Age verification system for access to online content

Specification for the use of the "Age of majority" credential

Version 1

June 30, 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

AUTHOR	Ministry for the Digital Transformation and Civil Service
PROJECT	Digital Wallet ^{BETA}
DOCUMENT NAME	Specification for the use of the “Age of majority” credential Age verification system for access to online content

Document Version Control

VERSION	AUTHOR	DATE	DESCRIPTION
V1	Ministry for the Digital Transformation and Civil Service	30-06-2024	Initial version

Contents

LIST OF FIGURES

1 INTRODUCTION

This document describes the ad-hoc solution designed for the Digital Wallet $^{\text{BETA}}$ project.

This solution ensures that a user can prove their age of majority to adult content providers while maintaining their anonymity. This solution is noteworthy for its significant reduction of user profiling, which in turn prevents tracking of transactions performed by users through their wallets.

In general terms, a solution based on the use of verifiable credentials has been defined, in which the user's age of majority can be proven by the possession of a credential issued by a trusted entity. This credential contains only a public key that is generated on the device itself and no information that can be linked to the user. The solution enables this credential to be issued in batches, which means that each credential can be reused multiple times with the same content provider but not with different providers. This minimizes the likelihood of tracing the user through the unique public key in each credential.

This document details the modifications to the base solution for issuing and storing the other credentials defined within the framework of the Digital Wallet $^{\text{BETA}}$ project, whose requirements are less rigorous than those associated with the credential of the age of majority.

> NOTE - This solution has been designed and proposed considering the current state of the art across widely spread cryptographic technologies and the principles that are being developed in the eIDAS2 regulation[1]. In any case, it is not a complete implementation of this regulation, which is still being developed.
>
> Work on all processes will continue and improvements made as the eIDAS2 regulation and ZKP[2] technologies evolve.

[1] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the establishment of the European Digital Identity Framework)

[2] Zero Knowledge Protocol, highly secure cryptographic systems focused on the minimum disclosure of information.

2 SPECIFICATIONS OF THE DIGITAL WALLET BETA

During the issuance process, the verifiable credentials are linked to a DID (decentralized identifier) that is created using the end user's public key, effectively making the DID the recipient of the verifiable credential confirming the age of majority. Through a signature made using the private key mathematically linked to the public key used to create the DID, this anonymous association guarantees that only the owner can present the verifiable credential. In other words, the credential is signed by **General Secretariat for Digital Administration** (SGAD) and then signed again by the user, ensuring that only the user can present it to third parties. This ensures traceability through the public key as content providers will consistently receive the same public key when the credential is presented. The solution presented in this document, developed by the General Secretariat of Digital Administration, aims to decrease user profiling.

2.1 Issuance of verifiable credentials

2.1.1 The credential of the age of majority

To reduce the traceability by public key and correlation among various content provider services, the **SGAD** (General Secretariat for Digital Administration) issues a batch of 30[2] verifiable credentials of majority, which are valid for one month, in response to a single request.

The Digital Wallet BETA generates 30 pairs of keys (public key and private key), together with the respective DID, for the issuer of the credentials. This ensures that each age of majority credential is linked to a different public key. During the credential issuance process, the user is authenticated using electronic ID, qualified certificates or the agreed keys of the Cl@ve PIN, mobile and permanent system (Cl@ve PIN, Cl@ve móvil o Cl@ve permanente). From the data collected in this authentication, the citizen's age is verified, and the age of majority credential is issued as a batch of 30 credentials. The following table shows the main characteristics of this solution:

User identification	Age verification	Issuance of credentials
Electronic DNI (Digital ID Card) **Requirement**: active certificates and known password (PIN).	**The age is verified using the ID card itself without the need to consult another source**.	**A batch of 30* credentials is generated for each request:** • **Anonymous**

[2] This number is configurable and will be modified according to system needs

Qualified Certificate **Requirement:** have a valid certificate issued by qualified Trust Service Providers.	**General Directorate for the Police identity verification service through the Data Intermediation Platform (PID)**	• **Each credential is associated with a different public key** ** • **Maximum validity 1 month** (initial proposal) **Pairs of 30 public-private keys are generated within the device**. The **user knowingly authorizes the request to issue the credential and store it in his wallet**. * Number configurable over time. **The General Secretariat for Digital Administration, the issuing entity, will not keep the link between the identity of the users and the public keys sent by the users from Digital Wallet $^{\text{BETA Version}}$.
CL@VE (CL@VE Permanente, CL@VE Móvil, CL@VE PIN) **Requirement:** prior registration in CL@VE.		

