Sistema de verificación de edad para el acceso a contenidos en línea

Especificación de uso de la credencial de “Mayoría de Edad”

Versión 1

30 de junio de 2024

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría General de Administración Digital
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
España | digital 2026

AUTOR	Ministerio para la Transformación Digital y de la Función Pública
PROYECTO	Cartera Digital [BETA]
NOMBRE DEL DOCUMENTO	Especificación de uso de la credencial de “mayoría de edad” Sistema de verificación de edad para el acceso a contenidos en línea

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
V1	Ministerio para la Transformación Digital y de la Función Pública	30-06-2024	Versión inicial

Índice

RELACIÓN DE FIGURAS

1 INTRODUCCIÓN

El presente documento tiene como objetivo explicar la solución ad-hoc diseñada para el proyecto Cartera Digital BETA.

Esta solución garantiza que un usuario pueda demostrar ante proveedores de contenido para adultos su mayoría de edad, a la par que asegura la anonimidad de este durante el proceso. De igual forma, esta solución destaca por reducir notablemente el perfilado del usuario, impidiendo así que se pueda llevar a cabo un seguimiento de las distintas operaciones que el usuario lleva a cabo con su cartera.

En términos generales, se ha definido una solución fundamentada en el uso de credenciales verificables, en la que la mayoría de edad del usuario es demostrable mediante la posesión de una credencial emitida por un emisor de confianza. Esta credencial no posee ningún tipo de información vinculable al usuario, a excepción de una clave pública generada en el propio dispositivo. La solución contempla la emisión de esta credencial en lotes, permitiendo la reutilización de cada credencial de forma finita frente a un mismo proveedor de contenidos y, en ningún caso, entre varios proveedores, reduciendo así al mínimo la trazabilidad del usuario a través de la clave pública individual presente en cada credencial.

De forma complementaria, en este documento se detallan aquellos ajustes realizados sobre la solución base, para llevar a cabo la emisión y almacenamiento de aquellas otras credenciales definidas en el marco del proyecto Cartera Digital BETA, que no presentan requerimientos tan exigentes como los asociados a la credencial de mayoría de edad.

> NOTA - Esta solución ha sido diseñada y planteada considerando el estado del arte actual en diferentes tecnologías criptográficas ampliamente extendidas y los principios que se están desarrollando en el reglamento eIDAS2[1]. En cualquier caso, no es una implementación completa de este reglamento que aún se está desarrollando.
>
> Se seguirá trabajando y mejorando en todos los procesos según vaya evolucionando el reglamento eIDAS2 y tecnologías de ZKP[2].

[1] Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital)

[2] Zero Knowledge Protocol, sistemas criptográficos altamente seguros focalizados en la revelación mínima de información

2 ESPECIFICACIÓN DE LA CARTERA DIGITAL BETA

Las credenciales verificables, en el proceso de emisión, se asocian a un DID (identificador descentralizado) generado a partir de la clave pública del usuario final, haciendo de esta manera al DID titular de la credencial verificable de mayoría de edad. Esta asociación, anónima, permite mediante una firma realizada con la clave privada asociada matemáticamente a la clave pública con la que se ha construido el DID, que la credencial verificable solo la pueda presentar el titular de esta, es decir, la credencial firmada por SGAD se presenta a su vez, firmada por el usuario final, de forma que, solo el usuario titular pueda presentar esta a terceros. Esto genera trazabilidad por clave pública, puesto que los proveedores de contenido recibirán siempre la misma clave pública cuando se presente dicha credencial. Con el objetivo de reducir el perfilado de usuarios, la Secretaría General de Administración Digital ha desarrollado la solución que trata el presente documento.

2.1 Emisión de credenciales verificables

2.1.1 Credencial de mayoría de edad

Con el objetivo de reducir la trazabilidad por clave pública y la correlación entre diferentes servicios de los proveedores de contenido, la Secretaría General de Administración Digital (SGAD) emite, bajo una única solicitud, un lote de 30[2] credenciales verificables de mayoría de edad, con un mes de vigencia.

