GSMA

eIDAS 2.0 and Privacy

Official Response

GSMA Europe

June 2023

GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

GSMA

Table of Contents

GSMA

1. Introduction

Overview

The GSMA, specifically representing the European Mobile Network Operators involved in identity services in this instance, warmly welcomes the publication of the Architecture and Reference Framework (ARF) for the European Digital Identity (EUDI) Wallet. We recognise the efforts undertaken in delivering the Framework and appreciate the planned release of iterative versions involving the stakeholder community. We are encouraged by the adoption of self-sovereign identity principles given the Regulation emphasis on delivering user control and privacy. We have previously outlined our considerations regarding privacy with the European Commission and the wider community. This document details the GSMA Official Response to the ARF in relation to privacy aspects.

Abbreviations

ARF	Architecture and Reference Framework
ANSSI	Agence nationale de la sécurité des systèmes d'information
BBS	Boneh, Boyen, and Shacham (Group Signature)
BSI	British Standards Institution
CL	Camenisch-Lysyanskaya (anonymity-enhanced cryptography signatures)
EC	European Commission
EUDI	European Digital Identity
LoA	Level of Assurance
LD	Linked Data
mDL	Mobile Driver's Licence
SE	Secure Elements
SD-JWT	Selective Disclosure JSON Web Token
SOG-IS	Senior Officials Group Information Systems security
ENISA	The European Union Agency for Cybersecurity
VP	Verifiable Proofs
VC	Verified Credentials
ZKP	Zero Knowledge Proofs

Table 1: Abbreviations

2. On the importance of privacy in eIDAS 2.0

Privacy is one of the fundamental rights defended by the European Union, especially through the European Commission. In addition, it is one of the core targets of the eIDAS 2.0 regulation. The European Parliament, in its latest contributions, is reinforcing this importance, and pushing for an explicit reference to Zero Knowledge Proofs (ZKP) and their mandatory implementation in the upcoming eIDAS 2.0 ecosystem.

Beyond the political willingness to strengthen privacy as a critical component of the European society in future, privacy is clearly a condition of success of eIDAS 2.0 and a matter of credibility for public authorities. Where people have no choice (or consider that they have no choice), experience proves that most prioritise ease of use over privacy. When they do have a choice, especially for their core identity data, they will care about privacy. Civil society will help them: the eIDAS 2.0 solutions will be analysed extensively by expert civil liberties organisations; there is a real risk that eIDAS 2.0 may be flagged as an invasion of privacy and accused of providing inadequate protection if not designed carefully, with privacy in mind. This issue must be dealt with, especially since the use of the EUDI Wallet will not be mandatory, and alternatives must remain available for all use cases. If the digitisation of sovereign documents and highly sensitive processes (health data management, KYC for adult services) do not use all available methods for protecting the privacy of citizens, national privacy authorities may disagree with the deployment of at least some use cases in their respective jurisdiction. Furthermore, if we accept that people are increasingly defiant towards public authorities, a mere “promise” of a legal privacy binding, without any form of technical enforcement may not fully convince users.

If state of the art tools and protocols are used, eIDAS 2.0 will offer a compelling opportunity to dramatically improve privacy in a way that could not be achieved in the physical world today. The privacy issue could therefore be transformed from a potential challenge to a positive differentiator of the EUDI Wallet, driving adoption.

3. What does privacy mean for eIDAS 2.0?

Privacy and minimisation

Privacy is a way to limit shared information to what is strictly functionally necessary for a particular transaction. It relies on the following elements:

1. Identifying what is “strictly necessary” for a particular transaction;
2. Technical means to provide only the information identified as “strictly necessary” for the transaction without jeopardising any other aspects (in particular security and ease of use);
3. Ensuring that no other information is leaked independently from the data knowingly shared by the participants.

In the context of eIDAS 2.0 this translates as follows:

1. Identification of “strictly necessary” information: there is a need for the definition / standardisation of requests and the acceptable attributes to be requested for each purpose (i.e., for each use case). We would welcome and participate to an EC initiative tackling this point.
2. Technical means to provide only the “strictly necessary” information: protocols or technologies need to support the minimisation of shared information, including supporting Yes/No questions. To our knowledge, the only current technology that can achieve this is ZKP (particularly combined with a ZKP-enabled signature scheme of the BBS+ family). Section 4 provides further analysis of this technology;
3. Ensuring no information leak: the underlying protocol infrastructure (and infrastructure in general) must preserve privacy and not leak any information that the service / identity layer does not want to share. This is unfortunately not the case in the current ARF (as of June 16th) due to the correlation that some of the proposed protocols induce between multiple transactions from the same Verified Credentials (VC) holder.

