Frequently Asked Questions (FAQ)

about the Proofs of Concept (PoCs) of systems for age verification and protection of minors from inappropriate content

December 2023

CONTENTS

1. WHY ARE THE DECALOGUE OF PRINCIPLES AND THE ASSOCIATED PROOFS OF CONCEPT PROPOSED?

The use of the Internet services is no longer an option, it has become the only way for the full development of the personal and economic life of citizens in many cases.

Regarding the access to Internet, minors must be protected in many different aspects. The fundamental rights of all Internet users too, regardless of their age. The protection of minors cannot be an excuse to violate fundamental rights. Fundamental rights, particularly data protection, cannot be used as an excuse for not protecting minors.

An age verification system can significantly impact people's privacy, their right to act, think, be informed, and educated freely, and the surveillance and supervision of each of their actions.

The AEPD mission is to protect the fundamental rights of citizens concerning data protection.

The principles establish how to reconcile the minor's best interests and the citizens' fundamental rights, and the PoCs demonstrate that it is possible to put them into practice in real scenarios, illustrating their viability.

2. WHAT IS THE MAIN ADVANTAGE OF THE PROPOSED PoCs?

The main advantages are the comprehensive protection of the minor, the guarantee of the fundamental rights of all users, universality, auditability and absolute transparency, and the suitability of a method that generates trust so that its use can be widespread.

Another advantage is that they are systems that can be exported to the entire world and that, at the same time, they are aligned with the Spanish and European identity providers that guarantee identity as a universal right.

3. SHOULD MINORS DOWNLOAD AND INSTALL ANY APPLICATION OR HAVE IDENTITY PROVIDERS IN THE PROPOSED PoCs?

On the contrary, minors who are subject to the greatest protection (under 14 years of age in Spain) do not need to download or install an application or have identity providers. It is required by users who want to access content labeled “for adults” or “inappropriate for minors” and who have to verify their age to demonstrate that they have the right to access said content.

4. WILL THE AGE VERIFICATION APP BE PROVIDED BY THE AEPD?

The AEPD is a Data Protection Authority, a supervisory authority. Its functions do not include providing this type of solution or application. The applications developed for the PoCs are only prototypes or demonstrators; they are not created to be offered to the public.

The verification app is not a new mechanism to provide identity. Identity is a right of citizenship, which in Spain is guaranteed by the State through the Ministry of the Interior or other entities such as the Fábrica Nacional de Moneda y Timbre (FNMT -Royal Mint and certificates).

Public or private entities must provide the verification app with different models and motivations. The AEPD has among its powers to ensure that all data protection guarantees are met when this happens and, therefore, the rights and freedoms of citizens adequately protected.

At least the FNMT has already committed to developing the age verification app for public use.

5. To perform age verification, are content providers supposed to know the identity of the person accessing content? Or at least know how old they are?

The purpose of protecting minors is to prevent them from accessing inappropriate content. The purpose is not to disclose the age of the people to the Internet content providers, or their identity. Although at first glance, it seems that both situations are equivalent, the second one would imply an intrusive way of achieving the real purpose of the processing.

The Decalogue, demonstrated with the PoCs, establishes that Internet content providers should not, and don't need, to know the identity or age of users. The regulations also do not establish legitimacy to carry out this processing, neither by content providers nor third parties, when it is not necessary for age verification.

6. If a minor or an adult person accesses content served from a server outside Europe, do they disclose their identity or age?

The principles in the Decalogue establish that identity needs to be processed independently of age verification. In the PoCs, the age verification processing is carried out in apps installed on the user's device itself, without accessing external servers; therefore, no information would be revealed to external servers, neither inside nor outside Europe.

7. Does the AEPD propose a new digital identity management system in the PoCs?

No. The AEPD shows in the PoCs that it is possible to make age verification independent from identity providers, so that it is not necessary to create new digital identity systems. It is enough with the identity providers that already exist for the physical or digital world, promoting technological neutrality and free market. Therefore, the solution proposed in the PoCs is compatible with a scheme based on the European digital wallet defined in eIDAS2 or with national or universal identification mechanisms, such as the passport, already available.

