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

Ecosistema de verificación 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

ÍNDICE

1 Componentes de la solución

2 Solicitud de evidencia

3 Evidencia

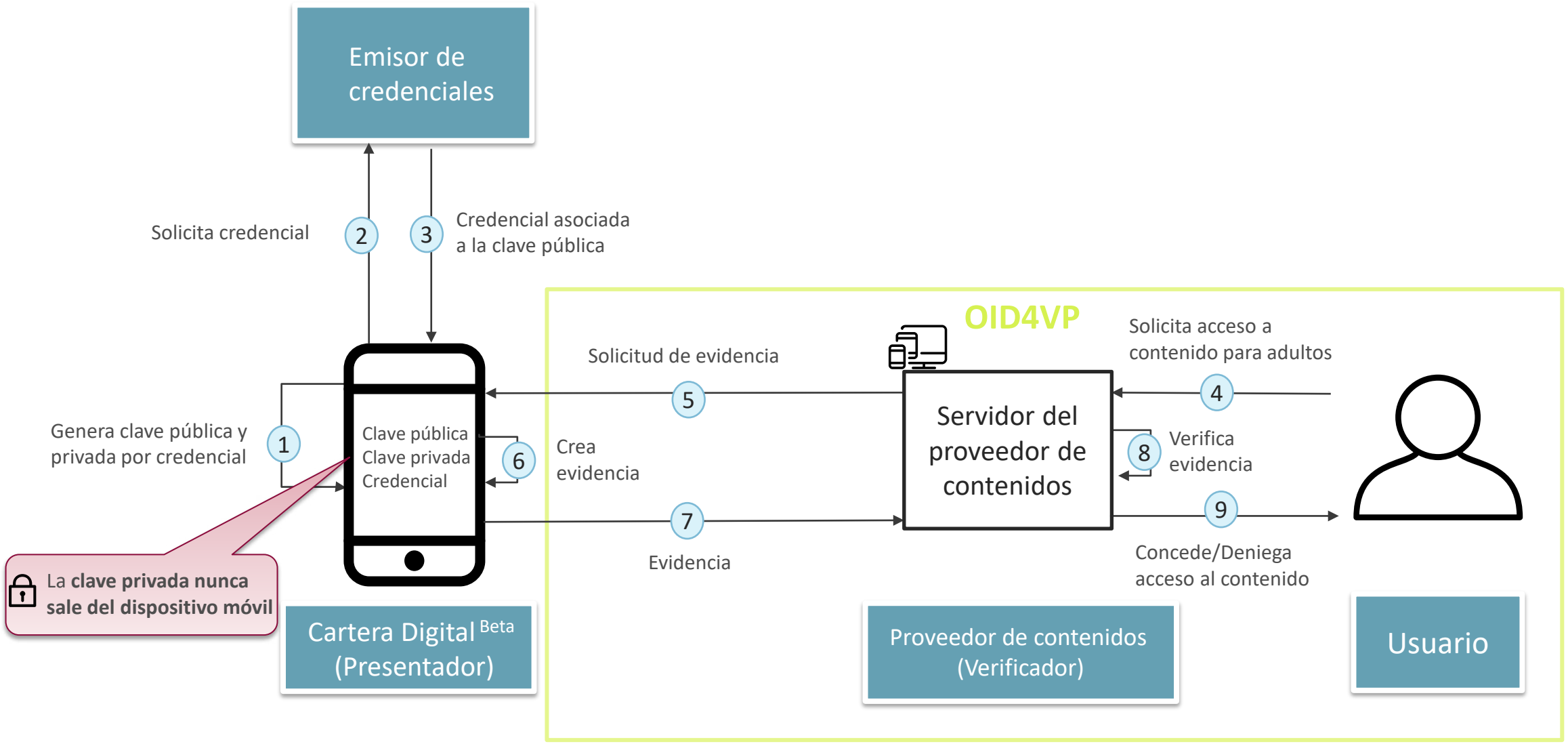
4 Verificación de la evidencia

5 Flujo de presentación de la evidencia

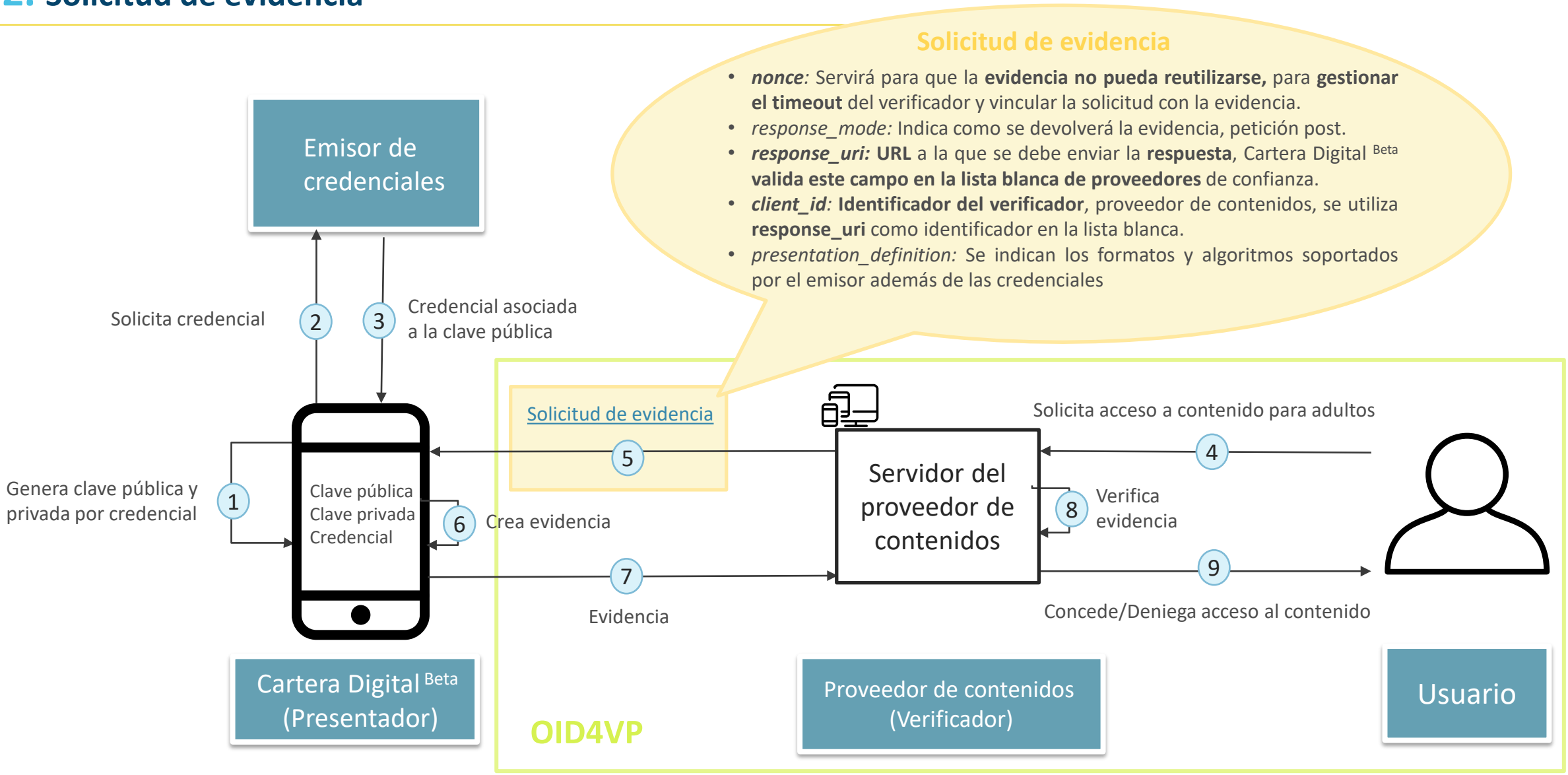
6 Modelo de datos

Componentes de la solución

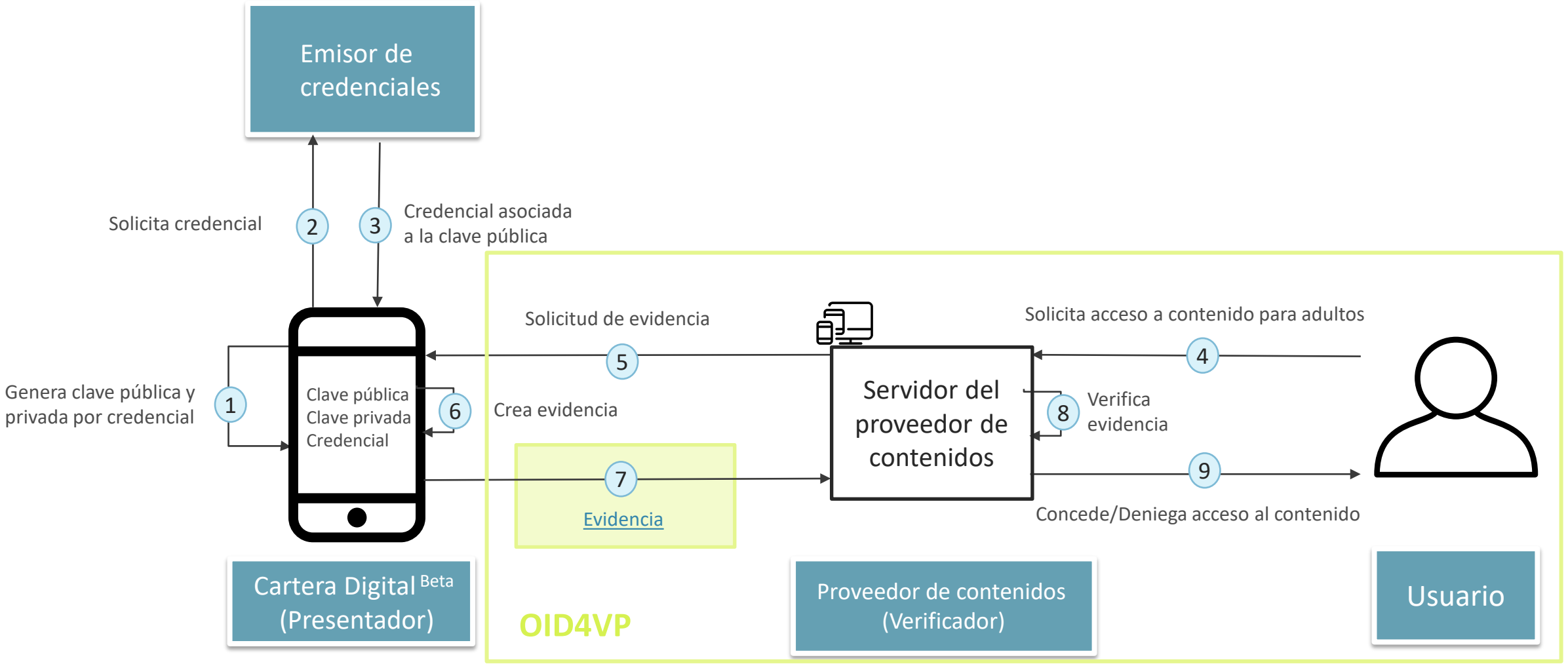
1. Componentes de solución general



2. Solicitud de evidencia



3. Evidencia


Emisor de credenciales
Solicita credencial
2
3
Credencial asociada a la clave pública
Genera clave pública y privada por credencial
1
Clave pública
Clave privada
Credencial
6
Solicitud de evidencia
5
Crea evidencia
7
Evidencia
Servidor del proveedor de contenidos
Solicita acceso a contenido para adultos
4
8
Verifica evidencia
9
Concede/Deniega acceso al contenido
Cartera Digital Beta (Presentador)
OID4VP
Proveedor de contenidos (Verificador)
Usuario

4. Evidencia

Evidencia (OID4VP)

Cabecera

(*typ, cty*…)