2.1.2 Other credentials

In addition to the age of majority credential, the Digital Wallet $^{\text{BETA}}$ solution can request, store and present the following credentials:

- Municipal Registry
- No record of sex offenses
- University degrees
- Non-university degrees

All other credentials can be requested using the same identification methods as those used in the age of majority credential use case. Subsequently, the issuer will consult the necessary data for each type of credential in the Data Intermediation Platform. Unlike the credential of majority, the request for the other credentials will generate a single credential.

User identification process	Consultation process credential data	Process for issuance of credentials
Electronic DNI (Digital ID Card)	Consultation service in each case through the **Data Intermediation Platform**.	**A credential associated with a different public key is generated for each request**. The public/private **key pair** is generated **within the device**. The **user consciously authorizes** the request to issue the credential and store it in their wallet.
Qualified Certificate		
CL@VE (CL@VE Permanente, CL@VE Móvil, CL@VE PIN)		

2.2 Presentation of the credential

Presentation of the credential that has been issued using the OpenID4VP (OpenID for Verifiable Presentations) protocol.

The presentation algorithm for the age of majority credential must ensure that user profiling is restricted, as outlined below. After storing a batch of credentials, the wallet can demonstrate the user's age of majority to adult content providers who demand it.

The process of presenting the credential of majority has three main parts:

- Content provider validation: Before presenting the age of majority credential, the Digital Wallet ^{BETA} checks that the content provider is a trusted entity. This process is carried out by consulting the whitelists described in the [DOC 1] trust framework.
- Credential selection: The mobile application implements an automatic process whereby up to three credentials are assigned to each content provider from the batch of thirty. These can be used randomly up to 10 times within the same provider but can never be used across multiple services. After 30 uses, with 10 uses allocated to each of the 3 credentials, a new subset of 3 credentials will be chosen from the batch of 30.
- Presentation of the evidence: The end user confirms the presentation of the credential and sends it in the form of evidence to the content provider following the OpenID4VP protocol.

Validation before the credential is presented	Credential selection (Batch of credentials)	Consent and presentation of the Evidence
The **mobile application checks that the content provider** who is requesting the credential, **is on the whitelist of trusted** content providers	The process **is automatic**, the Digital Wallet ^{BETA} mobile application will implement an algorithm for selecting and using the credentials, which is **transparent to the user**: **Each credential will be reused a maximum of 10 times with the same content provider and can never be used across different content providers**. Up to **3 different batch credentials (10%) will be assigned to each content provider**. **If the number of uses of a group of credentials for a content provider is exhausted**, new unused credentials will be assigned, if available. The record necessary for this algorithm is restarted with each batch. No **history log is kept**.	The user **confirms they wish to present the evidence of age of majority to a content platform.** The user must receive precise details regarding the type of credential provided, the personal data it contains, and the entity that requested it. When there is little time left until expiration, or few unused credentials, a notification must be displayed on the "Details" page (of the mobile application) where the above information is shown, informing the user they can renew the credential. **Advantages** **There is no correlation between the services of providers** of restricted content for adults. **Less profiling of users within the same content provider**, as these can only be reused a maximum of 10 times.

The Digital Wallet ^{BETA} must implement an algorithm for selecting and using the credentials that is transparent to the user and that meets the following conditions:

- Each credential will be reused a maximum of 10 times with the same content provider and can never be used across different content providers.
- Up to 3 different batch credentials (10%) will be assigned to each content provider. The credential that used will be selected randomly, and there is no need to exhaust all 10 uses of one credential before starting to use another credential linked with the same content provider.
- If a group of credentials for a content provider has reached its maximum usage, new unused credentials will be assigned, if they are available.

The record necessary for this algorithm is restarted with each batch. No history log is kept.

