EUDIW. Threats that have not been identified: Collusion attacks between users

Denis Pinkas. President of DP Security Consulting SAS (France)

Outline of the presentation

- What the eIDAS 2.0 REGULATION (EU) 2024/1183 mandates
- Alice and Bob Collusion attacks
- For online accesses, would it be possible to defeat ABC attacks ?
- The use case of digital credential wallets
- Towards a solution able to defeat one use case of ABC attacks
- The consequences for the certification of EUDIWs by ENISA
- The use case of cross-device authorization flows

What the eIDAS 2.0 REGULATION (EU) 2024/1183 states :

Article 5a from REGULATION (EU) 2024/1183 states in its item 16 :

16. The technical framework of the European Digital Identity Wallet shall :

(a) (...)

(b) enable privacy preserving techniques which ensure unlikeability, where the attestation of attributes does not require the identification of the user.

Note the error when using the word "unlikeability", instead of the word "unlinkability".

In which context are collusion attacks relevant ?

Users collusion attacks are relevant when the two following characteristics are simultaneously supported:

- the disclosure of attributes, without revealing the identity of the user, and
- the unlinkability property towards a single verifier (and multiple verifiers).

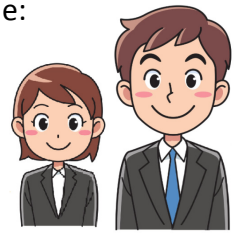
In the context of digital credential wallets, it means :

- that selective disclosure of attributes is supported and
- that one-time-use digital credentials are supported.

Alice and Bob Collusion attacks (ABC attacks)

There are many variations for these attacks, but the goal is the same:

- Alice (12) would like to access to a web site restricted to adults.
- Alice requests the collaboration of Bob (25).
- If Bob accepts, she will get an access to the web site, while the identity of Bob will not be revealed.



Alice (12) Bob (25)

Since Bob will not be identified, Bob can repeat the same trick with other people … either for free or for money on a large scale, e.g., with people all around the world.

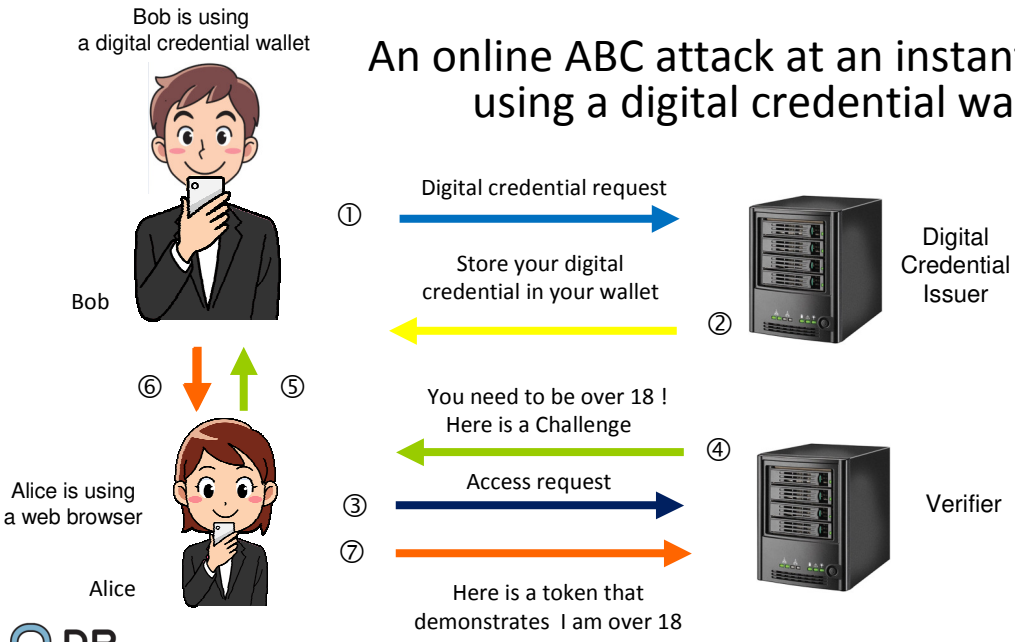
For online access, there are two main variants of ABC attacks

Alice can be recognized to be over 18:

(1) either at an instant of time, e.g., during a session with a verifier,

(2) or during a long period of time, if an “age over 18" attribute is memorized and associated with a user account managed by the verifier.

An online ABC attack at an instant of time using a digital credential wallet



Alice and Bob can be in different locations

Alice and Bob can be in the same location or in different locations, e.g., Alice can be in London, while Bob can be in Manchester.

- Alice and Bob will need to download a specific application (app) *developed by a specialist,* install it and use it.
- At the right moment, Alice's smart phone will make a call to Bob's smart phone and Bob will accept the connection from Alice.