Cuerpo

(*iat*, *exp*, *aud*…)
presentation_submission (Se utiliza para indicar al verificador formatos, algoritmos, …)
***nonce**: "*1b0a82db-9c82-4693-b9ca-97f62f4d5081"

Presentación Verificable (W3C)

Cabecera

(*typ, cty*…)

Cuerpo

iat (Fecha de creación)
exp (Fecha de **expiración de la evidencia**, podría ser **1 minuto**)
aud (**Entidad para la que se genera la evidencia***)*

Credencial Verificable (W3C)

Cabecera

(*typ, cty*…)

Cuerpo

type: ["VerifiableCredential", "K"] (Atributo que indica si el usuario está autorizado a acceder)
id: "did:key:${ClavePúblicaUsuario}"
validUntil: "2024-05-08T10:59:52Z" (Fecha de expiración, expira en un mes)
iss: "did:key:${ClavePúblicaEmisor}"

Prueba

d2k4O3FytQJf83kLh-HsXuPvh6yeOlhJETg… (**firma** del **EMISOR**)

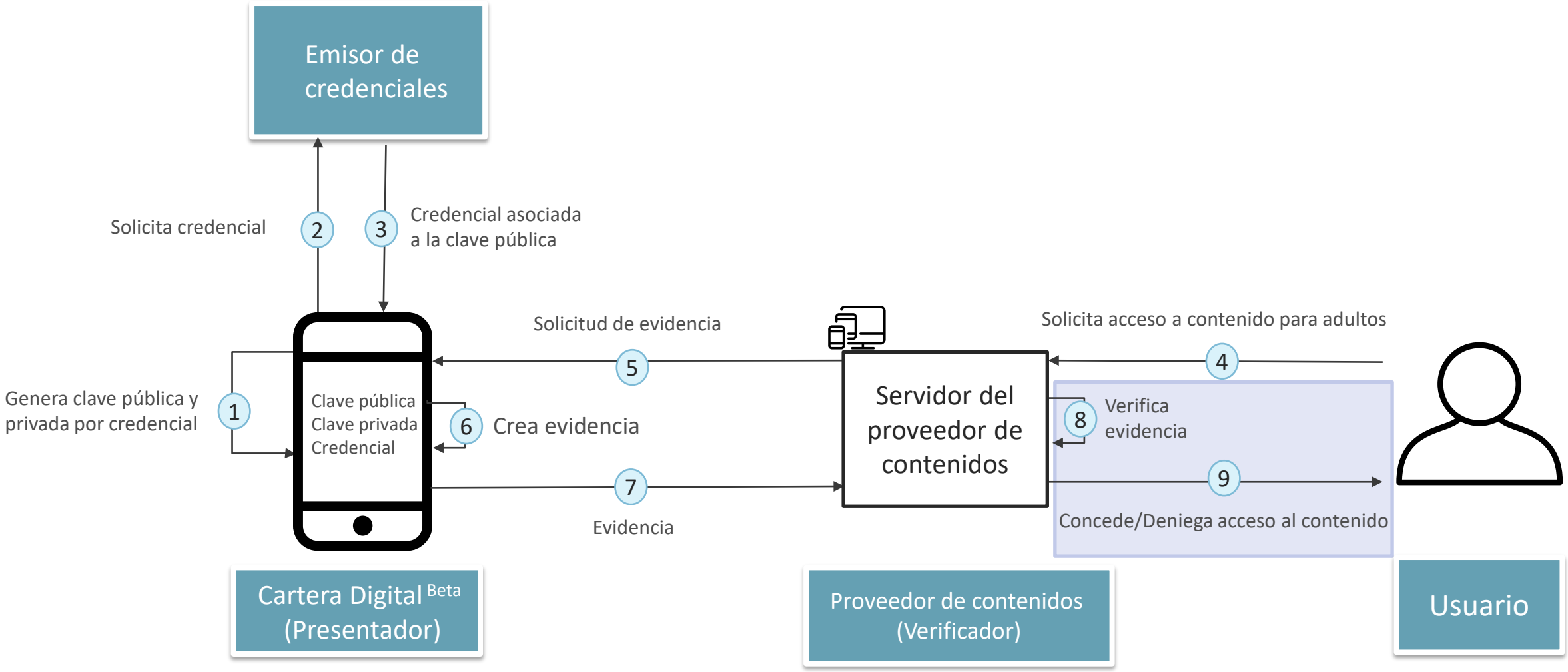
Prueba

Xakou0923klmrw… (**firma** del **USUARIO**)