8. With the proposed PoCs, should a person declare before a third party their desire to access adult content?

No. The proposed PoCs separate age verification from the declaration of the purpose of accessing adult content (done in the browser or in a specific application for accessing content from a particular provider, such as a social network provider).

A process in which the person must identify themselves to access adult content is not necessary. Nor do they declare to a third party that they have that purpose. In this way, the decision to access adult content is managed exclusively within the user's device, in which their status as a person "authorized to access" is dealt with, and thus trust is created and the system complies with the principle of adequacy, since if it were not widely used, it would be of useless.

9. Does the system proposed in the PoCs allow to link the user's browsing activity between different services?

No, it doesn't allow it. The use of certificates or biometric systems directly on the servers belonging to the content provider or third parties would allow it, revealing information about the user and allowing their profiling.

All systems based on an intermediary third party that, for example, gathers the user's browsing activity and link it with their verified identity, is very intrusive to people's privacy.

But in the PoCs, this linking is impossible because the age verification is executed on the user's device. Furthermore, this verification does not entail the person's identification.

10. ARE SOLUTIONS ADOPTED IN OTHER COUNTRIES THAT WORK AS AN INTERMEDIARY BETWEEN THE USER AND THE SERVICE THEY WANT TO ACCESS NOT VALID?

In some cases, age verification solutions that do not prevent the location of minors and the massive collection of data of all citizens have been adopted. Some of them are very intrusive to privacy and monetize users' browsing data, profile them, identify them and create parallel digital identity systems.

The most popular solutions based on trusted third parties that act as intermediaries between Internet users and the content they wish to access could involve serious risks for the rights and freedoms of all users. In particular, some of them could involve processing minors' data with significant risks for them. The same happens with other solutions, already available on the market, that are based on other designs or architectures but that also involve that type of risk. None of the solutions analyzed by the AEPD up to the moment complies with the proposed Decalogue of principles when it has been shown that it is possible thanks to the PoCs.

The urgency in applying age verification systems cannot be the excuse to expose minors to more significant risks, violate fundamental rights, and build parallel identity management systems that do not preserve privacy and turn identity into a service when it is a right of citizens.

11. WHAT HAPPENS WHEN A MINOR DOES NOT HAVE A MECHANISM TO PROVIDE THEIR IDENTITY?

The standpoint of the principles and the system proposed in the PoCs is that the minor must be free from identification or supervision. Therefore, minors should not be provided with identification mechanisms; they do not need them.

It is the people who are authorized to access the adult content who must use the mechanisms they already have to prove their age.

12. CAN AN ADULT SITE NOT KNOW THE IDENTITY OF THE USER?

An adult site will have the legitimacy to know the user's identity within the framework of a service contract with said person, provided that knowing certain aspects of their identity is essential to establishing the contract, and only when necessary. Also, when required by law.

However, this identification process differs from the age verification process that protects a minor from inappropriate content offered on the site. They constitute two different processing activities that must be independent.

13. COULD NOT PROVIDING THE AGE OF THE USER THROUGH THE USE OF CERTIFICATES, DIGITAL WALLETS, QR CODES OR OTHER METHODS INVOLVE THE EXCLUSION OF CERTAIN USERS FROM USING THE SYSTEM PROPOSED IN THE POCS?

Following the proposed principles, different identity providers must be allowed. Therefore, users can choose which is most appropriate in their case and check that these providers do not detect their access attempts, successful or not, to adult content or do not identify themselves to content providers. Citizens' right to their own identity is considered, offering mechanisms that are accessible to both European citizens and citizens from the rest of the

world. These different identity providers must be offered simultaneously to guarantee trust and non-discrimination. In this way, the right to act on the Internet is not mediated by a limited set of private services but is guaranteed as a right in the digital world.

