aepd agencia española protección datos

TECHNICAL NOTE

DESCRIPTION OF THE PROOFS OF CONCEPT OF SYSTEMS FOR AGE VERIFICATION AND PROTECTION OF MINORS FROM INAPPROPRIATE CONTENT

December 2023

CONTENTS

I. INTRODUCTION

The AEPD has proposed the “Decalogue of principles. Age verification and protection of minors from inappropriate content” (the Decalogue) which includes the principles that a system for age verification and protection of minors from inappropriate content must comply with. The objective of said Decalogue is to guarantee the protection of the minor's best interests and the principles, rights, and obligations established in the GDPR. Furthermore, to indicate the guidelines to guarantee the protection of the fundamental rights of all Internet users.

The protection of minors from inappropriate content must be framed to protect the minor's best interests. These best interests are broader than preventing their access to inappropriate content, they encompass the protection of all their fundamental rights, and in particular, all aspects that may affect their safety, health, development, and privacy.

The protection of minors from inappropriate content cannot be an excuse to violate fundamental rights, particularly of minors themselves. The fundamental rights of all Internet users must be protected regardless of age. Similarly, fundamental rights, particularly those related to data protection, cannot be used as an excuse for not developing appropriate measures to protect minors.

The protection of minors from uncontrolled exposure to content or sites inappropriate for them should not become the surveillance of all Internet users. In particular, this protection does not legitimize the continuous and massive collection of minors' data for their profiling and for the permanent exposure of this vulnerable group to the advertising that enriches these sites.

There are already solutions on the market that serve to verify the age of Internet users, and many of them do not address the global protection of the rights and freedoms of citizens. Some are based on sharing credentials or identity attributes with content providers so that they can perform age checks directly; others are based on the creation of specialized identity providers that process browsing data and history; others rely on age estimates made through the application of artificial intelligence techniques to facial images collected in real-time and many work with a combination of the above features. However, many of these solutions involve data processing that does not comply with the basic requirements of the GDPR, including high-risk operations for the rights and freedoms of users and, worse, establish significant limitations in protecting the minor's best interests and their fundamental rights.

A system that will affect all Internet users, with a particular impact on minors, must scrupulously comply with data protection regulations and involve high-risk processing to the extent that it can significantly impact fundamental rights. Age verification cannot imply the identification of Internet users, their detection (especially if they are minors), the linking of their activity in different services, excessive data gathering or processing, profiling, the use of potentially discriminatory systems that limit citizens' ability to operate in the digital world, etc.

The Decalogue of principles published by the AEPD establishes the way to reconcile both aspects: the best interests of minors and the fundamental rights of all Internet users.

This Decalogue sets the minimum conditions that a system for the protection of minors from inappropriate content must meet, among others, preventing a minor from being located through the Internet using these systems, guaranteeing anonymity of all users, minimize the data processed or disclosed to third parties, ensure that families participate in the criteria to protect minors or establish systems that generate trust, are suitable and protect the best interest of minors and the fundamental rights of citizens.

II. Proofs of concept

To demonstrate that compliance with the Decalogue is possible and that this type of solution could already be offered on the Internet, the AEPD, in collaboration with the General Council of Professional Colleges of Computer Engineering, has developed several proofs of concept that implement a protection system that is derived from said Decalogue.

The PoCs developed at the AEPD demonstrate that it is possible to put these principles into practice in real scenarios, showing their suitability and the practical application of the principle of necessity and data minimization.

Proofs of concept are fundamentally based on the fact that a clear separation is possible between identity management, age verification and content filtering. Therefore, they demonstrate that the identity providers that currently implement the right to self-identity of Spanish and European citizens are already sufficient and that it is not necessary to build parallel digital identity systems to access content inappropriate for minors. A fundamental aspect of avoiding discrimination and bias is that the age verification solution can interact with those identity providers most suitable for the user, giving them greater confidence. In particular, it is aimed at being compatible with the digital wallet and with the privacy guarantees that guide the eIDAS2 initiative and, at the same time, that they can be extrapolated to universal identity providers, such as those that currently issue passports or other physical or digital solutions.

The proofs of concept are also based on the fact that protection against inappropriate content can be carried out on the user's device, with people having complete control over their identity and age so that the systems are fully auditable and transparent.

Finally, the PoCs demonstrate that the location, monitoring and profiling of minors over the Internet (or Internet users in general) is not necessary to implement protection from inappropriate content.

The trust generated in citizens concerning these systems is essential to guarantee their suitability. An approach that does not generate sufficient trust in users will cause discrimination, self-censorship and, finally, rejection.

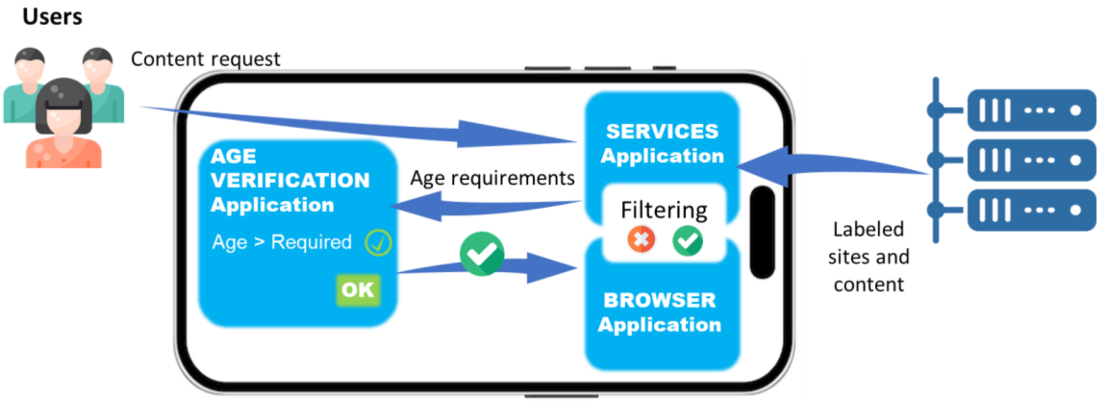
These PoCs open the door to other solutions or alternatives that can also comply with the principles by opting for different architectures or design decisions.

