Analysis of Electronic Resident Identity Card proposal

Ondřej Hladůvka

Introduction

This analysis evaluates proposed e-ID system's compliance agains given criteria.

Proposed requirements compliance

The system must manage encryption keys and signing keys securely, including usage of Hardware Security Modules (HSMs) where applicable

Not met. Usage of HSM is not even mentioned outside of section 2.2. thus it si certainly not enforced.

The e-ID data must be encrypted using strong, industry-standard encryption algorithms

Not met. Section 2.3 describes encryption of the e-ID credential by the issuer with:
DES[1] and RC4[2] which are insecure. SHA3 which is a hash family[3], not encryption. RSA-PSS which is signature algorithm[4], not encryption. And ElGamal-OFB which is not a block cipher[5], thus its not standardized in OFB mode

The system should rely on use of digital signatures to verify the authenticity of the e-ID data and to ensure that the data has not been tampered with

Partially met. LUOV/ECDSA signatures are proposed, but the issuer's signature on the e-ID is not explicitly verified by RPs.

The system must ensure that e-ID that was not created by the issuer does not pass verification by the RP

Not met. In Presentation protocol step 8 RPs only check for "meaningful plaintext," not issuer signatures, enabling tampering and unauthorised access.

The system must ensure post-quantum security for all the components

Not met. ECDSA is vulnerable to Shors algorithm, as confirming by NIST PQC standardization [6]. But its still proposed in both issuing and presentation protocols.

The system must use standardised cryptographic algorithms

Not met. LUOV is not standardized and was rulled out by NIST[7]. Voulnabirities was found[8] and proposal does not mention any mitigation. DES[1] and RC4[2] are deprecated.

The system must ensure that attackers getting access to the user's device are not able present honest user's credential to the RP

Not met. System lacks device-level authentication or any other second factor, allowing attackers to present credentials.

The system must ensure strong user authentication before credential is issued

Not met. System proposes just photo verification which is weak and unrealiable[9]. No multi-factor authentication is required.

The system must ensure that adversary cloning the mobile device memory, does not gain access to user' private information

Not met. Private keys arent explicitly stored in HSM, thus they are vulnerable to memory cloning[10].

The system must ensure that adversary cloning the mobile device memory is not able to issue revocation, issuing and presentation requests (without active participation of user)

Not met. Revocation requires no user verification enabling misuse by attackers.

Additional notes

Insecure Communication

Section 2.2 proposes to send all the information over public communication channel without TLS, this is a critical flaw.

Offline Revocation

Users can self-revoke/modify e-IDs without issuer, risking fraud.

Unencrypted Cloud Storage

Lack of encryption at rest for cloud storage of e-IDs risks data breach.

Denial of service

System do not restrict the number of field in the credentials, risking overload by maliciously large input.

Conclusion

Proposal makes several false claims, proposes usage of deprecated (DES, RC4) as well as experimental ciphers (LUOV). Does not enforce HSM usage, multifactor authentication and data at rest encryption. It also fails at choosing standardised ciphers and does not enforce post-quantum cryptography. And is by design vulnarable to denial of service.
I do not recommend system implementation until these issues are resolved as it would not improve security compared to present system.

References

[1] Scott G. Kelly, RFC 4772, 2006. Available: https://datatracker.ietf.org/doc/html/rfc4772

[2] Andrei Popov, RFC 7465, 2015. Available: https://datatracker.ietf.org/doc/html/rfc7465

[3] Kelsey John, Chang Shu-jen, and Perlner Ray, "SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash," National Institute of Standards and Technology (NIST), NIST Special Publication 800-185, 2016. Available: https://doi.org/10.6028/NIST.SP.800-185

[4] Jakob Jonsson and Burt Kaliski, RFC 3447, 2003. Available: https://datatracker.ietf.org/doc/html/rfc3447#section-8.1

[5] Taher Elgamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," 1985. doi: 10.1109/TIT.1985.1057074.

[6] "Module-Lattice-Based Digital Signature Standard (ML-DSA)," National Institute of Standards and Technology (NIST), 2024. Available: https://doi.org/10.6028/NIST.FIPS.204

[7] Alkemade Nicky *et al.*, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process Section 3.24," National Institute of Standards and Technology (NIST), 2020. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

[8] Beullens Ward, "The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes," 2020, *International Association for Cryptologic Research (IACR)*. Available: https://eprint.iacr.org/2020/967

[9] "Authentication Cheat Sheet," Open Web Application Security Project (OWASP), 2023. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[10] Song Wenna *et al.*, "Android Data-Clone Attack via Operating System Customization," *IEEE Access*, pp. 184708–184720, 2020, doi: 10.1109/ACCESS.2020.3035089.