For this reason, in the PoCs, the identity provision mechanisms have been separated from those for age verification, on Android, iOS and Windows devices, identity providers have been used so that the age of the users can be verified in a certain way relying on different approaches: passport, DNI/TIE, QR codes, or European digital wallet emulators.

14. When could the entire minor protection system be fully operational from inappropriate content?

These systems should already be in operation.

Content and service providers, in collaboration with those involved in the Internet ecosystem and with civil society, have a guide for compliance with the RGPD principle of active responsibility and for the application of data protection by default and by design.

15. Are the mechanisms presented by the AEPD in the PoCs the only ones allowed?

The PoCs demonstrate that there are ways to comply with the principles and that the AEPD can demand compliance with these principles. A solution that complies with the principles will be as valid as any other approach.

Other mechanisms and solutions that respect all the principles included in the Decalogue and that, therefore, guarantee compliance with data protection regulations; protecting the minor's best interests and the rights and freedoms of citizens will be considered appropriate from the point of view of the AEPD.

16. Has it been considered that additional development would be required for the PoCs to become solutions that can be used on the Internet?

The AEPD has been working on the definition of the principles included in the Decalogue, the design and implementation of the PoCs, with a great effort of dialogue with multiple stakeholders, within the framework of an Age Verification Working Group created in March 2023 in which the Comisión Nacional de los Mercados y la Competencia (Competence Authority), the Fábrica Nacional de Moneda y Timbre (Royal Mint, smart cards and electronic certificates), the Ministry of Internal Affairs and the Ministry of Digital Transformation have participated.

The role of the AEPD, which is that of the supervisory authority, is not implementing the final systems. This task is for the industry and the Internet ecosystem, which must assume their responsibility. All the material generated should serve as a guide and orientation and facilitate their work.

17. In the PoCs there are aspects that have yet to be defined or improved. When is the AEPD going to do it?

The AEPD is a Data Protection Authority, that is, a supervisory authority. These PoCs demonstrate that the proposed principles can be met; they will not become final products. That is, the AEPD does not intend to put these solutions into production itself, but rather to promote it to be possible. This will be a task for the industry, public entities and civil society, who will also be able to propose better approaches.

18. EVERY TIME AN ADULT WANTS TO ACCESS CONTENT LABELED FOR ADULTS WILL IT BE NECESSARY TO SCAN A QR CODE, ACCESS A DIGITAL WALLET OR READ AN IDENTITY DOCUMENT? WON'T THESE TYPES OF PROCESSES HINDER NAVIGATION?

The solutions proposed so far on the market, in which users need to authenticate themselves to a service from a third party through the Internet and without guarantees of response times, can be in fact limiting.

The Decalogue does not make low-level proposals with technical design or implementation details, so it can be met with solutions that require the user to register with their identity only once or with solutions that need checking identity attributes or age much more frequently. The providers of age verification applications will probably try to strike a balance between reliability and usability since, in fact, constantly asking for proof would hinder adults browsing content.

19. SHOULD THE AGE VERIFICATION PROCESS BE CARRIED OUT EVERY TIME A SITE OR INTERNET CONTENT LABELED FOR ADULTS IS ACCESSED?

The greatest reliability is obtained if the user's age is verified in each access to content labeled "for adults" or as "inappropriate" for people under a certain age. The greatest usability is obtained by checking only once, when installing the age verification application and configuring it for the user The providers of age verification applications will probably try to strike a balance between reliability and usability, somewhere between these two extreme approaches.

The appropriate balance could consider, for example, the type of device with which content is accessed (mobile phone, computer, console, television, etc.), the time between two attempts to access content or from the last access attempt, reboots, updates or reconfigurations of the device or the age verification application, the criticality of the content or the site, etc.

The Decalogue does not make low-level proposals with technical design or implementation details, so it can be met with solutions that resolve this problem in different ways.