A. HIGH-LEVEL DESCRIPTION OF THE PoCs

The proofs of concept are based on the use of two applications:

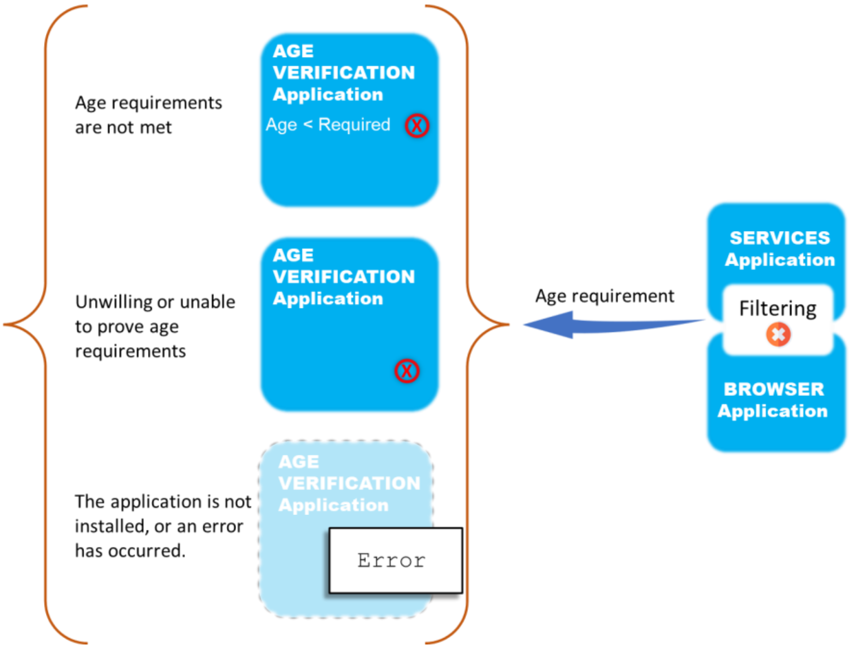
- A content access application, such as a browser or an app specific for an Internet service (the app to access a social network, for example). This application receives content from the content provider on the Internet. If it is labelled for "all audiences", it is displayed without limitations. If it is labeled as "for adults" or "inappropriate for minors", it is only shown after the user's age is verified.
- An age verification application, which receives the verification request from the previous application, verifies the user's age and generates the condition of a person "authorized to access" if the user can prove the age necessary to access that content (could be 14 years, 18 years, or other figures).

An essential aspect is that the entire age verification process and the protection from inappropriate content is carried out without leaving the user's device or accessing external resources.



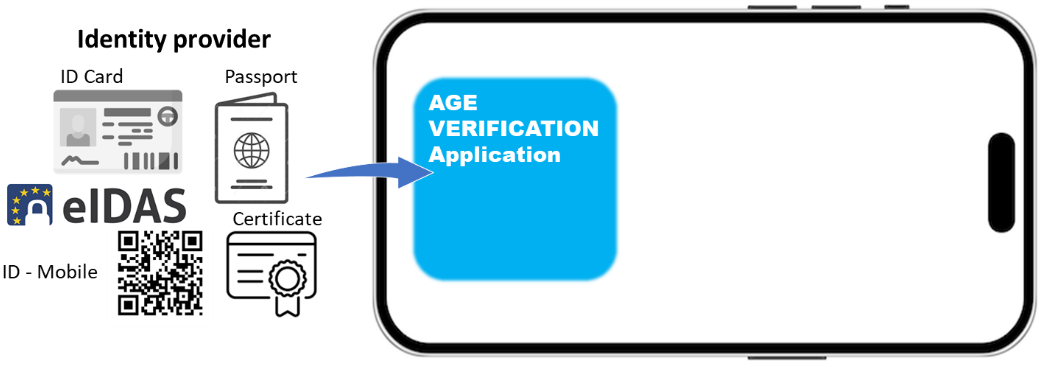
High-level description of the system implemented in the PoCs

To avoid the detection of minors on the Internet, it is crucial to keep in mind that when the age verification application does not respond with the condition of a person "authorized to access", it may be for several reasons: because the user does not have the required age, but also because they have not been able or wanted to prove it, because an error has occurred, etc. All of these situations should not be distinguishable from each other.


Age requirements are not met
AGE VERIFICATION Application
Age < Required
Unwilling or unable to prove age requirements
AGE VERIFICATION Application
The application is not installed, or an error has occurred.
AGE VERIFICATION Application
Error
Age requirement
SERVICES Application
Filtering
BROWSER Application

Situations in which the condition of a person "authorized to access" is not generated

It is also important to mention that the age verification application requires the user to prove their age in a certain way without exposing their identity. An age verification app is used, which acts as an intermediary between different identity providers and the application that must verify the age to allow access to certain content (the browser, for example). The developed PoCs have been based on using QR codes, digital identities stored in electronic wallets or physical identity documents. Both processes, registration in an identity management system to use the identity and age verification, are considered independent. The age verification app, running only on the personal device and provided by an entity selected by the user, prevents identity dissemination. By placing itself between the identity and the generation of the condition "authorized to access," this app allows auditing so that the identity is never revealed to content providers or third parties.



