el servicio de identificación digital bajo el contexto de la presente Política dispone, como parte de sus sistemas, de un componente denominado Proveedor de identidades (IdP).

El propósito del Proveedor de Identidades es que los usuarios registrados en el servicio de identificación del PSCo cuenten con un único conjunto de medios digitales de identificación y punto de autenticación, para hacer uso de servicios de terceros.

En otras palabras, el Proveedor de Identidades (IdP) de un PSCo brinda el servicio de autenticación a Proveedores de Servicio (SP), mediante una integración técnica y de confianza entre ambos sistemas.

El rol del IdP de un PSCo finaliza luego del proceso de autenticación electrónica y comunicación del resultado de ese proceso al Proveedor de Servicio (SP), quien, como consecuencia de este proceso, verifica el nivel de identidad digital obtenido por el usuario en el IdP y lo utiliza para otorgar los accesos a sus servicios que considere pertinentes.

El Proveedor de Identidades (IdP) es el responsable técnico del proceso de autenticación electrónica de los usuarios registrados en el servicio de identificación digital del PSCo y, por lo tanto, el encargado de:

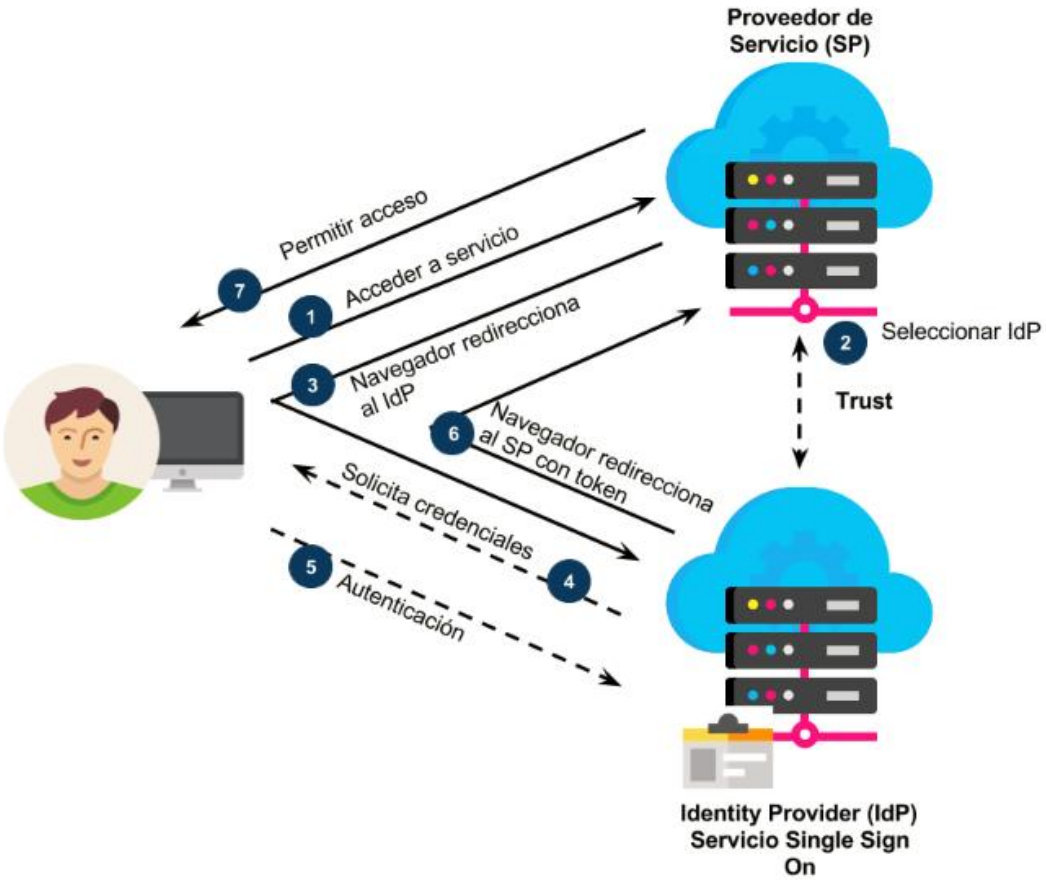
-solicitar los medios digitales correspondientes al Usuario del servicio de identificación digital.

-aceptar o rechazar la autenticación del Usuario del servicio de identificación digital.

-asignar el nivel de seguridad correspondiente a la identidad digital según las condiciones definidas en la presente política.

-transmitir el resultado del proceso de autenticación y por tanto el nivel de identidad digital del Usuario a los Proveedores de Servicio (SP) mediante aserciones.

En el siguiente diagrama se ejemplifica el proceso de autenticación de un Usuario sobre el Proveedor de Servicios (SP) a través del Proveedor de Identidades (IdP) perteneciente a los sistemas del PSCo.



1-El usuario desea acceder a un servicio ofrecido por el Proveedor de Servicio (SP).

2-El Proveedor de Servicio (SP) selecciona el Proveedor de Identidades (IdP) del PSCo, en el cual confía el proceso de autenticación electrónica de sus usuarios. En este punto el SP puede brindar la posibilidad de elección del PSCo al usuario.

3-Luego de seleccionado el PSCo, el usuario es redirigido al IdP (perteneciente a un PSCo) para realizar el proceso de autenticación electrónica y presentar los medios digitales correspondientes.

4-El IdP solicita los medios digitales al usuario para el proceso de autenticación electrónica.

5-El usuario realiza el proceso de autenticación electrónica en el IdP presentando los medios digitales.