An example of the “minimisation” process alluded to in the second point above would allow a citizen to prove that they are “over 18” (actually proving the answer to a Yes/No question), rather than providing their date of birth, in order to perform an age sensitive transaction.

It is important to note that privacy implementation will not prevent Member States from accessing the content of transactions when legally required e.g. counter-terrorism and criminal investigations.

Unlinkability of transactions

We now expand on the challenge to ensure no information is leaked independently from the data knowingly shared by the participants. This requires the inability for any party to correlate a citizen's unrelated or subsequent actions, assuming that the citizen does not want the correlation to be known or even suspected. This property is the "unlinkability" of transactions. Three main issues may undermine or even prevent unlinkability:

- The use of an explicit and/or implicit (e.g. an issuer signature) identifier in the transactions. We call this issue "**id tracking**" in the remainder of this document. In detail, if the protocol used to generate Verifiable Proofs (VP) carries the signature of the involved VC unaltered into the VP, any further processing of the VC content will not prevent the tracking of user behaviour across the ecosystem.
- The deanonymisation through metadata, e.g. through the technical configuration of a particular wallet. We call this issue "**metadata tracking**" in the remainder of this document.
- The deanonymization through "**behavioural tracking**" (e.g. "phoning home"). For example, if, in order to check the validity / non revocation of a specific VC the verifier needs to interrogate the issuer of this VC, the VC issuer can easily track the activity of the citizen..

The pitfalls of an incomplete privacy implementation

Addressing the challenges we've just described, the implementation of mitigation measures is critical. This implementation requires careful planning and execution. This entails an explicit specification phase of the privacy characteristics of the solution.

In particular, if a solution was presented as ensuring "selective disclosure" or "data minimisation" because it enabled hiding some of the attributes of the VC or deriving some properties of the attributes, but with no guarantee of unlinkability, this could lead to worse outcomes in terms of user trust, than if no data minimisation or selective disclosure was promised.

The following example illustrates how negative outcomes could arise. The example fits well with the use of mDL, one of the protocols mandated by the ARF:

- An adult citizen buys alcohol, browses adult sites online and participates in online gambling platforms - each time using their driving license to validate their age but without revealing their full identity using "selective disclosure"
- This citizen then travels abroad and uses their wallet to display their driving license as identification, therefore providing their complete ID
- Through correlation it becomes possible to build a complete profile of this citizen including their full identity and activities across sites.

As we can see through this example, ID tracking would result in the exact situation that the citizen was expecting to avoid. The citizen's expectation would probably have been that their privacy was protected because of "selective disclosure". Such scenario may damage trust more than if no "selective disclosure" had been offered. If citizens are informed that there is no "selective disclosure", they can make a better-informed decision.

While the above example might look extreme, there is an economic incentive for the advertisement industry to perform the richest and widest possible correlations to create large and data rich identity databases. Once created, these databases can be used for purposes beyond advertisement by many actors including foreign intelligence agencies. Technical prevention forms the only reliable safeguard against such risks.

Consequences for implementations

Full privacy must be the default configuration for transactions. Data fields should only be revealed depending on the specific data requirements of a use case, with these requirements being pre-defined for common use cases. There is no reason for the infrastructure to be set up to leak data that has not been requested legitimately by a service.

In an attempt to mitigate the privacy issues inherent to some of the protocols, some of the standards, including mDL which is mandatory in the ARF, advise multiplying VC instances for the same document for the same wallet, in order to try and regain some diversity when presented to relying parties. We believe these attempts will fall short of the privacy required by eIDAS 2.0 due to structural protocol design issues. Beyond standardisation bodies, we observe some stakeholders searching for workarounds to address structural issues, leading up to very complex solutions which will probably be very difficult to operate. See the following Netherlands document for illustration:

NLW-Design-Consi
derations-v1.0.3-for

We believe that better solutions exist and we describe BBS+ ZKP in the following section. It is important to note that the implementation of these solutions can still allow Member States to access the content of transactions when legally required. There are ways to allow controlled deanonymisation of transactions to cater for this requirement, e.g. by cryptographically mandating that at least three different authorised individuals from relevant public authorities agree.

