Liaison Statement

Liaison Statement Title:	LS on the need for a revised analysis of the privacy aspects in the ETSI TR 119 476 V1.1.1
Security Classification:	Non-confidential

Source Meeting Information		
Meeting Number	Meeting Date	Meeting Location
EIGEUID#34	7 September 2023	Conference Call

Document Details		
Document Number:	Creation Date:	Document Authors:
EIGEUID#34-01	11 September 2023	Hélène Vigué, GSMA
Originating GSMA Source:	Deadline for response:	Liaison Statement Contact
GSMA Europe, European Identity Group	See below	GSMALiaisons@gsma.com

Action Required by Recipient	
External Recipients:	ETSI ESI
Internal Recipients:	GSMA Europe: Policy Group Europe, Digital Economy Expert Group and European Identity Group

1 Summary

GSMA Europe notes that the following technical report has been published by ETSI ESI: https://www.etsi.org/deliver/etsi_tr/119400_119499/119476/01.01.01_60/tr_119476v010101p.pdf

GSMA Europe welcomes the effort to formalize a high-quality analysis of the capabilities of many of the protocols available today to perform ID related transactions in the context of eIDAS2 with an emphasis on privacy aspects. As was expressed in https://www.gsma.com/gsmaeurope/resources/eidas-2-0-and-privacy/ , GSMA Europe thinks that privacy is a critical aspect of eIDAS2 which may be decisive for its successful adoption by civil society. GSMA Europe has therefore worked to identify and publicise the solution enablers that could transform privacy from a challenge to an opportunity for eIDAS2.

2 Comments on the evaluation criteria

GSMA Europe has studied the referenced ETSI document and believes that the solutions have not been compared against all of the best practice privacy criteria. In particular:

- The notion of unlinkability seems to be weaker than the commonly understood one (e.g. here). In particular, it doesn't cover the case where issuers are colluding with verifiers, voluntarily or not, e.g. in case of hack.
- The drawbacks of multi-issuance are not to be underestimated. In particular, any actor that is able to witness the exchanges of the holder would be able to correlate the holder's actions across the ecosystem. Also, it remains to be proven that all EU governments would be happy issuing multiple certificates to the same individual.
- Everlasting privacy ensures that whatever happens in the future (including a secret leak, a breach in the protocol, etc…), the data and the actors of the transaction cannot be retrieved. This is a mathematically provable property. GSMA Europe therefore thinks that Everlasting Privacy is an important property for eIDAS2 to consider and it must be a comparison criterion in the report.
- A missing criterion is the ability to implement in Secure Elements, at least the critical part related to the end-user private key.
- The protocol maturity should consider other factors including commercial implementations and beyond the sole criterion of inclusion in SOG-IS. Inclusion in SOG-IS could be accelerated in light of the privacy requirements of eIDAS2 and does not reflect any intrinsic protocol weakness.

3 Comments on the detailed assessment and conclusions

It is challenging to inform stakeholders accurately on topics as complex as the comparison of advanced ID protocols and complex ZKP methods and ZKP friendly signatures. GSMA Europe thinks that the detailed assessment and conclusions of the report are not accurate when it states that the ARF is today a solid basis for ensuring adequate privacy. Specifically

- The proposed protocols / schemes do not offer a solution for data minimization (e.g. "I am over 18" as opposed to "my date of birth is XX/YY/ZZZZ"). We note that the proposed solution ("a new approach to calculate predicates based on hash chains in conjunction with hashes of salted attributes") lacks maturity, not having yet been peer reviewed. Moreover, it only delivers minimization as range proofs (e.g. no set membership proof).
- The challenge of storing all necessary private keys for protocols like mDL is made even harder by the use of multi-issuance which should impact SE implementability.

- Outside of quantum resistance, BBS+ has all the necessary properties for as ambitious an ID framework as eIDAS2. Among key benefits BBS+ provides full unlinkability, everlasting privacy, scalable and privacy-preserving revocation, and implementability on Secure Elements. It offers much better properties than mDL, SD-JWT or both united, none of which are quantum resistant on their own.

4 Actions

GSMA Europe kindly requests ETSI ESI:

- To review the technical report with regards to the evaluation criteria in section 2
- To review the conclusion, taking into account the comments of GSMA Europe in section 3
- To provide feedback on the outcome of this review and to provide a new revision of the report (if applicable).

GSMA Europe looks forward to continued collaboration with ETSI ESI.

5 GSMA Europe European Identity Group meetings

EIG EUID – Weekly conference calls.

6 Contact

In the case of any questions and/or feedback, these can be directed to GSMALiaisons@gsma.com.