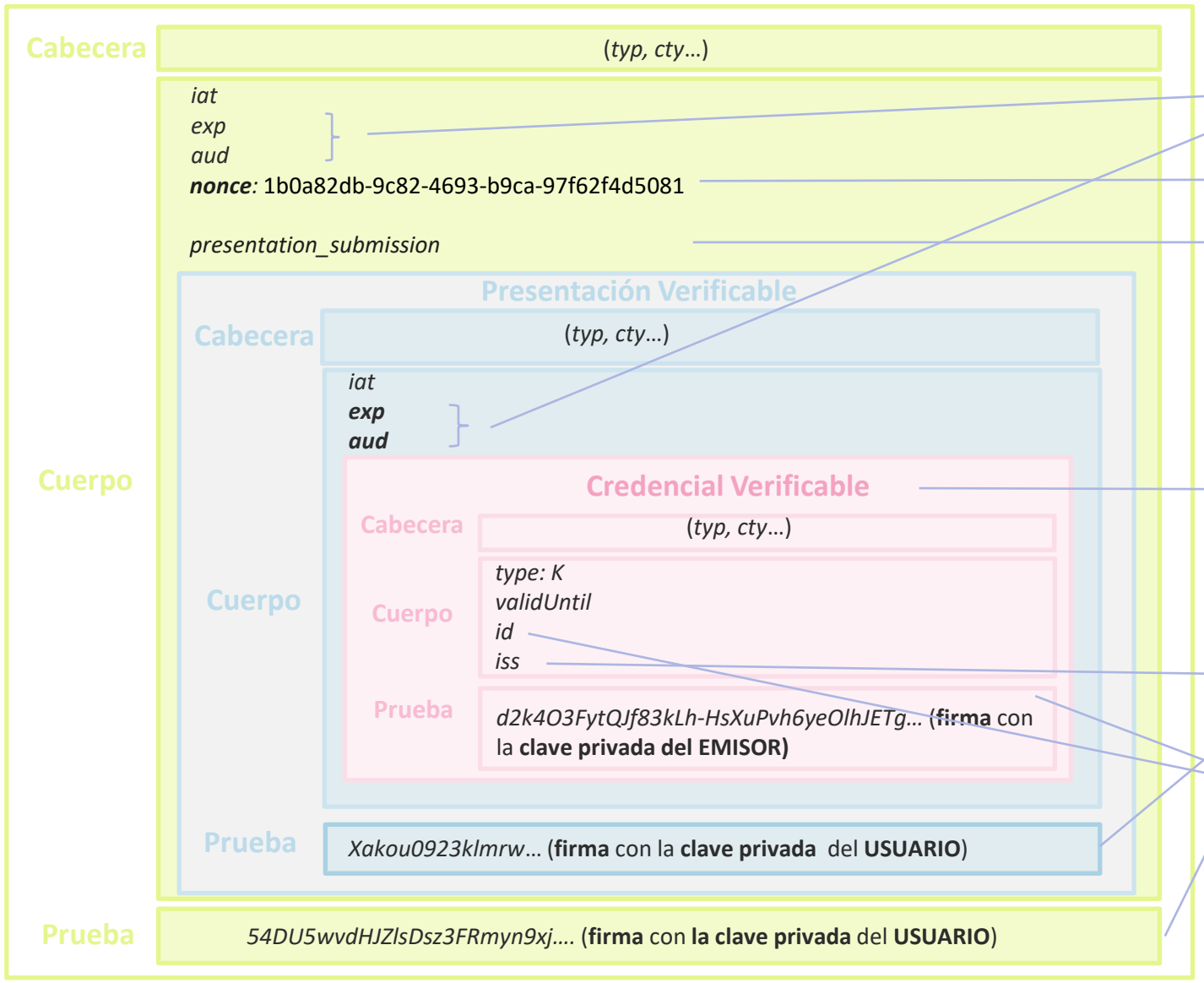
Prueba

54DU5wvdHJZlsDsz3FRmyn9xj…. (**firma** del **USUARIO,** para que **no se puedan presentar credenciales de otras personas**)