Identity management independent of age verification, which will therefore be anonymous

Content filtering policies are also executed on the device to avoid the exposure of the user's status as a minor, that is, to prevent there being a way to locate minors over the Internet. The objective of minors' protection is not to allow Internet providers to find, identify and profile minors. On the contrary, providers must remain ignorant of the minor status of users. Furthermore, the execution of content filtering policies on the device itself has other collateral advantages: greater transparency, auditability of the execution of the policies, parental adjustment of the policies for minors with particular vulnerabilities, etc.

The PoCs have simulated content providers that provide labeled content. For example, the scheme proposed by Age.xml, which emerged in the MIRACLE (Machine-readable and interoperable age classification labels in Europe) project funded by the European Commission, can be used.

B. PoC FOCUSED ON COMPUTERS AND VIDEOGAME CONSOLES

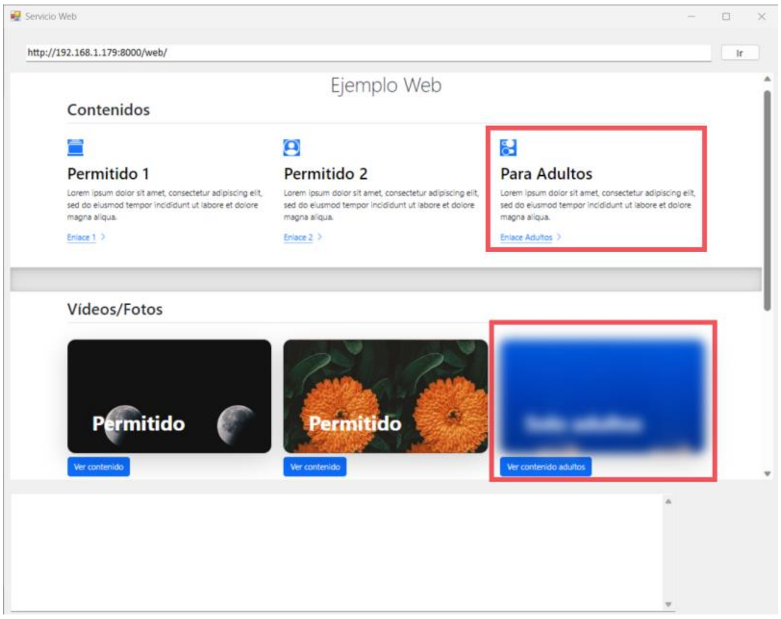
The first proof of concept aims to demonstrate a solution to the problem of accessing content from a device, such as a computer or video game console, running an operating system from the Windows family. In the following link, you can see an example of the execution of the developed solution.

The user must use the age verification application developed at the Agency and a modified browser installed on said device to work with it.

A brief description of this proof of concept follows. Before using the system, the user would obtain a QR code, provided, for example, by the FNMT developments for the Ministry of the Interior, on their mobile phone. The QR information may or may not be anonymous, as the verification app will block the identity from spreading. The user's age attribute will be stored in the verification application for a limited period to avoid correlations between QR requests and access to adult content.

Next:

1. The user requests access to content labeled “for adults” from the browser.
2. The content is received with its label and the display of the content on the device is preventively blocked (in the PoC the content is shown blurred). In this way, the status of a minor is not revealed to the content provider, the content is always served.



Ejemplo Web

Contenidos

Permitido 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Enlace 1 >

Permitido 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Enlace 2 >

Para Adultos

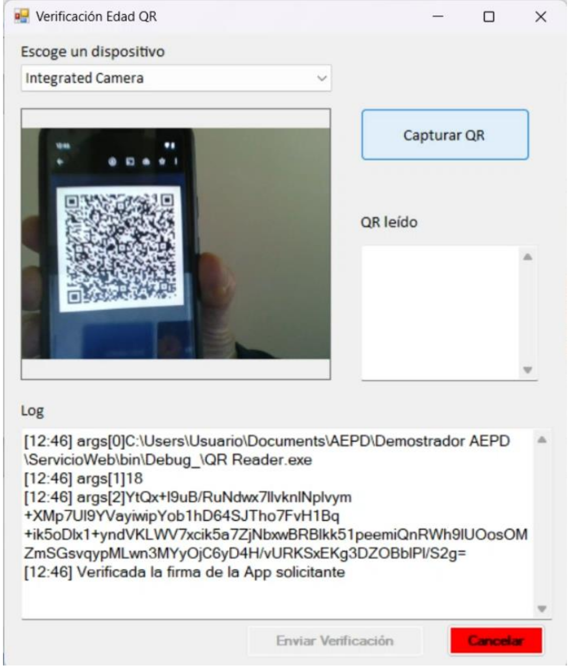
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Enlace Adultos >

Vídeos/Fotos

Browser that receives labeled content, but does not display it if it requires age verification

3. The browser calls the verification application to determine if the user is of the appropriate age to access the content (over 14, over 18, or other conditions). The age verification application asks the user to show their QR code (on their mobile phone) close to the computer or console camera.