An online ABC attack
when a user account has been created on a verifier

Bob

Pseudonym
and password

Alice

Bob uses his smart-phone and creates a user account on the verifier using a pseudonym and a password.

He then connects to the verifier using this pseudonym and this password.

Afterwards, he uses his digital credential wallet to obtain a token that demonstrates he is over 18. The verifier memorizes the "age over 18" attribute for one year.

Bob logs off and then communicates to Alice the pseudonym and the password so that she can connect to the verifier.

For online accesses, would a cryptographic algorithm or a protocol be able to defeat ABC attacks ?

The response is negative

If two individuals accept to collaborate,
whatever kind of cryptography will be used,
whatever kind of protocol will be used,

a software-only solution

will be unable to prevent the transfer of an attribute of an individual that possesses it, to another individual that does not possess it.

For online accesses, would it be possible to defeat the ABC attack ?

General principle:

The verifier needs to know the characteristics of the hardware device and of the applications used by the individual to perform the access (without being able to uniquely identify the device or the application).

Let us apply this principle to digital credential wallets.

Some vocabulary around for digital credentials

digital credential

set of data structures managed by a digital credential wallet composed of:

(1) one or more public parts that contains attributes about an individual that are signed by a digital credential issuer and

(2) **private cryptographic information** stored into a digital credential wallet that allows an individual to demonstrate to a verifier the ownership of selectively disclosed attributes

digital credential wallet

digital wallet which can obtain, store and manage digital credentials, as well as it can derive *digital credential proofs* from these digital credentials so that they can be presented to a verifier

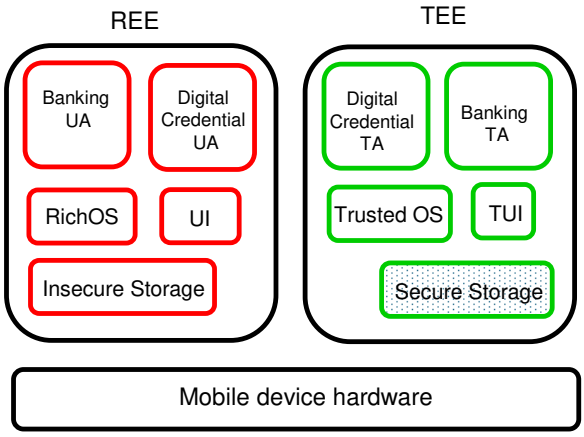
The foundations of an innovative solution using a digital credential wallet (1/4)

A digital credential wallet is composed of a pair of applications :

- an application running in a Rich Execution Environment (REE), under a RichOS, called an untrusted application (UA).

and

- an application running in a Trusted Execution Environment (TEE), under a Trusted OS called a trusted application (TA), with a secure communication with the user via a Trusted User Interface (TUI).



The foundations of an innovative solution using a digital credential wallet (2/4)

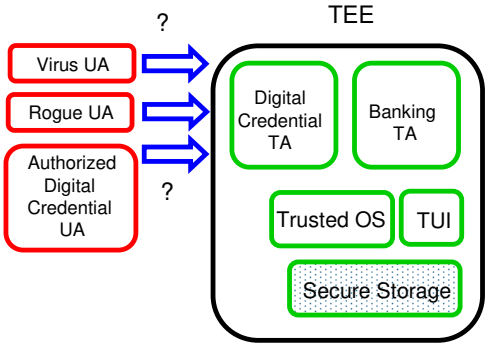
Most smartphones (if not all) support a TEE, e.g., Apple Secure Enclave ® or using Arm's TrustZone technology ®.

The **private cryptographic information** shall be stored into the Secure Storage of the TEE and shall only be used by the right TA.

While necessary, this condition is insufficient.

To call a TA, a UA only needs to know the value of the UUID (Universally Unique Identifier) of the TA.

The **private cryptographic information** shall only be used by the right UA. This means that the TA shall only accept calls from authorized UAs.



The foundations of an innovative solution using a digital credential wallet (3/4)

1) When a TA is first called by a UA, the TA shall verify (with the help of the TEE) that this UA is an *authorized UA*, otherwise, it shall return an error.

2) An "*authorized UA*" shall be a member of a set of authorized applications. The TA shall contain a set of URLs and of self-signed certificates to perform this verification.

3) The TA shall also verify that the calling *authorized UA* is up-to-date.

4) Should the mobile device be rooted or jail-broken, the TEE shall detect it as soon as possible and shall immediately stop this TA.

This approach is only effective during a session with a verifier.

This approach is not sufficient when a user account is created by the verifier.

The foundations of an innovative solution using a digital credential wallet (4/4)

A Secure Element (SE) is defined by the GlobalPlatform Device Technology TEE System Architecture. Version 1.1. January 2017. Document Reference: GPD_SPE_009 as :

> **Secure Element (SE)**
>
> A tamper resistant component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. Can exist in any form factor such as UICC, embedded SE, smartSD, smart microSD, etc.