6-El IdP realiza una redirección al usuario hacia el SP con el resultado de la autenticación contenido en una aserción, incluyendo el nivel de identidad digital logrado por el usuario en el IdP.

7-El SP autoriza o no el acceso a sus servicios, verificando el nivel de identidad digital obtenido por el usuario en el IdP.

Durante el proceso de autenticación descripto en el ejemplo, existe una relación de confianza entre el IdP y SP para el traspaso de la información de autenticación e identidad de los usuarios.

En el siguiente punto se describen las consideraciones técnicas y de seguridad para ese traspaso de información, denominado federación.

6. Federación de identidades y aserciones.

La federación implica la transferencia de atributos de una persona a un tercero que no está involucrado en una transacción a través de aserciones.

Una aserción utilizada para la autenticación es un conjunto de valores de atributos o referencias de atributos asociados con un usuario autenticado que se traspasan del Proveedor de Identidades (IdP) al Proveedor de Servicios (SP) en un sistema de identidad federado. Las aserciones contienen una variedad de información, que incluye ente otros datos: metadatos de aseveración, valores de atributos y referencias de atributos sobre el usuario.

En el caso de una identidad digital de nivel 3 equivalente al presencial, se deberán tener en cuenta por parte de los PSCo las siguientes consideraciones para la implementación de su federación en su componente Proveedor de Identidades (IdP).

-Implementar la estrategia de federación utilizando SAML 2.0 u OpenID Connect.

-Las aserciones deberán ser firmadas por el IdP y cifradas mediante criptografía asimétrica y clave pública perteneciente al Proveedor de Servicios (SP) o criptografía simétrica y clave compartida.

Las consideraciones se basan en el nivel “FAL2” definido por el NIST en el documento “Digital identity Guidelines” [9] SP 800-63C para federación de identidades.

7. Terceros que validan una identidad.

Según el artículo 7 del Decreto N° 70/018[1], es responsabilidad de quienes utilizan servicios de identificación digital requerir, en la prestación de sus servicios, un nivel de seguridad adecuado para la identificación digital de las personas.

Esto quiere decir que el Proveedor de Servicios (SP) que integra los servicios de un PSCo acreditado es responsable de solicitar el nivel de identidad digital adecuado para la operación o funcionalidad, según su negocio.

Por ejemplo:

Si el servicio a utilizar por los usuarios en el SP requiere una garantía de identidad digital de nivel 3, el SP deberá exigir que el usuario se autentique en el IdP del PSCo con un nivel de identidad digital 3.

8. Controles operativos, de seguridad y técnicos

Un PSCo que desee acreditarse para brindar el servicio de identificación electrónica de personas físicas, deberá demostrar cumplimento de estándares y requisitos adecuados en Seguridad de la Información.

Para la definición de estándares y requisitos de seguridad apropiados, se tomará como referencia el Marco de Ciberseguridad publicado por AGESIC [10] aplicado a los sistemas asociados al servicio de identificación del PSCo.

Certificaciones de seguridad como ISO 27001, pueden ser tenidas en cuenta, siempre y cuando se demuestre su aplicación sobre los sistemas asociados al servicio de identificación del PSCo.

De forma adicional, el PSCo deberá demostrar el cumplimiento de las condiciones establecidas para los niveles de seguridad de una identidad digital con nivel equivalente al presencial, establecidas para:

-el procedimiento de registro de identificación digital (sección 4.1),

-la asociación de medios de identificación digital (sección 4.3),

-el proceso de autenticación electrónica (sección 4.4),

-y la federación de identidades (sección 6).

El cumplimiento de las condiciones mencionadas deberá verse reflejado en los procedimientos vigentes del PSCo.

9. Suspensión y revocación de la acreditación de los prestadores de servicios de confianza

La suspensión y revocación de la acreditación de los prestadores de servicios de confianza de generación, almacenamiento y firma electrónica avanzada, así como sus efectos, se regirán por lo establecido para los prestadores de servicios de certificación según la Política de Certificación de la ACRN [6].

10. Cese de actividades del prestador de servicios de confianza acreditado.

Los prestadores de servicios de confianza acreditados que cesen en sus actividades estarán obligados a comunicarlo a través del Diario Oficial y cualquier otro medio electrónico o tradicional que considere pertinente.

Referencias Externas

1. **Poder Ejecutivo, República Oriental del Uruguay.** Decreto N° 70/018 – Reglamentación de los artículos 31 a 33 de la Ley N° 18.600 de 21 de Setiembre de 2009. https://medios.presidencia.gub.uy/legal/2018/decretos/03/cons_min_625.pdf

2. **Poder Legislativo, República Oriental del Uruguay.** Ley N° 18.600 de 21 de Setiembre de 2009 sobre Documento Electrónico y Firma Electrónica. 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. **Reglamento (UE) N° 910/2014,** del Parlamento Europeo, de 23 de julio de 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,** Política de Certificación de la Autoridad Certificadora Raíz Nacional. http://uce.gub.uy/informacion-tecnica/politicas/

7. **Unidad de Certificación Electrónica,** Política de Certificación de Persona Física última versión. http://uce.gub.uy/informacion-tecnica/politicas/

8. **Poder Ejecutivo, República Oriental del Uruguay.** Decreto N° 436/011 de 8 de Diciembre de 2011 - Reglamentación del Documento Electrónico y Firma Electrónica. 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. **Marco de ciberseguridad v 4.0,** https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad-v40.html