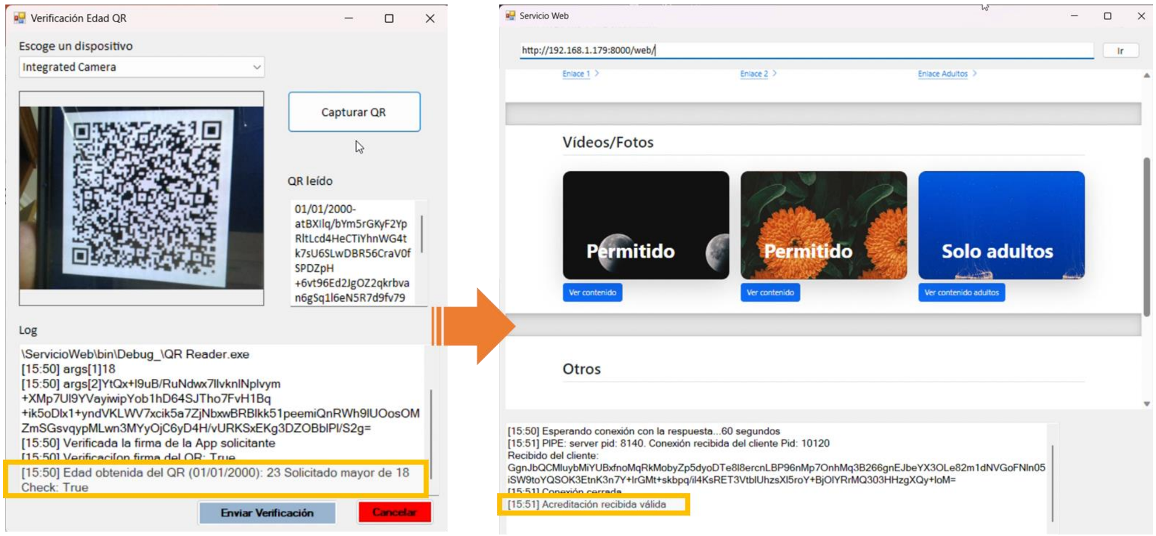


```
[12:46] args[0]C:\Users\Usuario\Documents\AEPD\Demostrador AEPD
\ServicioWeb\bin\Debug_\QR Reader.exe
[12:46] args[1]18
[12:46] args[2]YtQx+I9uB/RuNdwx7IlvknINplvym
+XMp7UI9YVayiwipYob1hD64SJTho7FvH1Bq
+ik5oDlx1+yndVKLWV7xcik5a7ZjNbxwBRBlkk51peemiQnRWh9lUOosOM
ZmSGsvqypMLwn3MYyOjC6yD4H/vURKSxEKg3DZOBbIPl/S2g=
[12:46] Verificada la firma de la App solicitante
```

Reading and checking QR in age verification application

4. Two different situations can arise:

a. The age verification application responds with the condition "authorized to access", without revealing identity information. The browser removes the filter, and the content is accessed without any type of restriction.



```
01/01/2000-
atBXIlq/bYm5rGKyF2Yp
RltLcd4HeCTiYhnWG4t
k7sU6SLwDBR56CraV0f
SPDZpH
+6vt96Ed2JgOZ2qkrbva
n6gSq1l6eN5R7d9fv79
```

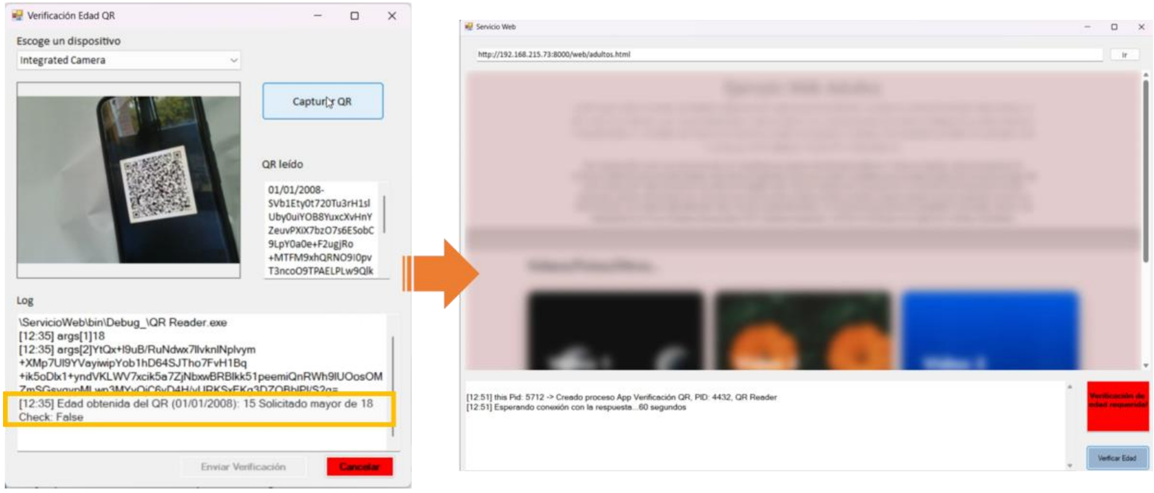
```
\ServicioWeb\bin\Debug_\QR Reader.exe
[15:50] args[1]18
[15:50] args[2]YtQx+I9uB/RuNdwx7llvknlNplvym
+XMp7UI9YVayiwipYob1hD64SJTho7FvH1Bq
+ik5oDlx1+yndVKLWV7xcik5a7ZjNbxwBRBlkk51peemiQnRWh9lUOosOM
ZmSGsvqypMLwn3MYyOjC6yD4H/vURKSxEKg3DZOBblPI/S2g=
[15:50] Verificada la firma de la App solicitante
[15:50] Verificaci[on firma del QR: True
[15:50] Edad obtenida del QR (01/01/2000): 23 Solicitado mayor de 18
Check: True
```

```
http://192.168.1.179:8000/web/
```

```
[15:50] Esperando conexión con la respuesta...60 segundos
[15:51] PIPE: server pid: 8140. Conexión recibida del cliente Pid: 10120
Recibido del cliente:
GgnJbQCMluybMiYUBxfnoMqRkMobyZp5dyoDTe8l8ercnLBP96nMp7OnhMq3B266gnEJbeYX3OLe82m1dNVGoFNln05
iSW9toYQSOK3EtnK3n7Y+IrGMt+skbpq/il4KsRET3VtblUhzsXl5roY+BjOlYRrMQ303HHzgXQy+loM=
[15:51] Conexión cerrada
[15:51] Acreditación recibida válida
```