4. How can BBS+ ZKP solve the privacy challenges of eIDAS 2.0?

Introduction to BBS+ ZKP

The goal of Zero Knowledge Proofs is to eliminate the amount of additional information that needs to be shared as part of a transaction, beyond what is strictly necessary for the transaction.
ZKP can theoretically be used to prove any assertion. Practical limitations are due to the computing power required to prove some types of assertions. However, in the context of eIDAS 2.0, by

choosing the right protocols and the right structure of VC and VP, Secure Elements (SE) should have sufficient processing power to avoid such limitations.

BBS+ is a signature protocol based on Public Key Cryptography. It allows extremely efficient ZKP and possesses many advantageous properties. The process is to sign the attributes with BBS+ and then to perform ZKP on these signatures to demonstrate properties of the underlying attributes.

Features and benefits of BBS+ ZKP

With the right combination of protocols and in particular, using a BBS+ variant for signature, the following features of ZKP can be achieved:

A. **Scalability**: BBS+ is based on elliptic curves and is the most efficient among the ZKP-enabled signature schemes, allowing the computation to be carried on an SE in a matter of hundreds of milliseconds. Furthermore, without downgrading the resulting security or privacy levels, it is possible to perform a significant part of the computation outside of the SE, and to only perform on the SE the sensitive part of the computation involving a secret element. All the features, algorithms and methods mentioned in this paper allow strong scalability and can be executed on an SE, at least for the client part.

B. **No replay**: the ZKP done for generating a VP based on the same VC, the same wallet and the same secret key will appear completely different across two subsequent performances, while proving exactly the same assertion on the same data.

C. **Light on data and management**: A single private key per citizen is the only element that needs to be maintained by the infrastructure in the long term.

D. **“Everlasting privacy”**: BBS+ as a signature scheme is not theoretically immune to quantum computer attacks. If and when quantum computers reach the required scalability, someone could use them to forge falsified Verifiable Credentials proving, for example, that they are an alumnus of KU Leuven university when they are not. However, it will not be possible to deanonymise past anonymous VP generated with BBS+, even for quantum computer attackers or attackers with unlimited computational power, contrary to some “quantum resistant” algorithms. For the identity usages envisioned in eIDAS 2.0, we think this property is sufficient. A fully quantum resistant protocol can be introduced in future.

Note: Other signature schemes are sometimes mentioned e.g. Idemix, CL, etc... To our knowledge, BBS+ is the only signature scheme with all the above advantageous properties while being so efficient to implement, both in terms of key length and required computing power.

Applications of ZKP to eIDAS 2.0 requirements

This section presents how ZKP enabled by signature schemes of the BBS+ family can solve some of the most perilous challenges of privacy for identity:

- **Data minimisation:** ZKP allow minimisation of data. For instance, it is easy to derive a ZKP proof of “over 18” from a date of birth attribute.

- **Unlikability**: The previously mentioned property of avoiding replays (B.) ensures that there is no issuer signature tracking, which tends to be one of the main means of ID tracking.

- **Non revocation:** Accumulators can be used including in “half-offline” situations (when the phone is offline but not the verifier). These are extremely scalable and allow anonymous proofs of non-revocation, as opposed to “phoning home” methods.

- **Decentralised generation of pseudonyms**: By generating a hash of a combination of
    - their private key
    - the identifier of a particular relying party and
    - an element that can be constant to enable tracking or variable e.g. a counter,

  the citizen can easily generate pseudonyms and they can easily prove these pseudonyms to belong to them. Contrary to existing identity federation solutions, pseudonyms are therefore not delivered through a central entity but automatically generated in a decentralized way by citizens.

- **Anonymous presentation of multiple credentials**: It is straightforward to link anonymously multiple VC by creating a ZKP that they were both issued to the same citizen, PID or wallet.

- **Anonymous billing**: It is even possible to do “anonymous billing”, i.e. securely calculating the aggregated use of resources without knowing at any moment which actor did which transaction (e.g. which verifier did how many transactions with which issuer in the last month). Achieving this with ZKP is not straightforward and a follow up document will provide detailed explanations.