5. Verificación de la evidencia



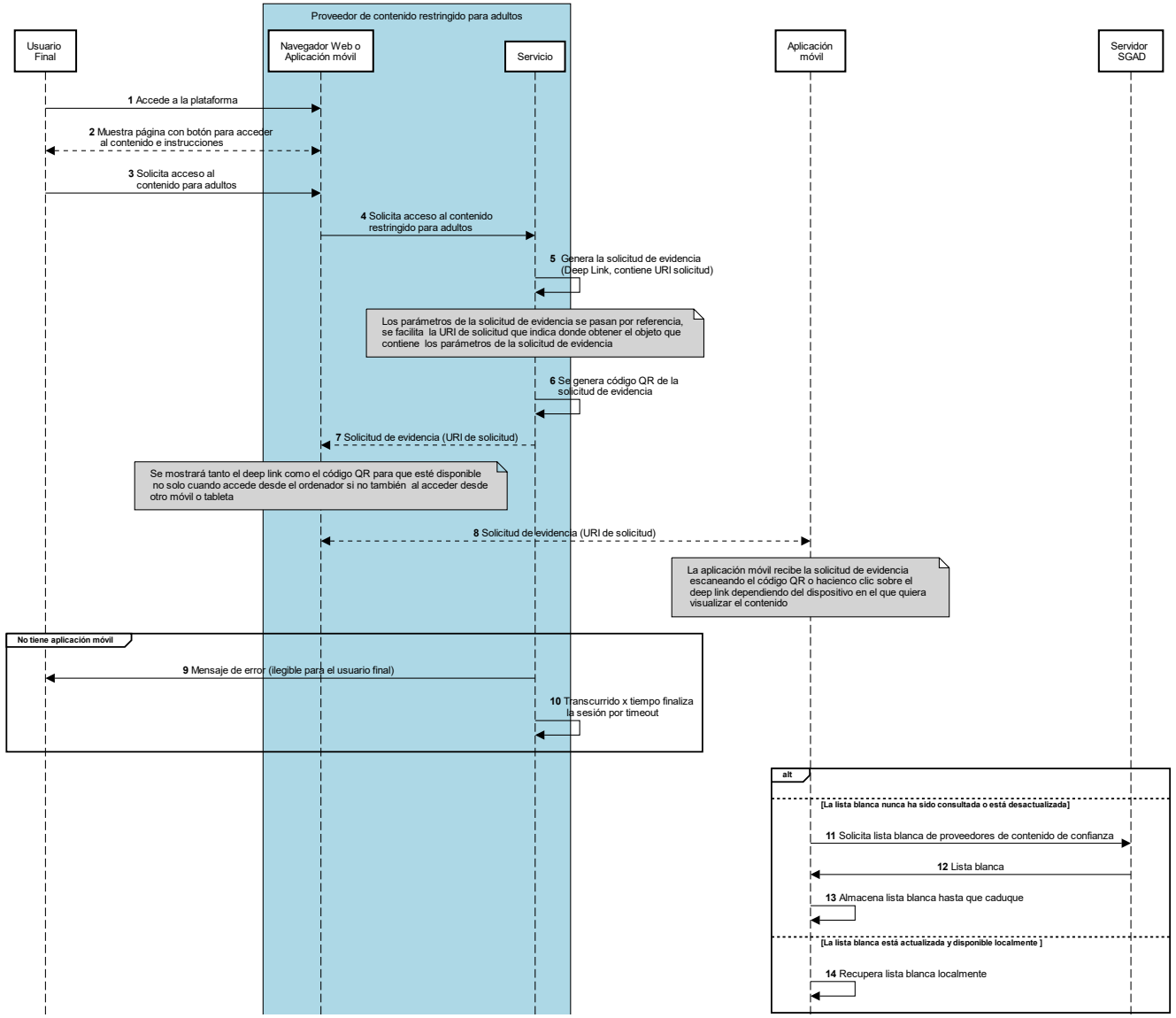
6. Verificación de la evidencia



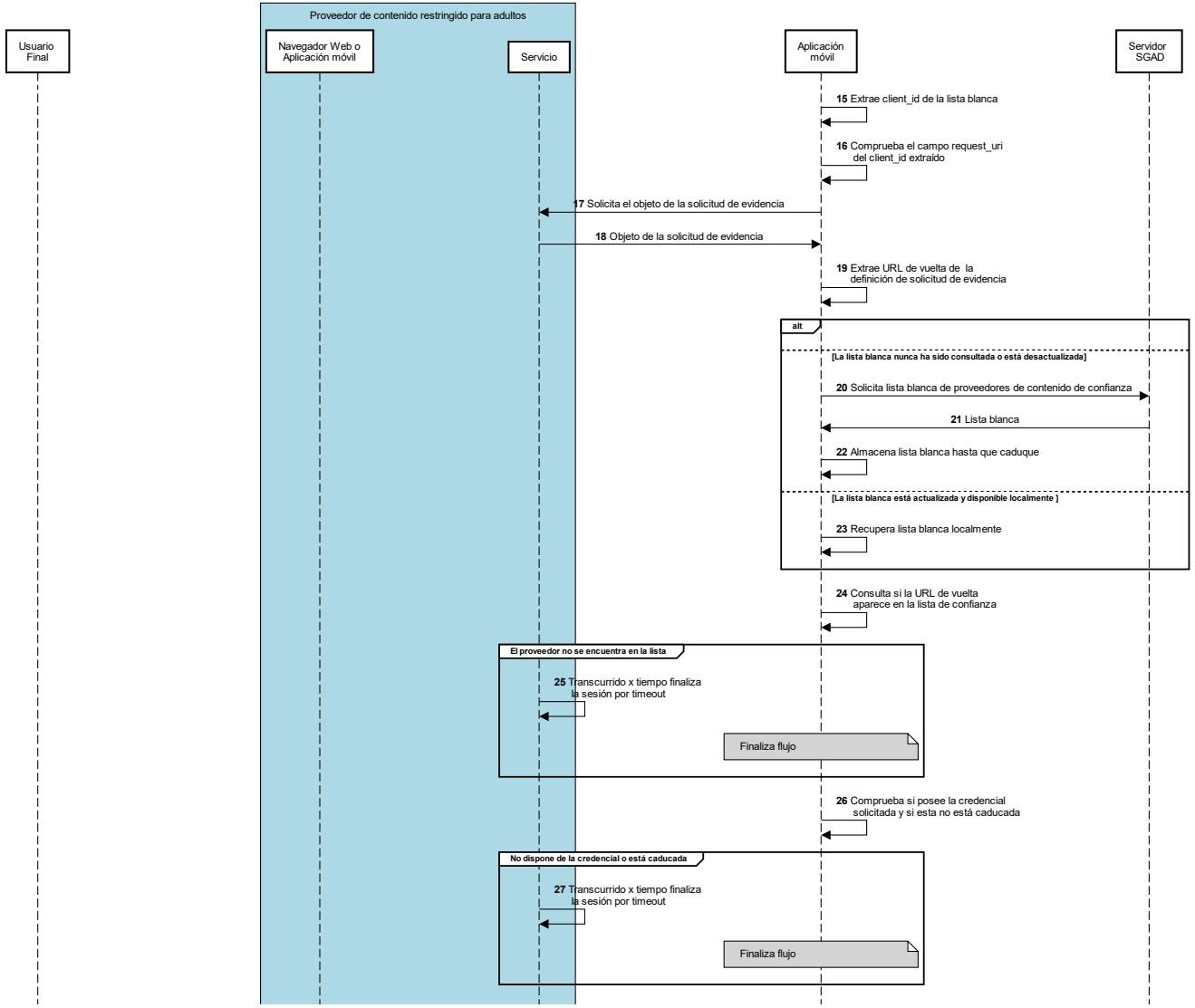
1. Se valida que no esté caducado y que haya sido generada para ese proveedor de contenido en concreto.
2. Se recupera la sesión junto a la solicitud de evidencia. Se comprueba que no haya sido previamente utilizado.
3. Se comprueba que se responde a lo solicitado en la solicitud de evidencia, por ejemplo, que se incluye la credencial *ageOverNN* y que se utilizan formatos y algoritmos soportados por el proveedor de contenido.
4. Se verifica que no esté caducada y que *ageOver18* sea *true.*
5. Se verifica que ambas firmas de la evidencia coincidan con el titular de la credencial.
6. Se verifica que el emisor de la credencial sea una entidad de confianza consultando la lista blanca de emisores de confianza y se valida la firma con la clave pública de este.