Successful age verification, the condition "authorized to access" is generated and consequently the content is shown with no limitations

b. The age verification application does not respond with the condition "authorized to access". In fact, it does not respond in any way, so after a while the browser stops waiting for a response and keeps the content filter. This may occur because the person is not of the required age (but the status of minor is not revealed), or because the age verification application has not been installed, or because its use is not authorized, or the QR code is not available, or for any other circumstance.



```
01/01/2008-
SVb1Ety0t720Tu3rH1sl
Uby0uiYOB8YuxcXvHnY
ZeuvPXiX7bzO7s6ESobC
9LpY0a0e+F2ugjRo
+MTFM9xhQRNO9I0pv
T3ncoO9TPAELPLw9Qlk
```

```
\ServicioWeb\bin\Debug_\QR Reader.exe
[12:35] args[1]18
[12:35] args[2]YtQx+I9uB/RuNdwx7llvknlNplvym
+XMp7UI9YVayiwipYob1hD64SJTho7FvH1Bq
+ik5oDlx1+yndVKLWV7xcik5a7ZjNbxwBRBlkk51peemiQnRWh9lUOosOM
ZmSGsvqypMLwn3MYyOjC6yD4H/vURKSxEKg3DZOBblPI/S2g=
[12:35] Edad obtenida del QR (01/01/2008): 15 Solicitado mayor de 18
Check: False
```

```
http://192.168.215.73:8000/web/adultos.html
```

```
[12:51] this Pid: 5712 -> Creado proceso App Verificación QR, PID: 4432, QR Reader
[12:51] Esperando conexión con la respuesta...60 segundos
```

Not successful age verification, the condition "authorized to access" is not produced (the Send Verification button - Enviar verificación- is not enabled, in this example, because the user is not old enough) and consequently the content is still not shown

C. PoC focused on Android smartphones

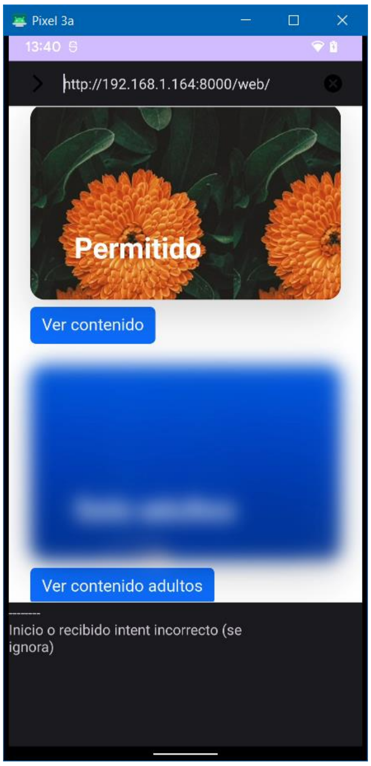
In the second proof of concept, access to content is done with an Android smartphone. The user must install the age verification app developed by the AEPD and a modified browser to work with it on this phone. An example of the PoC execution can be viewed in the following link.

A brief description of this proof of concept follows. Before using the system, the user needs to have a digital wallet (e-wallet) app on their phone; for example, one option will be the wallet provided by the General Secretariat of Digital Administration (SGAD) compatible with the European regulation eIDAS2. This approach is valid with any document or certificate issued by a trusted entity or provider including age information.

The digital wallet will provide an age attribute that may or may not be anonymous, as the verification app will block identity disclosure. The user's age attribute will be stored in the age verification app for a limited period to avoid correlations between requests to the digital wallet and access to adult content.

Next:

1. The user requests access to content labeled “for adults” from the browser.
2. The content is received with its label and the display of the content on the device is preventively blocked (in the PoC the content is shown blurred). In this way, the status of a minor is not revealed to the content provider, the content is always served.

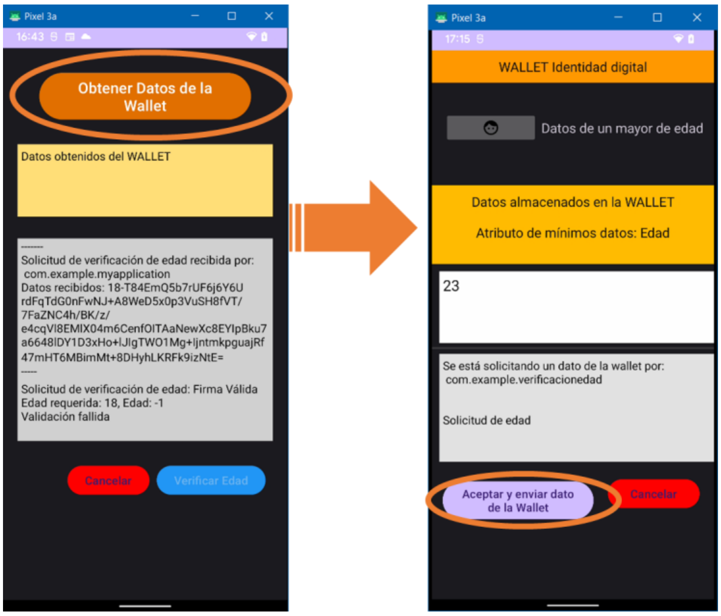


http://192.168.1.164:8000/web/

Inicio o recibido intent incorrecto (se ignora)

Browser that receives labeled content, but does not display it if it requires age verification