BBS+ ZKP Summary

In summary, not only are ZKP able to perform unprecedented rich privacy preserving transactions, they also do so without any scalability, security nor ease of use issues. Given all the advantages of a properly engineered BBS+ ZKP architecture, we think a state-of-the-art privacy preserving identity infrastructure should be built with ZKP and would therefore strongly recommend to include them on a mandatory basis for all eIDAS 2.0 services and transactions. Maturity concerns are sometimes raised for BBS+. However we note that the BBS family of protocols has been defined since 2006 without any major security issue raised since. BBS standardisation is progressing actively thanks to multiple actors in the digital identity community. BBS is increasingly implemented in commercial products, usually in ID Wallets. It is not referenced currently in SOG-IS but discussions should happen in the near future.

5. Impacts on ARF

The proposed philosophy of using BBS+ ZKP for transactions as the basis for ensuring privacy by design is quite a departure from the current ARF. Thereafter we list the main required evolutions.

Privacy: it should be a major ARF topic, especially since there is no adverse impact on other aspects, indeed quite the opposite. This means including all required privacy definitions, following privacy by design principles and finally detailing the resulting necessary protocols.

Protocols: mDL and SD-JWT structurally do not allow unlinkability, due to issuer signature tracking. There is no simple way to remedy this without fundamentally changing the protocols. Therefore, these protocols need to be removed from the ARF. For remote flows, LD-Proofs form an obvious replacement. For proximity flows, alternative must be sought and encouraged by the EU. GSMA can contribute to this effort.

Configurations: configurations seem confusing, and it is not clear why a usual LoA method (requested LoA and then achieved LoA) is not used instead. However, if configurations remain in the ARF, they should all mandate the same target level for privacy: privacy friendly protocols and information disclosure based on higher layers in the stack, according and proportionate to the needs of each use case.

Ideally, the requirements for disclosure should be defined use case by use case in a standard way, at least for the most common requests. Thus, the user would not have to identify themselves what data is legitimate to share or not. This should probably be tackled as part of the Toolbox.

6. Proposed actions and next steps

It is important to act immediately to ensure that the eIDAS 2.0 ecosystem is designed on a sustainable basis and that no lack of robust privacy foundations impair the adoption of the EUDIW across Europe.
The main tasks we propose are as follows:

- Update the ARF as proposed in this document;
- Work with security agencies (in particular ENISA, BSI, ANSSI) to ensure that ZKP related protocols get recognized, and in particular that an alternative protocol such as BBS+ gets included in the SOG-IS list of agreed cryptographic mechanisms as soon as possible;
- Urgently look for a replacement of mDL for the proximity use case;
- Ensure that the necessary privacy evolutions of the ARF translate immediately to the Large-Scale Pilots, in particular to confirm the benefits and maturity of BBS+.

7. Conclusion

eIDAS 2.0 is a unique opportunity to build the identity landscape on strong foundations through a public-private sector cooperative initiative. If eIDAS 2.0 is successful, it will set the pace for at least two decades. The stakes for Europe are major and civil society will scrutinise the initiative when the first wallets are launched commercially.

On one hand, this presents an opportunity for Europe to set the standard for the digital infrastructure of the next 20 years. Alternatively, if privacy is considered as a lesser priority and if the powerful privacy ensuring technologies available today are not included in the core design, there is a strong risk that the adoption of eIDAS 2.0 suffers, together with the credibility of Europe as a leader in defending human rights.

ANNEXES

For further reading we suggest the following references.

BBS+ references

Academic papers

Crypto conference (2004): original BBS paper.
Improved efficiency and multi-attribute management (2016), deemed BBS+: paper and paper.

Standardisation

Current BBS+ RFC draft
Current W3C draft

Performance testing

SIM test performance (2017): paper

ID Wallet implementation

Implemented in the dock.io wallet: e.g. here and here

Accumulator references

For an example of an already implemented accumulator: here
Example implementations: here and here
Benchmark showing the scalability: here

Pseudonyms reference (DAA)

Latest publication: here (benchmark also included in section 5.2)
Standard: here (used among others by Intel SGX and FIDO across millions of devices)

Deanonymization example

Explanation of an example deanonymization process: here

Contacts

Elizabeth Wiltshire
Manager, EU Affairs, GSMA
ewiltshire@gsma.com

Helene Vigue
Identity and Data Director, GSMA
hvigue@gsma.com

Andrzej Ochocki
Chair of the European Identity Group, GSMA
Head of Identity, Deutsche Telekom
Andrzej.Ochocki@telekom.de