Here is an example that illustrates the use of a batch of age of majority credentials in the context of multiple adult content platforms:

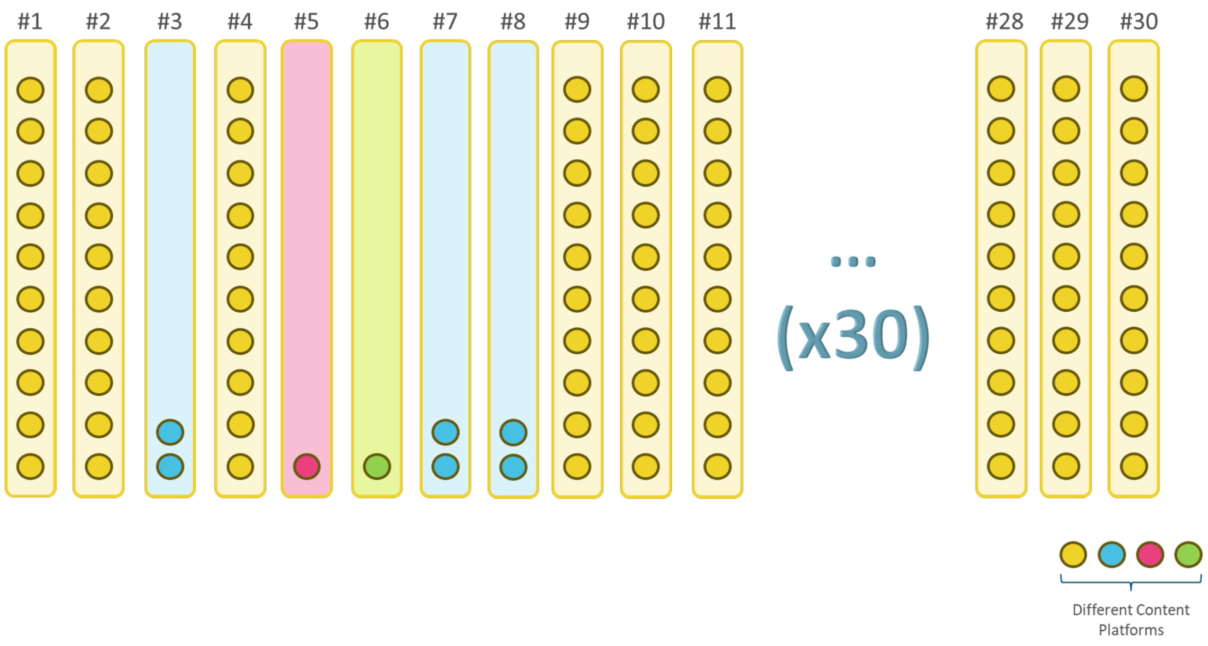

Figure 1. Presentation of credential of the age of majority

Complying with these requirements ensures there is no correlation between adult content providers' services and reduces user profiling within the same provider. Each credential in the batch will be reused a maximum of 10 times.

2.3 Renewal of credentials

Logically, to renew credentials, the same general process of issuing batches must be followed, requiring the repetition of the authentication process and the collation of corresponding data, according to the use case.

2.3.1 The credential of the age of majority

The batch of credentials can be renewed before expiration if there are less than three days left until expiry, or based on the level of reuse, if less than 10% of credentials remain unused. Additionally, in the case of a batch of 30 credentials, renewal can occur if there are only three credentials unused. If any of the specified conditions are met, the option to request a renewal is enabled. This results in the issuance of a new batch and the removal of the old batch's credentials from the wallet. This avoids accumulating unnecessary credentials.

Requirements to apply for renewal (under 10% rule)	Process for renewing the credential
On expiration It is allowed to request renewal if there are fewer than 3 days before expiration (3 days out of 30 days validity)	This follows the **same general process of the 1st application /age verification/ issuance. Therefore, the user must identify themselves again and their legal age must be checked.** The entire active batch up to that point is deleted to avoid its use it and accumulating unnecessary credentials.
Because of the reuse of the batch credentials reaching the allowed limit Renewal can be requested if up to 10% of credentials unused (3 credentials out of a batch of 30)	

2.3.2 Other credentials

For all other credentials, renewal requests are only permitted upon expiration, as their validity periods are longer. Renewal may be allowed if there are fewer than 30 days until expiration. Once the credential has been renewed, the old one will be inactive.

Requirements for requesting renewal	Process for renewing the credential
On expiration Renewal may be requested if there are fewer than 3 days before expiration	This follows the **same general process of the 1st request / issuance.** • The expired or expiring credential is inactive in the Digital Wallet BETA.

3 ANNEX I – REFERENCES

[DOC 1] Age Verification Protocol v1.0

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