3. The browser calls the verification application to determine if the user is of the appropriate age to access the content (over 14, over 18, or other conditions). The age verification application uses the information stored in the digital wallet to carry out the necessary checks.



```
Datos obtenidos del WALLET
```

```
--------
Solicitud de verificación de edad recibida por:
 com.example.myapplication
Datos recibidos: 18-T84EmQ5b7rUF6j6Y6U
rdFqTdG0nFwNJ+A8WeD5x0p3VuSH8fVT/
7FaZNC4h/BK/z/
e4cqVI8EMIX04m6CenfOITAaNewXc8EYIpBku7
a6648lDY1D3xHo+lJIgTWO1Mg+ljntmkpguajRf
47mHT6MBimMt+8DHyhLKRFk9izNtE=
-----
Solicitud de verificación de edad: Firma Válida
Edad requerida: 18, Edad: -1
Validación fallida
```

Datos de un mayor de edad

Datos almacenados en la WALLET

Atributo de mínimos datos: Edad

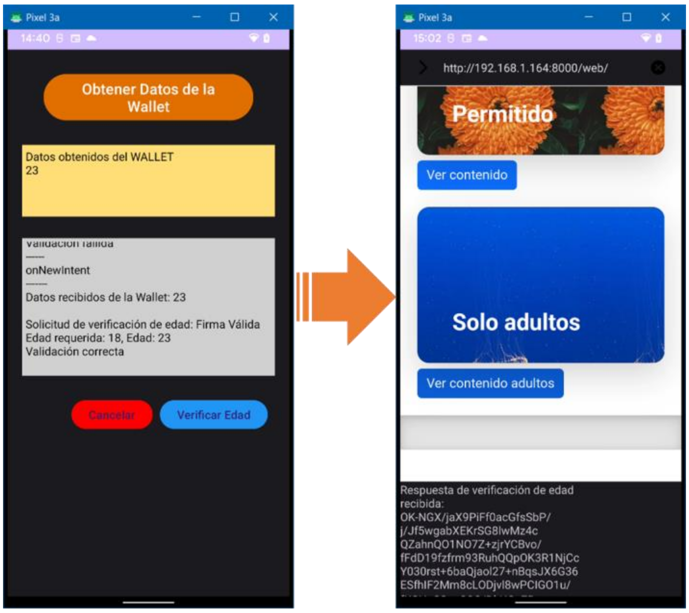
23

Se está solicitando un dato de la wallet por:
com.example.verificacionedad

Solicitud de edad

The age verification app receives the request from the browser and communicates with the digital wallet

4. Two different situations can arise:
    a. The age verification application responds with the condition "authorized to access", without revealing identity information. The browser removes the filter, and the content is accessed without any type of restriction.



```
Datos obtenidos del WALLET
23
```

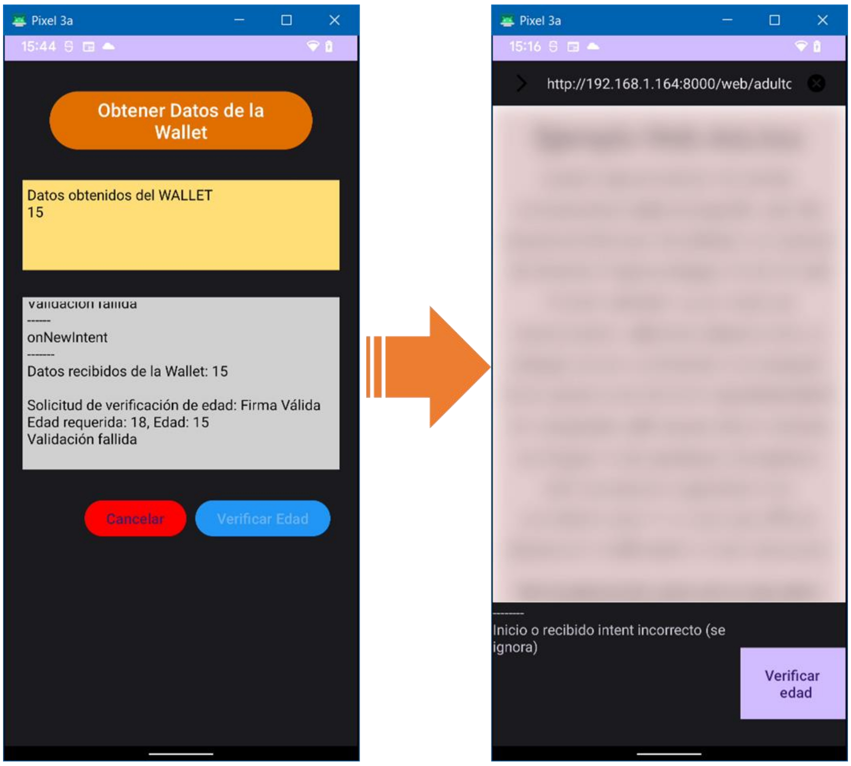
```
Validación fallida
------
onNewIntent
------
Datos recibidos de la Wallet: 23

Solicitud de verificación de edad: Firma Válida
Edad requerida: 18, Edad: 23
Validación correcta
```

http://192.168.1.164:8000/web/

```
Respuesta de verificación de edad
recibida:
OK-NGX/jaX9PiFf0acGfsSbP/
j/Jf5wgabXEKrSG8lwMz4c
QZahnQO1NO7Z+zjrYCBvo/
fFdD19fzfrm93RuhQQpOK3R1NjCc
Y030rst+6baQjaol27+nBqsJX6G36
ESfhIF2Mm8cLODjvl8wPCIGO1u/
```

Successful age verification, the condition "authorized to access" is generated and consequently the content is shown with no limitations

b. The age verification application does not respond with the condition “authorized to access”. In fact, it does not respond in any way, so after a while the browser stops waiting for a response and keeps the content filter. This may occur because the person is not of the required age (but the status of minor is not revealed), or because the age verification application has not been installed, or because its use is not authorized, or a digital wallet app is not installed on the phone or there is not age information available in it, or for any other circumstance.