La Cartera Digital [BETA] genera 30 pares de claves (clave pública y clave privada), junto con los DID respectivos, que le serán facilitados al emisor de las credenciales, de forma que cada credencial de mayoría de edad esté vinculada a una clave pública diferente. Durante el proceso de emisión de la credencial se realiza la autenticación del usuario mediante DNI electrónico, certificados cualificados o las claves concertadas del sistema Cl@ve (Cl@ve PIN, Cl@ve móvil o Cl@ve permanente). A partir de los datos recabados en esta autenticación, se realizará una verificación de la edad del ciudadano para finalmente emitir la credencial de mayoría de edad como un lote de 30 credenciales. La siguiente tabla muestra las principales características de esta solución:

Identificación del usuario	Verificación de edad	Emisión de credenciales
DNI electrónico **Requisito**: certificados activos y contraseña (PIN) conocida.	**La verificación de edad se realiza con el propio DNI sin necesidad de consultar otra fuente**.	**Para cada solicitud se genera un lote de 30* credenciales:** • **Anónimas** • Asociada **cada credencial a una clave pública distinta****

[2] Número configurable que se irá modificando según necesidades del sistema

Certificado Cualificado **Requisito:** disponer de un certificado vigente emitido por Proveedores de Servicios de Confianza cualificados.	**Servicio de verificación de identidad de la DGP a través de la Plataforma de Intermediación de Datos (PID)**	• **Vigencia máxima 1 mes** (propuesta inicial) **Pares de 30 claves públicas-privadas se generan dentro del dispositivo**. El **usuario autoriza**, de manera consciente, **la solicitud de dicha emisión y el almacenamiento de la credencial en su cartera**. * Número configurable en el tiempo. **La SGAD, como entidad emisora, no guardará la vinculación entre la identidad de los usuarios y las claves públicas remitidas por los usuarios desde Cartera Digital BETA.
CL@VE (CL@VE Permanente, CL@VE Móvil, CL@VE PIN) **Requisito:** registro previo en CL@VE.		

2.1.2 Resto de credenciales

Además de la credencial de mayoría de edad, la solución Cartera Digital BETA será capaz de solicitar, almacenar y presentar las siguientes credenciales:

- Padrón
- Ausencia de antecedentes por delitos sexuales
- Titulaciones universitarias
- Titulaciones no universitarias

Siguiendo el mismo protocolo de comunicación que el contemplado en el caso de uso de la credencial de mayoría de edad, el resto de las credenciales podrán ser solicitadas con los mismos métodos de identificación. Posteriormente, el emisor consultará los datos necesarios para cada tipo de credencial en la Plataforma de Intermediación de Datos (PID). A diferencia de la credencial de mayoría de edad, la solicitud del resto de credenciales generará una única credencial.

Proceso Identificación del Usuario	Proceso Consulta Datos Credencial	Proceso para la Emisión de Credenciales
DNI electrónico	Servicio de consulta en cada caso a través de la **Plataforma de Intermediación de Datos** (PID)	**Para cada solicitud se genera una credencial** asociada a una clave pública distinta. El **par de claves** pública/privada se genera **dentro del dispositivo**. **El usuario autoriza, de manera consciente**, la solicitud de dicha emisión y el almacenamiento de la credencial en su cartera.
Certificado Cualificado		
CL@VE (CL@VE Permanente, CL@VE Móvil, CL@VE PIN)		

2.2 Presentación de la credencial

La presentación de las credenciales se realizará presentando mediante el protocolo OpenID4VP (OpenID for Verifiable Presentations) la credencial que ha sido emitida.

El caso de la credencial de mayoría de edad requiere de un algoritmo de presentación que garantice la reducción del perfilado del usuario detallado a continuación. Una vez la cartera almacena el lote de credenciales recibido, esta se encuentra en disposición de demostrar la mayoría de edad del usuario ante aquellos proveedores de contenido para adultos que lo requieran.

El proceso de presentación de la credencial de mayoría de edad consta de tres partes principales:

- Validación del proveedor de contenidos: La Cartera Digital [BETA] valida antes de presentar la credencial de mayoría de edad que el proveedor de contenidos sea una entidad de confianza. Dicho proceso se realiza consultando las listas blancas descritas en el marco de confianza del [DOC 1].
- Selección de la credencial: Es un proceso automático, implementado dentro de la aplicación móvil, en el que, del lote de 30 credenciales, se asignan 3 como máximo a cada proveedor de contenidos. Estas se utilizan aleatoriamente dentro de un mismo proveedor un máximo de 10 veces y nunca entre varios servicios. Cuando se realicen 30 usos, 10 por cada una de las 3 credenciales, se seleccionará otro subconjunto de 3 credenciales del lote de 30.
- Presentación de la evidencia: El usuario final confirma la presentación de la credencial y envía esta en forma de evidencia al proveedor de contenidos siguiendo el protocolo OpenID4VP.