Flujo de presentación de la evidencia

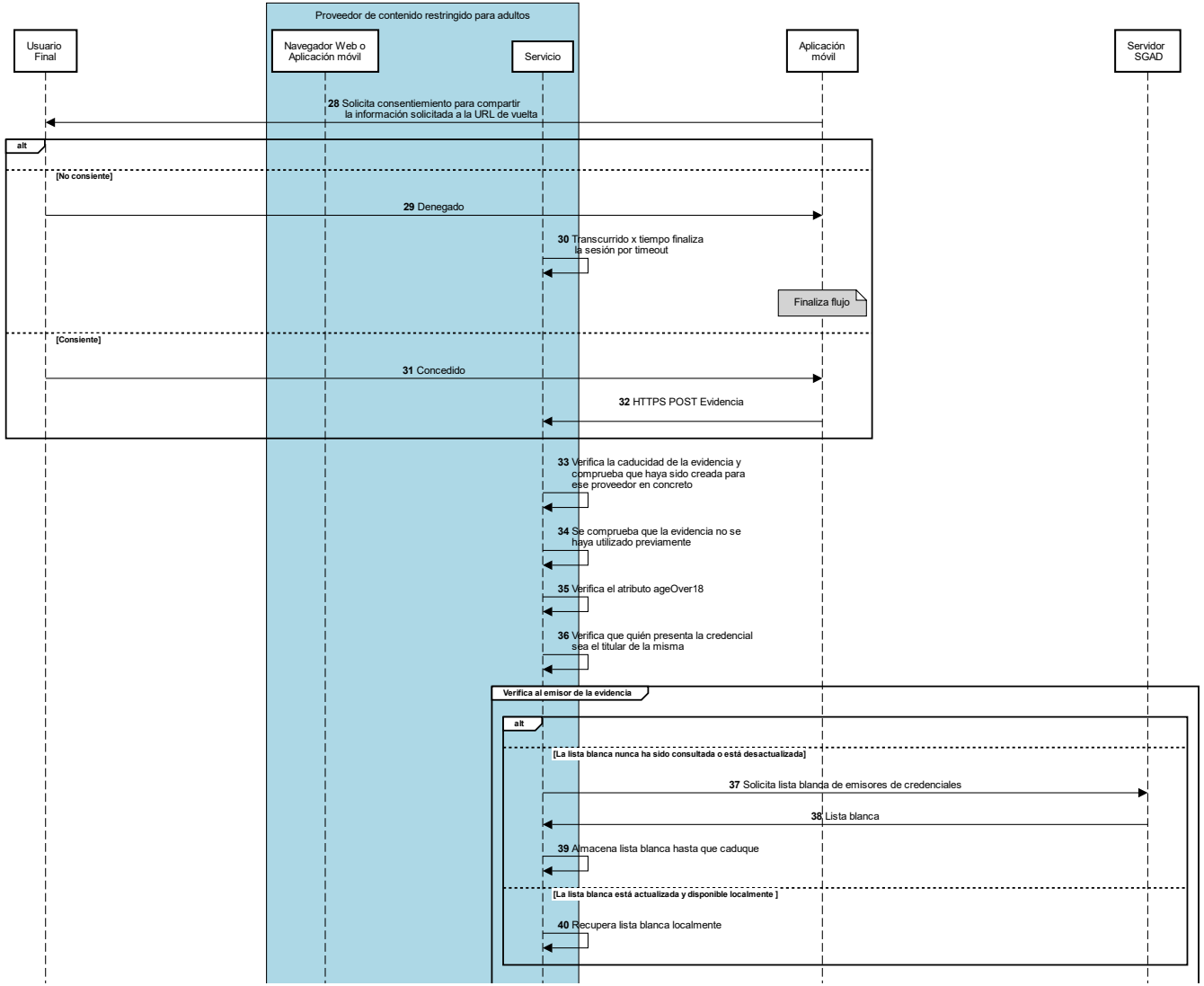
10. Flujo de presentación de la evidencia



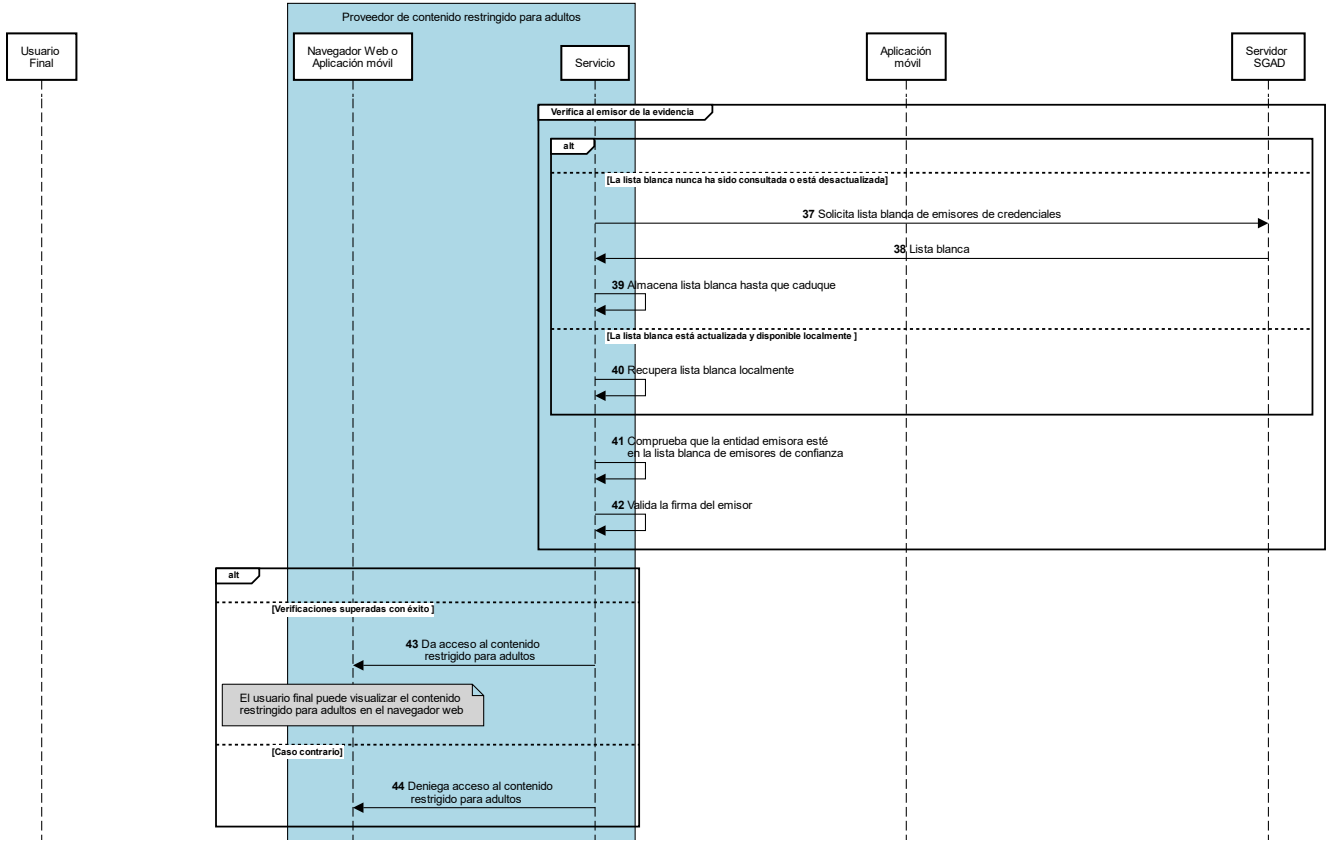
10. Flujo de presentación de la evidencia