20. IS NOT BIOMETRIC AUTHENTICATION ON THE USER'S DEVICE AN INACCURATE MECHANISM?

Biometric authentication carried out by the users themselves on their own device without sharing any data with external resources or servers is one of the options that a commercial solution should offer to provide the opportunity to verify that the user who gathers age data from an official identity document is the person who owns the said document, comparing the photograph recovered from the document with a selfie obtained in real-time. This use case has been included in one of the PoCs to show that alternative mechanisms that guarantee trust and digital non-discrimination must be allowed simultaneously; it is one of all the possible ones.

Even so, biometric authentication on the mobile device's resources, in a purely personal activity, can have sufficient performance for many situations and users. If not, one of the other possible mechanisms would have to be available.

21. WHY IS AN ESTIMATIVE SYSTEM NOT CONSIDERED APPROPRIATE IN THE DECALOGUE? ISN'T IT LESS INVASIVE TO PRIVACY?

Different reasons make an estimative system not suitable from the point of view of data protection.

Most of those currently on the market have been implemented in a way that fails to comply with most of the Decalogue: they allow minors to be detected, identify users, collect browsing habits, profile users, hinder transparency and auditability, imply biases and unfounded limitations on the right to the capacity to act, allow people belonging to other vulnerable groups different from minors to be detected, etc.

On the other hand, estimative systems executed on the user's device (without sending data to external servers) would be far from complying with the requirement of reliable "verification" of age included as an obligation in current regulation, as they are probabilistic systems.

22. How are users prevented from exploiting the vulnerabilities of the age verification app? Or malicious versions of these age verification apps end up being installed? Could a "fake" age verification application be created that allows a minor to always be verified as an adult?

Of course, as in any system that must be implemented securely, a global governance model must consider that 100% security does not exist, and even less on mobile devices. In particular, the vulnerabilities or weaknesses that must be adequately managed in time.

Whoever provides these apps must maintain them appropriately within the governance framework, with updates that resolve weaknesses or vulnerabilities discovered when they are already in use. Due to their impact, the governance framework of age verification and protection from inappropriate content systems should be incorporated into the incident notification and supervision processes established within the framework of the NIS2 Directive.

As for malicious apps, cryptographic mechanisms can be established to guarantee the legitimacy of age verification apps (or their origin), as is already done in the case of others that require users' trust (banking and payment apps, security tools, chat and messaging, etc.).

23. How is it guaranteed that all data related to age verification or access to content for adults does not end up in the hands of a third party who monitors profiles users? Through the device manufacturer, the operating system, other apps. Smartphones are very unsafe.

It is true that there are weaknesses and vulnerabilities in smartphones that can expose user's privacy. We must continue advancing so that the privacy and security of devices increases significantly.

Otherwise, nothing currently running on the devices will be private or secure. The proposed solution could guarantee the same levels of privacy and security as the apps that users now trust to make payments, banking transactions, communications, access content, etc. At least the same practices and recommendations currently followed for all these apps would be followed.

24. Who will label the content for adults? Can these labels be trusted, who audits them? Is this label model scalable? And how does it adjust to the religion or culture of each country, for example?

The AEPD has prepared a technical note with a proposal for this labeling system based on Age.xml, which arises from the European MIRACLE project. This solution is scalable, can be adjusted to different cultures and religions and is based on self-assessment (the content

providers themselves carry out the labelling), which could be controlled or qualified by various committees and commissions formed by authorities, industry, parent associations, etc.

It is the system already used, for example, in Germany. Other labeling systems could be valid as long as they were compatible with the proposed Decalogue of principles.

25. WOULD THE PROPOSED SYSTEM ALLOW A FAMILY TO IMPLEMENT SPECIFIC PROTECTION MEASURES IN CASE OF A MINOR WHO NEEDS SPECIAL PROTECTION?

The Internet universe has allowed the expansion of new psychological problems in minors, such as obsessive behaviors, eating disorders, etc. Not all the minors are the same, have the same vulnerabilities neither are in the same social and cultural framework.