Validación previa a la presentación de la credencial	Selección de Credencial (Lote de Credenciales)	Consentimiento y presentación de la Evidencia
La **aplicación móvil valida que el proveedor** de contenidos, solicitante de la credencial, **esté presente en la lista blanca de proveedores de** contenido de **confianza**	El proceso **es automático**, la aplicación móvil Cartera Digital BETA implementará un algoritmo de selección y uso de las credenciales, **transparente al usuario**: **Cada credencial se reutilizará un máximo de 10 veces con un mismo proveedor y nunca entre diferentes proveedores**. Se irán asignando hasta **3 credenciales distintas del lote (10%) por cada proveedor de contenido**. **Si se agota el número de usos de un grupo de credenciales para un proveedor**, se irán asignando nuevas credenciales sin utilizar, si existen disponibles. El registro necesario para este algoritmo se reinicia con cada lote. N**o se mantiene un histórico**.	El usuario **confirma presentar la evidencia de mayoría de edad a una plataforma de contenidos.** Debe tener información clara de qué tipo de credencial se presenta, qué datos personales incluye, y quién la ha solicitado. En la página de "Detalle" (de la aplicación móvil), donde se le muestra esa información, si queda poco tiempo para la caducidad, o pocas credenciales sin usar, se debe indicar que puede proceder a la renovación de la credencial. **Ventajas** **No existe correlación entre diferentes servicios de proveedores** de contenido restringido para adultos. **Menor perfilado de usuarios dentro de un mismo proveedor**, pues estas solo se reutilizan un máximo de 10 veces.

La Cartera Digital BETA debe implementar un algoritmo de selección y uso de las credenciales transparente al usuario que cumpla con las siguientes condiciones:

- Cada credencial se reutilizará un máximo de 10 veces con un mismo proveedor y nunca entre diferentes proveedores.
- Se irán asignando hasta 3 credenciales distintas del lote (10%) por cada proveedor de contenido. La selección de la credencial a utilizar se realizará de forma aleatoria, no siendo necesario haber agotado los 10 usos de una credencial para comenzar a consumir los usos de otra credencial asociada al mismo proveedor.
- Si se agota el número de usos de un grupo de credenciales para un proveedor, se irán asignando nuevas credenciales sin utilizar, si existen disponibles.

El registro necesario para este algoritmo se reinicia con cada lote. No se mantiene un histórico.

A continuación, se representa, a modo de ejemplo ilustrativo, el uso de un lote de credenciales de mayoría de edad, considerando la existencia de múltiples plataformas de contenido para adultos:

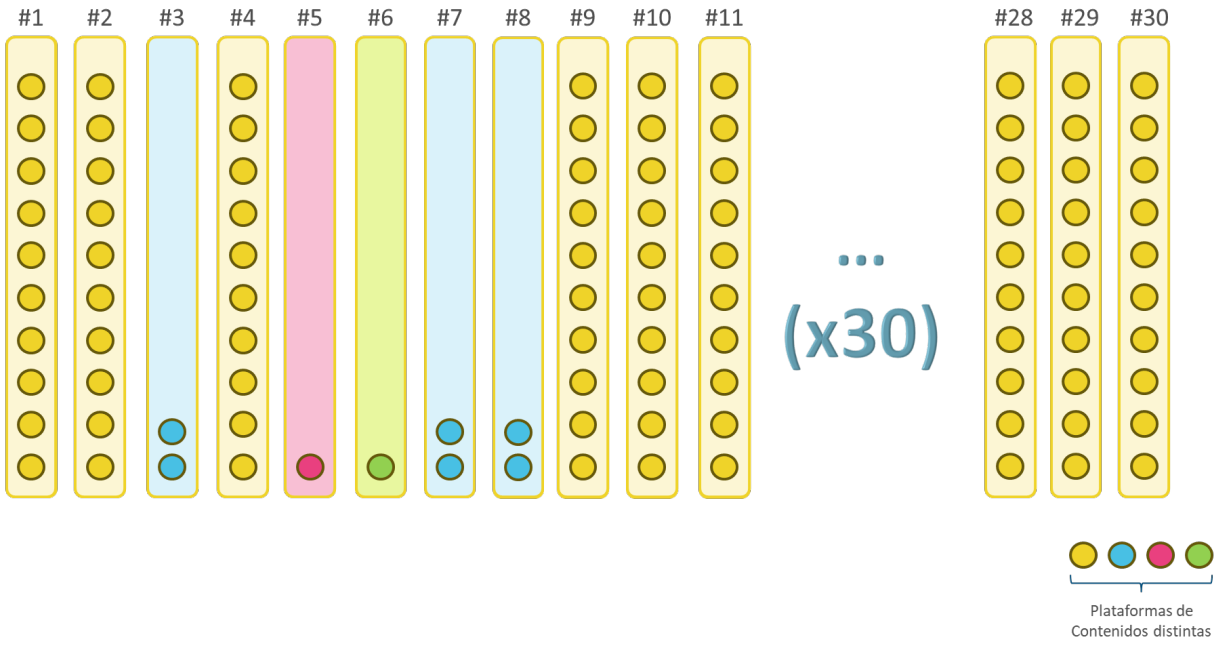

Figura 1: Presentación de credenciales de mayoría de edad

El cumplimiento de estos requerimientos garantiza la no existencia de correlación entre diferentes servicios de proveedores de contenido restringido para adultos, así como un menor perfilado de usuarios dentro un mismo proveedor, ya que cada credencial del lote solo se reutilizará un máximo de 10 veces.

2.3 Renovación de credenciales

A nivel lógico, la funcionalidad de renovación debe seguir el mismo proceso general de emisión de lotes de credenciales, siendo necesaria, por tanto, realizar de nuevo el proceso de autenticación, así como el cotejo de los datos correspondientes, dependiendo del caso de uso.

2.3.1 Credencial de mayoría de edad

Se permitirá renovar el lote de credenciales por caducidad, si quedan menos de 3 días de vigencia o por grado de reutilización, si queda menos de un 10% de credenciales sin uso, en el caso del lote de 30 credenciales, si quedan 3 credenciales sin uso. Si se cumple alguna de estas condiciones, se habilita la posibilidad de realizar una solicitud de renovación, que finalizará con la emisión de un nuevo lote y la eliminación, en la cartera, de las credenciales pertenecientes al lote antiguo. Se evita así una acumulación de credenciales no necesarias.

Requisitos para solicitar la Renovación (regla menos del 10%)	Proceso para la Renovación de la Credencial
Por caducidad Se permite solicitar la renovación si quedan menos de 3 días para la caducidad (3 días sobre 30 días de vigencia[1])	Sigue el **mismo proceso general de la solicitud / verificación de edad / emisión de la 1ª vez. Será necesario, por tanto, identificarse de nuevo y cotejar la mayoría de edad.** Todo el lote activo hasta ese momento se elimina para evitar su uso y la acumulación de credenciales no necesarias.
Por grado de reutilización de las credenciales del lote, llegándose al límite permitido Se permite solicitar la renovación si quedan como mucho un 10% de credenciales sin uso (3 credenciales sobre un lote de 30[2])	

2.3.2 Resto de credenciales

En el caso del resto de credenciales, la caducidad es la única condición para poder realizar una solicitud de renovación, dado que el periodo de vigencia de estas es mayor, cuando queden menos de 30 días se permitirá su renovación. Una vez renovada la credencial la antigua quedará inactiva.

Requisitos para solicitar la Renovación	Proceso para la Renovación de la Credencial
Por caducidad Se permite solicitar la renovación si quedan menos de 30 días para la caducidad	Sigue el **mismo proceso general de la solicitud / emisión de la 1ª vez.** • La credencial caducada o a punto de caducar queda Inactiva en la Cartera Digital BETA.

3 ANEXO I – REFERENCIAS

[DOC 1] Protocolo Verificación de Edad v1.0