10. Flujo de presentación de la evidencia



10. Flujo de presentación de la evidencia



Modelo de datos de la solución

11. Modelo de datos - Presentación Verificable

Cuerpo de la Presentación Verificable

```
{
  "id":"urn:uuid:00000000-0000-0000-0000-000000000000",#Identificador único de la presentación
  "type": [
    "VerifiablePresentation "                          #Tipo de la presentación
  ],
  "verifiableCredential":[                             #Listado de credenciales verificables incluidas en la presentación
   {
    "@context" :"https://www.w3.org/ns/credentials/v2",   #Mapea conceptos abreviados en la credencial a URLs
    "id":"data:application/vc+ld+json+jwt;${VCJWT}",      #Sigue el RFC data URL, contiene la credencial verificable en formato JWT
    "type":"EnvelopedVerifiableCredential"                #Tipo estipulado en W3C para credenciales verificables envueltas
   }
  ],
  "holder":"did:key:z2dmzD81cgP…t35e "                 #Identificador descentralizado generado a partir de la clave pública del usuario
                                                       que genera la presentación, debe coincidir con el titular de las credenciales
                                                       que se presenten
}
```

Ir a la evidencia

11. Modelo de datos - Presentación Verificable

Presentación Verificable asegurada con la Clave Privada del usuario final


```
eyJraWQiOiJFeEhrQk1XOWZtYmt2VjI2Nm1ScHVQMnNVWV9OX0VXSU4xbGFwVXpPOHJv
IiwiYWxnIjoiRVMzODQifQ.eyJAY29udGV4dCI6WyJodHRwczovL3d3dy53My5vcmcvb
nMvY3JlZGVudGlhbHMvdjIiLCJodHRwczovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhb
HMvZXhhbXBsZXMvdjIiXSwidHlwZSI6IlZlcmlmaWFibGVQcmVzZW50YXRpb24iLCJ2Z
XJpZmlhYmxlQ3JlZGVudGlhbCI6W3siQGNvbnRleHQiOiJodHRwczovL3d3dy53My5vc
mcvbnMvY3JlZGVudGlhbHMvdjIiLCJpZCI6ImRhdGE6YXBwbGljYXRpb24vdmMrbGQra
nNvbitqd3Q7ZXlKcmFXUWlPaUpGZUVoclFrMVhPV1p0WW10MlZqSTJObTFTY0hWUU1uT
lZXVjlPWDBWWFNVNHhiR0Z3VlhwUE9ISnZJaXdpWVd4bklqb2lSVk16T0RRaWZRLmV5S
kFZMjl1ZEdWNGRDSTZXeUpvZEhSd2N6b3ZMM2QzZHk1M015NXZjbWN2Ym5NdlkzSmxaR
1Z1ZEdsaGJITXZkaklpTENKb2RIUndjem92TDNkM2R5NTNNeTV2Y21jdmJuTXZZM0psW
kdWdWRHbGhiSE12WlhoaGJYQnNaWE12ZGpJaVhTd2lhV1FpT2lKb2RIUndPaTh2ZFc1c
GRtVnljMmwwZVM1bGVHRnRjR3hsTDJOeVpXUmxiblJwWVd4ekx6RTROeklpTENKMGVYQ
mxJanBiSWxabGNtbG1hV0ZpYkdWRGNtVmtaVzUwYVdGc0lpd2lSWGhoYlhCc1pVRnNkV
zF1YVVOeVpXUmxiblJwWVd3aVhTd2lhWE56ZFdWeUlqb2lhSFIwY0hNNkx5OTFibWwyW
lhKemFYUjVMbVY0WVcxd2JHVXZhWE56ZFdWeWN5ODFOalV3TkRraUxDSjJZV3hwWkVae
WIyMGlPaUl5TURFd0xUQXhMVEF4VkRFNU9qSXpPakkwV2lJc0ltTnlaV1JsYm5ScFlXe
FRZMmhsYldFaU9uc2lhV1FpT2lKb2RIUndjem92TDJWNFlXMXdiR1V1YjNKbkwyVjRZV
zF3YkdWekwyUmxaM0psWlM1cWMyOXVJaXdpZEhsd1pTSTZJa3B6YjI1VFkyaGxiV0VpZ
lN3aVkzSmxaR1Z1ZEdsaGJGTjFZbXBsWTNRaU9uc2lhV1FpT2lKa2FXUTZaWGhoYlhCc
1pUb3hNak1pTENKa1pXZHlaV1VpT25zaWRIbHdaU0k2SWtKaFkyaGxiRzl5UkdWbmNtV
mxJaXdpYm1GdFpTSTZJa0poWTJobGJHOXlJRzltSUZOamFXVnVZMlVnWVc1a0lFRnlkS
E1pZlgxOS5kMms0TzNGeXRRSmY4M2tMaC1Ic1h1UHZoNnllT2xoSkVMVm81VEY3MWd1N
2Vsc2xReU9mMlpJdEFYcnRiWEY0S3o5V2l2TmR6dE9heXo0VlVRME13YTh5Q0Raa1A5Q
jJwSC05U190Y0FGeGVvZUo2WjRYbkZ1TF9ET2ZrUjFmUCIsInR5cGUiOiJFbnZlbG9wZ
WRWZXJpZmlhYmxlQ3JlZGVudGlhbCJ9XX0.54DU5wvdHJZlsDsz3FRmyn9xj23IC56OW
6t6RQMQQuw9omLOxZ8Dkvg-12AADWJeKfYRaCKEIV7YmBkCe1JkQdV5NGxxtOvES4Ip-
VARZqVLi201sakDFERMMfbrBl7n
```


```
{
    “iss”: "did:key:z2dmzD81cgP…t35e“, #emisor de la evidencia
    “iat”: "did:key:z2dmzD81cgP…t35e“  #fecha de emisión de la evidencia
    “exp”: "1618496351",               #fecha de expiración de la evidencia,
                                       formato NumericDate JWT. Valor
                                       establecido a 1 minuto.
    “vp” :{
      "id":"urn:uuid:00000000-0000-0000-0000-000000000000",
      "type": [
        "VerifiablePresentation“
      ],
      "verifiableCredential":[
        {
          "@context" :"https://www.w3.org/ns/credentials/v2",
          "id":"data:application/vc+ld+json+jwt;${VCJWT}",
          "type":"EnvelopedVerifiableCredential“
        }
      ],
     "holder":"did:key:z2dmzD81cgP…t35e“
    }
}
```