The system proposed in the PoC, by filtering content on the device, would allow content providers to include configurations in their apps so that the family can incorporate additional protections on specific content, complementing (not necessarily replacing) the parental control tools.

26. IS THE RESPONSIBILITY OF CONTENT PROVIDERS THEN LIMITED TO THE LABELING OF THE CONTENT THEY OFFER?

No, these providers must assume their responsibilities in the complete data processing that protects minors from inappropriate content.

In this processing activity, content labeling is an essential part. However, content providers also must assume their share of responsibility regarding age verification mechanisms or the implementation of access policies. This is a shared responsibility in a complex ecosystem where other operators participate, such as identity providers, content access apps or browsers, age verification solutions, etc. But this complexity is no reason to avoid said responsibility.

The governance model must guarantee the assumption of responsibilities.

27. IN THE SOLUTION PRESENTED IN THE POCS, THE CONTENT PROVIDERS DO NOT HAVE TO PERFORM ANY TASK. DOES THE ENTIRE PROTECTION SYSTEM FALL ON THE USERS AND THE VERIFICATION APP?

The operation of this system establishes demands on the services and content providers. On the one hand, they must label content appropriately or use a standard format to determine that the entire site has age restrictions (online gaming, pornographic content platforms, etc.), with labels that are adequately interpretable by browsers or other content access applications.

On the other hand, when they offer their own applications for accessing content, content providers must implement protection mechanisms and communication with the age verification app. Browsers must also implement protection mechanisms and communication with the age verification app based on the labeling of the content they receive.

The protection mechanisms mentioned must include content filtering on the device.

Furthermore, content providers must implement governance measures to guarantee transparency and auditability and avoid the impersonation of apps, the exploitation of their possible vulnerabilities or access to services with unlabeled content, to name a few examples.

28. How can a content provider assume its responsibility for protecting minors from inappropriate content if they do not receive any information about the person trying to access their content? Should not he receive some attribute related to their age?

The PoCs developed by the AEPD demonstrate that it is possible to assume this responsibility without receiving any data about the user, thus complying with the proposed Decalogue of principles, and avoiding the risks and threats identified in current age verification solutions. It is possible to carry out all the processing without sending data outside the user's device; therefore, the content provider does not need to receive any data about the person accessing content. Likewise, the provider can assume its responsibilities without the need to run any processing on its own servers or develop proprietary solutions.

29. On platforms that require an account to access content and on which there is content for minors and adults, would this solution proposed in the PoCs still valid?

Yes, content suitable for all audiences would be accessed normally, without performing age verification. And only in the case of content that is inappropriate for minors (principle 4) verification processes would be carried out to determine whether a minor should be protected.

30. How is it guaranteed that those who exercise parental authority are who finally decide what the minor can see and what cannot, effectively?

According to the Decalogue of principles that has been developed, through the governance mechanisms of the system (principle 10), the audit of content filtering mechanisms, and active participation in content labeling schemes (principle 8).

31. What happens if an adult downloads adult content and serve them from their own server to distribute them publicly, without labels or limitations? Or if a content provider do not label adult content as such? Could a "parallel" internet be built?

This is where the governance framework and authentication tools for age verification apps and content/browser access apps must be applied (the latter must incorporate protection mechanisms and communication with the age verification app).

Any solution that is presented as perfect is missing the truth and undervalues the human imagination. Governance mechanisms must continuously monitor and react to new vulnerabilities and weaknesses.

On the Internet accessible to all citizens through the usual tools and protocols (sometimes called the "Clearnet"), these "malicious" servers could be searched, which will be easy to detect because they will not use age labels or will have them incorrectly assigned (labeling everything as suitable for all audiences, which could imply constant complaints from users to the committees or commissions that supervise the labeling scheme). These detections would make it possible to create blocklists for parental control tools or DNS servers, penalize these sites in the results of searches carried out with the usual engines (so that they do not appear or appear with very low priority), sanctions could be imposed, etc. In any case, the existence of methods to circumvent protections does not justify failing to establish measures and try to make them as effective as possible.