If the SE is removable, the SE has no way to know that it is called by an authorized and unmodified application. The same applies if the SE is on a remote server.

> Conclusion : Secure Elements (SE), as defined by the the GlobalPlatform, cannot support TAs that are resistant to collaborative attacks.

Which information shall be added into a digital credential ?

The following information shall be added into the *digital credential* so that it can be known by the verifier :

(1) the characteristics of the Rich OS,
(2) the characteristics of the Trusted OS,
(3) the characteristics of the TA, and
(4) optionally, the characteristics of the UA.

It will be up to the verifier, when it receives a digital proof that is derived from one or more digital credentials, to decide whether these characteristics are adequate or not.

Consequences for the EUDIW certification (1/2)

The COMMISSION IMPLEMENTING REGULATION (EU) 2024/2981 of 28 November 2024 (...) as regards the certification of European Digital Identity Wallets states:

- providers of wallet solutions (…) should define and implement processes to evaluate the severity and potential impact of vulnerabilities.
- the security requirements necessary to address the cybersecurity risks and threats listed in the risk register set out in Annex I of this Regulation, up to the required assurance level, and to meet, where applicable, the objectives defined in Article 51 of Regulation (EU) 2019/881.

Unfortunately, Regulation (EU) 2019/881 of 8 September 2015 only sets out minimum technical specifications and procedures for assurance levels for **electronic identification**.

This is the reason why the risk register from Regulation (EU) 2024/2981 does NOT identify user collusion attacks.

Consequences for the EUDIW certification (2/2)

The European Network Information Security Agency (ENISA) has a mandate to define and launch a security certification scheme for EUDI wallets, according to the Implementing Act 2024/29814.

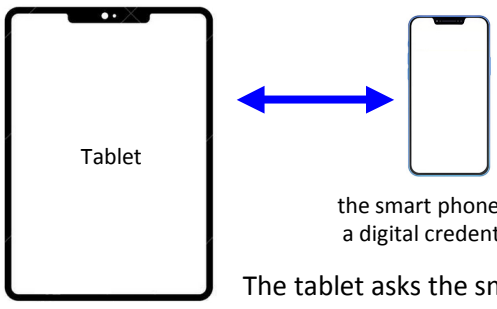
The requirements that will be defined in December 2026 willl only be suited to electronic identification but will not be suited to support the unlinkability property, nor the selective disclosure of attributes.

A digital wallet cannot be an "open-source code". The code of a TA is specific to the Trusted OS. It is not portable and will not be disclosed by smart phone manufacturers.
The code of TAs will not be made public. Only the code of the UAs can be an "open-source code".

It is very unlikely, that in the near term, the security certification schemes for EUDI wallets will able to address user collusion attacks and support the unlinkability property; i.e., the item 16 within Article 5 a from REGULATION (EU) 2024/1183 (see the second slide).

Cross-device authorization flows (1/3)

A user uses a tablet to access a website that wants to know if he is over 18.



The tablet asks the smart phone to generate a *digital credential proof*.

Question: Do the tablet and the smart phone really belong to the same user ?

Cross-device authorization flows (2/3)

The IETF draft draft-ietf-oauth-cross-device-security-15 explores the best current practices: "Cross-Device Flows: Security Best Current Practice".

Section 4.3.10 "Out of Scope" indicates:

> " For other attacks, where the user is willingly colluding with the attacker, the threat model, security implications and potential mitigations are very different".

A first step, as currently recommended in the IETF draft, is to mandate a proximity mode of connection between the two devices, such as Bluetooth Low Energy (BLE), Near Field Communications (NFC) or Ultra Wideband (UWB).

A second step will be needed to make sure that both devices are owned by the same person.

A possible solution would be to use biometric controls, but not those currently supported by the device which are more a "commodity feature" rather than a "security feature".

Cross-device authorization flows (3/3)

Using biometric controls for cross-device authorization flows … is an uncharted territory. At the moment, it seems difficult to fully defeat collusion attacks, but it looks possible to mitigate them.

It is a common practice to use more than one biometric template for face recognition.

When registering a master biometric template, a local age estimation shall be done for that template. If the estimated age of an alternative biometric template is lower than, e.g., 18 months, from the estimated age of the master biometric template, it shall not be possible to register this alternative biometric template. In this way, once Bob has registered his own template, it will not be possible to register Alice's template.

At the time of the registration of a new device eligible to cross-device authorization flows by a smartphone, the user shall perform a successful face recognition against each of the biometric templates registered in both devices.

Comments or Questions ?

"On the Internet, nobody knows you're a dog"
Cartoon from The New Yorker magazine - 1993