11. Modelo de datos - Presentación Verificable

Presentación Verificable Envuelta

```
{
  "@context": "https://www.w3.org/ns/credentials/v2",     #Mapea conceptos abreviados en la presentación a URLs
  "id":"data:application/vp+ld+json+jwt;${VPJWT}”,        #Sigue el RFC data URL, contiene la presentación verificable en formato
                                                          JWT
  "type": "EnvelopedVerifiablePresentation“               #Tipo estipulado en W3C para presentaciones verificables envueltas
}
```

11. Modelo de datos- Solicitud de evidencia

Solicitud Evidencia

URI que referencia los datos de la solicitud de autorización. Contiene los siguientes parámetros en formato *application/x-www-form-urlencoded:*

- request_uri: URI absoluta de la solicitud del objeto de autorización. Por ejemplo,

```
https%3A%2F%2Fauth.sitioadultos.com%2Frequest.json%2FGkurKxf5T0Y-mnPFCHqWOMiZi4VS138cQO_V7PZHAdM
```

- client_id: Identificador del proveedor de contenido, se utilizará la URL de vuelta establecida como identificador en la lista blanca.

Se propone que la solicitud de autorización sea un *deep link*:

```
ageverification://authorize?client_id={response_uri}&request_uri=https%3A%2F%2Fauth.sitioadultos.com%2Frequest.json%2FGkurKxf5T0Y-mnPFCHqWOMiZi4VS138cQO_V7PZHAdM
```

10. Modelo de datos – Objeto de la solicitud de evidencia

Objeto de la solicitud de evidencia

```
{
        “response_type”: “vp_token”,                    #Indica que la respuesta es un token, en concreto, el token representa una presentación verificable
        “client_id_schema”: “redirect_uri”,             #Tipo de esquema de cliente, define
        “response_mode”: “direct_post.jwt”,             #Modo de respuesta, dado que el verificador puede estar en un dispositivo diferente la respuesta de
                                                        autorización se enviará mediante una petición POST en lugar de hacerlo mediante redirección
        “response_uri”: ${URI de vuelta},               #URI a la que la aplicación móvil envía la respuesta de autorización, deberá validar que es de confianza en la lista blanca
                                                        de proveedores de confianza donde el identificador de cada proveedor será su URI de vuelta
        “client_id”: “${response_uri}”,                 #La URI de vuelta se utiliza como identificador del cliente, proveedor de contenidos
        “nonce”: “07d54d63-7136-3ff1-11d8-f 9d17bdb0620”,      #Identificador único que utiliza el proveedor de contenido para vincular la solicitud con la respuesta, se
                                                                utilizará para gestionar el tiempo que se mantiene la sesión abierta y que no se reutilice la presentación
        “presentation_definition”: {
              “id”: “32f54163-7166-48f1-93d8-f f217bdb0653”,  #Identificador único de la definciión de presentación
              “format”: {                                    #Formatos soportados por el verificador
                    “jwt_vc”: {
                        "alg": [“RS512”]                     #Algoritmos soportados por el verificador
                     },
                    “jwt_vp”: {
                        "alg": [“RS512”]                     #Algoritmos soportados por el verificador
                     },

              },
              “input_descriptors”: [{
                    “id”: “Age over 18”,                                  #Identificador de los campos solicitados
                    “constrainst”: {
                          “fields”: [{
                                “path”: [
                                      “$.credentialSubject.ageOver18”     #Campos que se validarán primero en la verificación de la presentación
                                 ]
                          }]
                    },
                    “format”: {                                           #Formato soportado por el verificador para el conjunto de elementos
                                                                           solicitado en el input_descriptor que lo contiene en específico
                          “jwt_vc”: {
                               "alg": [“RS512“]
                          }
                     }
              }]
        }
}
```

11. Modelo de datos - Presentación de QR (solicitud) desde proveedor de contenidos

Cuerpo de la evidencia

```
{
      “vp_token”: {                                                    #presentación verificable
        "@context": "https://www.w3.org/ns/credentials/v2",
        "id":"data:application/vp+ld+json+jwt;${presentacionVerificableJWT}”,
        "type":"EnvelopedVerifiablePresentation"
      },
      “presentation_submission”:{
            "id": "a30e3b91-fb77-4d22-95fa-871689c322e2",
            "definition_id": “32f54163-7166-48f1-93d8-f f217bdb0653”,       #id de la definición de presentación
            "descriptor_map": [{
                        "id": “Age over 18”,                                    #id input descriptor
                        "format": "jwt_vc",
                        "path": "$.verifiableCredential[0]”
            }]
      },
      “nonce”: “07d54d63-7136-3ff1-11d8-f 9d17bdb0620”                    #Campo nonce de la solicitud de autorización, sirve para gestionar
                                                                          la sesión y asegurar que la presentación no sea reutilizada
}
```

Evidencia firmada por el titular de la credencial

Se asegura la evidencia firmando con la clave privada del usuario final el cuerpo de la respuesta de autorización, asegurando así, que **aunque se intercepte la evidencia** y se solicite un nonce al proveedor de contenido **no se podrá enviar una respuesta de autorización válida** puesto que no se posee la clave privada del titular de la credencial incluida en la evidencia.

Gracias por su atención