Datos obtenidos del WALLET
15

validacion fallida
------
onNewIntent

Datos recibidos de la Wallet: 15

Solicitud de verificación de edad: Firma Válida
Edad requerida: 18, Edad: 15
Validación fallida

http://192.168.1.164:8000/web/adultc

Inicio o recibido intent incorrecto (se ignora)

Not successful age verification, the condition “authorized to access” is not produced (the Verify Age button -Verificar Edad- is not enabled, in this example, because the user is not old enough) and consequently the content is still not shown

D. PoC FOCUSED ON iOS SMARTPHONES

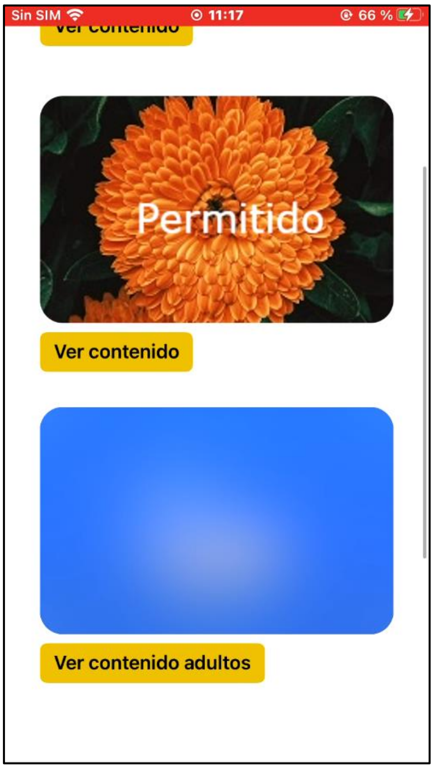
In the third and final PoC, access to content is done again with a smartphone, but in this case, with the iOS operating system installed. An example of the PoC execution can be viewed in the following link.

A brief description of this PoC follows. Before using the system, the user needs to install an app on their phone that can recover data related to their age from physical identity documents (identity card, passport, etc.). It can be done through a document image via OCR or by reading the certificate stored in the chip they include via NFC.

Then, the user is authenticated by digital signature or biometrics (comparing the photo of the document with the one obtained through a selfie) to verify that the document provided for age verification is theirs. In all cases, the processing, including biometrics, is executed on the device without accessing third parties, so it is exclusively personal processing. The age verification app will block the dissemination of the identity obtained from the official document, storing the user's age attribute for a limited period.

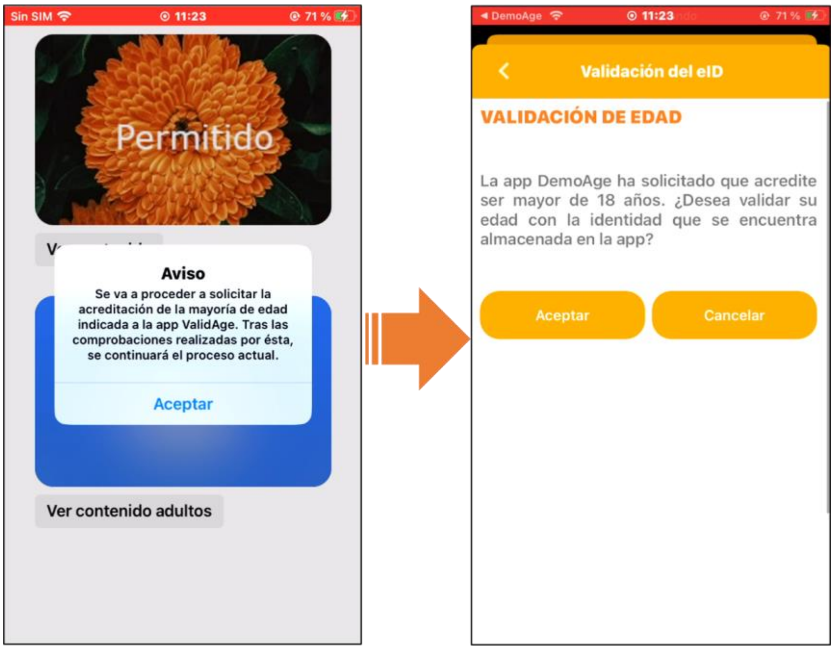
Next:

1. The user requests access to content labeled “for adults” from a specific application (for example, the one used to access content within a social network).
2. The content is received with its label and the display of the content on the device is preventively blocked. In this way, the status of a minor is not revealed to the content provider, the content is always served.



App that receives labeled content, but does not display it if it requires age verification

3. The browser calls the verification application to determine if the user is of the appropriate age to access the content (over 14, over 18, or other conditions). The age verification application uses the information gathered from the physical identity documents to carry out the necessary checks.