32. Is it not possible that browsers or content access applications come up that skip content filtering and do not verify the age of the users?

This is where the governance framework and authentication tools for age verification apps and content/browser access apps must be applied (the latter must incorporate protection mechanisms and communication with the age verification app). It must be assumed that technology does not offer a complete guarantee, but rather requires continuous adaptation. For this reason, governance mechanisms must continuously monitor and react to new vulnerabilities and weaknesses.

There are technical solutions that allow content suitable for all audiences to be accessed from any browser or app, but those that are for adults can only be accessed from browsers or apps that perform age verification. Again, the existence of methods to circumvent protections does not justify failing to establish measures and try to make them as effective as possible.

Whoever provides these apps must maintain them appropriately within the governance framework, with updates that resolve weaknesses or vulnerabilities discovered when they are already in use. Due to their impact, the governance framework of age verification and protection from inappropriate content systems should be incorporated into the incident notification and supervision processes established within the framework of the NIS2 Directive.

33. What happens if a VPN is used to access adult content?

The system proposed in the PoCs is more robust against VPNs than others currently used since it is not based on knowing where the content request is made.

Policies are established and run locally, by being executed on the user's device, regardless of the server accessed or where the request originates from.

34. Is it not possible for a minor to access inappropriate content using an adult's device?

The verification, periodically or at each device restart for example, that the person using the device is its owner and has the verified age, avoids this circumstance.

It is always necessary to strike a balance between the reliability of the age verification solution and its usability (you cannot constantly ask for proof as this would hinder browsing content for adults).

The existence of methods to circumvent protections does not justify failing to establish measures and try to make them as effective as possible.

35. Wouldn't it be simpler to block content in the SIM as it is already done in other countries?

It is necessary to be careful because this type of solution could easily detect minors, who would be registered in some way as minors when purchasing the phone, registering the SIM, etc.

Furthermore, reality shows us that many smartphones for minors are acquired without indicating that the use will be for a minor or that phones are inherited from adults.

In any case, any solution should comply with the Decalogue of Principles to guarantee compliance with data protection regulation and the rights and freedoms of citizens. Different solutions could be applied simultaneously for greater guarantee.

36. What is the scope of application of the PoCs, would they be valid in the international context or do they only work in Spain?

They would be valid internationally since they allow the users accessing content to verify their age with different mechanisms (QR code, digital wallet, official identification documents in physical format) relying on different identity providers. It is enough for at least one of these mechanisms to be available in the user's country of origin so that age verification can be carried out in some of the proposed ways. At least, gathering the age data from the passport, where data are stored in a universal application format.

37. Is this an initiative only from Spain?

This model has been proposed at the European level. On a Spanish initiative, there is already a mandate from the plenary session of the European Data Protection Committee for the Key Provisions group to work on age verification criteria and it will be raised in the known as “Berlin Group” of the Global Privacy Assembly.

38. Are the PoCs compatible with the new European digital identity regulation, eIDAS2?

Yes, they are. One of them, which allows access to content through an Android mobile phone, is based on a digital wallet, which could be the one developed by SGAD and FNMT in Spain in the future. Furthermore, the principles included in the Decalogue are perfectly compatible (concerning data minimization, keeping the user control regarding their own data sharing, etc.) with the spirit of the eIDAS2 regulation.

39. Do the PoCs respect the principle of technological neutrality?

Both the PoCs and the principles are independent of device manufacturers, operating systems, identity providers, etc.

The principles are entirely neutral in this sense. Regarding the PoCs, three proofs have been developed to try to show how these principles can be transferred to real scenarios using different types of devices from different manufacturers, with different operating systems, heterogeneous identity providers, etc. Any approach that respects the principles is valid, regardless of the technologies or architectures selected for implementation.