SLIDEDroid: A Secure Lightweight Identity for the Android Platform

Tim Ohlendorf, Wolfgang Studier, and Marian Margraf

Fraunhofer AISEC

31st Crypto Day, 17/18 Oktober 2019

In today's world, digital identities (eIDs) play an increasingly important role, slowly replacing physical identity documents in both public and commercial domains. Having evolved to a daily companion, the smartphone therefore offers an optimal platform for storing and using eIDs. To ensure the trustworthiness of a smartphone-based eID, privacy and security measurements have to be implemented. While there are already various secure and privacy-aware smartphone-based eID reference architectures defined in literature (e.g. see GlobalPlatform (2015) or ISO/IEC CD 18013-5 (2019)), only a few solutions on the market make actual use of them. This is mainly caused by missing or not broadly accessible hardware security measurements in current smartphones. Especially in the mid- and low-range price segment trusted components, like Secure Elements or Trusted Execution Environments are still absent. Additionally, many programmers lack knowledge of secure application development (see Weir, Rashid & Noble (2016)) and therefore do not take available security resources into account.

Hence, an ideal eID solution for the smartphone should work without additional, non-standard or not available security hardware, but should still guarantee a high level of security and privacy for its users. A simple architectural design also reduces the complexity of the eID system and thereby the number of possible implementation errors.

In this work, a new secure lightweight identity solution (SLIDEDroid) which allows to securely distribute, store and use an eID on a smartphone, is presented. It only requires well-established standards and mechanism available on state-of-the-art smartphones which were already evaluated by Ohlendorf, Studier & Margraf (2019). In detail, SLIDEDroid uses a Public-Key infrastructure to authenticate eIDs. By implementing a hashing approach, it enables the eID holders to selectively choose which of their identity attributes they want to share with a service provider. A prototypical implementation for Android and iOS shows that both platforms are already compatible with SLIDEDroid. The results of a performed security evaluation based on the eIDAS regulation (Commission (2015-09-08)) prove, that SLIDEDroid fulfills the eIDAS requirements for assurance level substantial. This means, that SLIDEDroid is ready to be used as an authentication means for public online services in the European Union.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-24

1 Acknowledgment

This work has received funding from the European Union's Connecting Europe Facility TELECOM Call (2017-DE-IA-0022) in the context of the StudIES+ project.

References

European Commission (2015-09-08). COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *OJ* **L 235**, 7–20.

GlobalPlatform (2015). Mobile ID: Realization of Mobile Identity Solutions by GlobalPlatform Technologies. Technical report, GlobalPlatform Inc.

ISO/IEC CD 18013-5 (2019). Information technology – Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence application (mDL). Standard, International Organization for Standardization, Geneva, CH.

Tim Ohlendorf, Wolfgang Studier & Marian Margraf (2019). Digitale Identitäten auf dem Smartphone. *Datenschutz und Datensicherheit-DuD* **43**(1), 17–22.

Charles Weir, Awais Rashid & James Noble (2016). How to improve the security skills of mobile app developers? Comparing and contrasting expert views. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).*