Aviso

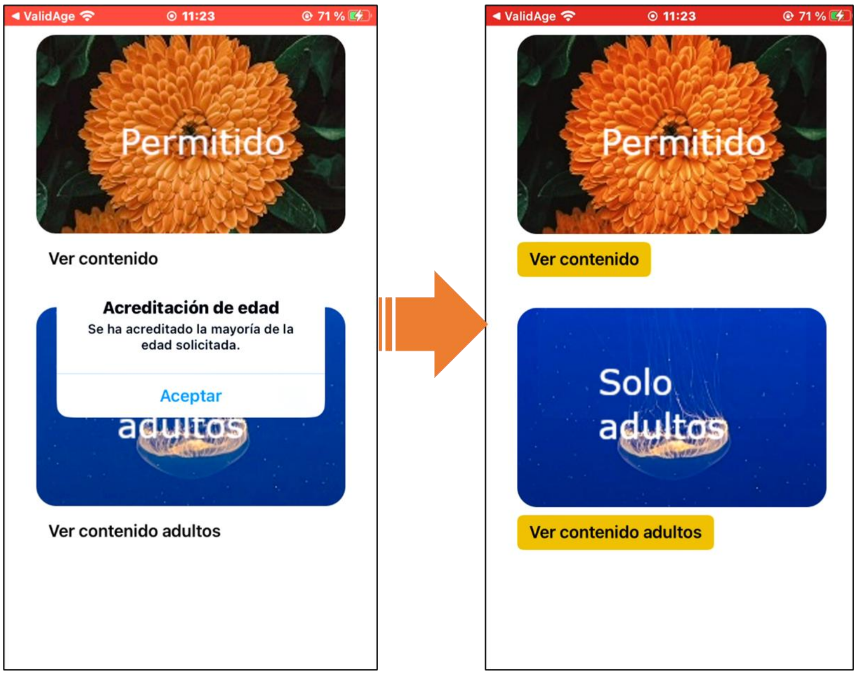
Se va a proceder a solicitar la acreditación de la mayoría de edad indicada a la app ValidAge. Tras las comprobaciones realizadas por ésta, se continuará el proceso actual.

VALIDACIÓN DE EDAD

La app DemoAge ha solicitado que acredite ser mayor de 18 años. ¿Desea validar su edad con la identidad que se encuentra almacenada en la app?

The age verification app receives the request from the content Access app (everything happens with the knowledge of the user, who is aware of the process and must accept the age verification for it to occur)

5. Two different situations can arise:
   a. The age verification application responds with the condition "authorized to access", without revealing identity information. The app removes the filter, and the content is accessed without any type of restriction.

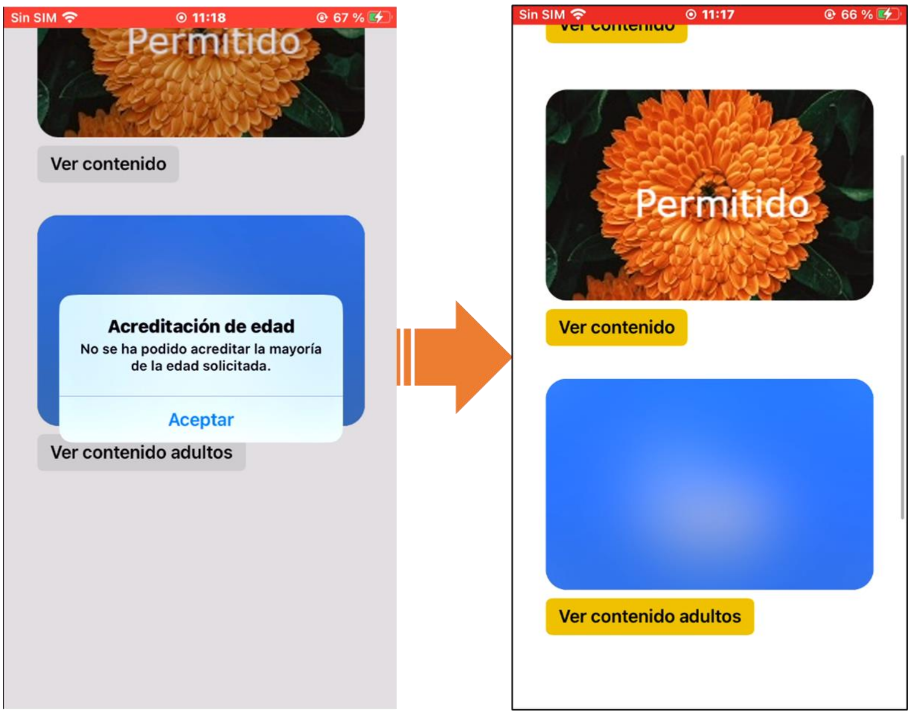


Acreditación de edad

Se ha acreditado la mayoría de edad solicitada.

Successful age verification, the condition "authorized to access" is generated and consequently the content is shown with no limitations

b. The age verification application does not respond with the condition “authorized to access”. In fact, it does not respond in any way, so after a while the browser stops waiting for a response and keeps the content filter. This may occur because the person is not of the required age (but the status of minor is not revealed), or because the age verification application has not been installed, or because its use is not authorized, or there is not age information available in it, or for any other circumstance.



Acreditación de edad

No se ha podido acreditar la mayoría de la edad solicitada.

Not successful age verification, the condition “authorized to access” is not produced and consequently the content is still not shown

III. CONCLUSIONS

Protecting minors from inappropriate content cannot be an excuse to violate fundamental rights. Likewise, fundamental rights, particularly those related to data protection, cannot be used as an excuse for not developing appropriate measures to protect minors. The protection of minors must address the minor's best interests in all its facets.

The urgency of the need for solutions to protect against inappropriate content does not justify the use of data processing that does not comply with the GDPR principles, rights and obligations or the presence of high-risk operations which establish essential limitations in the protection of the best interests of the minor and the rights and freedoms of all Internet users.

The three PoCs developed by the AEPD in collaboration with the General Council of Professional Colleges of Computer Engineering demonstrate how the "Decalogue of principles. Age verification and protection of minors from inappropriate content" can be fulfilled effectively and efficiently.

These PoCs demonstrate that there are options that avoid exposure of minors, regulatory non-compliance or the risks and threats detected in the current solutions available on the market, while being transparent and auditable and not requiring the development of new identity providers different from those already established in Europe. They also show that it is possible to develop solutions for different devices, operating systems and ways to prove that you are old enough to access the content in each case (computers or video game consoles, Android phones , iOS phones) from a necessary technological neutrality.

For a more extensive explanation of some of the doubts that these PoCs may raise, you can consult the following frequently asked questions page.