Poster: Towards an Architecture for Private Digital Authentication in the Physical World

René Mayrhofer, Michael Roland, and Tobias Höller
Johannes Kepler University Linz, Institute of Networks and Security
{rm, roland, hoeller}@ins.jku.at

***Abstract*—How can we use digital identity for authentication in the physical world without compromising user privacy? Enabling individuals to – for example – use public transport and other payment/ticketing applications, access computing resources on public terminals, or even cross country borders without carrying any form of physical identity document or trusted mobile device is an important open question. Moving towards such a device-free infrastructure-based authentication could be easily facilitated by centralized databases with full biometric records of all individuals, authenticating and therefore tracking people in all their interactions in both the digital and physical world. However, such centralized tracking does not seen compatible with fundamental human rights to data privacy. We therefore propose a fully decentralized approach to digital user authentication in the physical world, giving each individual better control over their interactions and data traces they leave.**

In project *Digidow*, we assign each individual in the physical world with a personal identity agent (PIA) in the digital world, facilitating their interactions with purely digital or digitally mediated services in both worlds. We have two major issues to overcome. The first is a problem of massive scale, moving from current users of digital identity to the whole global population as the potential target group. The second is even more fundamental: by moving from trusted physical documents or devices and centralized databases to a fully decentralized and infrastructure-based approach, we remove the currently essential elements of trust. In this poster, we present a system architecture to enable trustworthy distributed authentication and a simple, specific scenario to benchmark an initial prototype that is currently under development. We hope to engage with the NDSS community to both present the problem statement and receive early feedback on the current architecture, additional scenarios and stakeholders, as well as international conditions for practical deployment.

I. Motivation

In the last few years, personal mobile devices – in particular the ubiquitous smart phones – have seen increased use for managing digital identities as proxies for their users. Moving beyond the digital into the physical world, user authentication becomes directly entwined with activities and interactions of each individual, often spanning the boundaries between these domains. One motivating example is crossing country borders: currently, we have to handle physical objects (passports) that serve two purposes: to carry digital information (the various aspects of the individual's identity), and to make forging harder by relying on physical tokens that are supposedly more difficult to clone than the information they carry[1]. Such an interaction in the physical world then has direct consequences in the digital: validating information provided by the physical token in centralized databases, storing data traces of those interactions, debiting an account, etc. Many actions in the "real" physical world are therefore already shadowed in the digital one.

In addition to being inconvenient, the current reliance on physical objects poses a security risk of these objects being lost, stolen, or becoming unusable. Biometric authentication of individuals together with cryptographically signed digital identity documents stored in centralized databases has long been envisioned as a way to more seamlessly bridge this gap, supporting users to use even more different services with less direct attention. The obvious disadvantage is that these centralized databases, tracking each interaction of individuals across both worlds, are in direct conflict with the fundamental human right to privacy [2], [11]. Additionally, many such existing databases have already been breached[2].

We therefore aim for trustworthy infrastructure based biometric authentication *without* centralized databases. With biometric sensors distributed in the infrastructure, individuals should no longer be required to carry any physical objects for proving their identity, improving both convenience and security. Our work is orthogonal to other projects like STORK [13] and FutureID [4] or the eIDAS regulation [1]: many current projects focus on the first phase of creating/provisioning digital IDs, while Digidow focuses on the privacy-preserving *use* of such IDs in physical world transactions, including meta data protection against passive global adversaries. Security and privacy requirements are similar to previous work on digital ID on smart phones [3], [5]–[10], [12], but need to be extended particularly w.r.t. hiding meta data in live transactions during use of IDs. In the following, we present one of the first scenarios we will prototype and use to evaluate our system on and our proposal for a distributed network architecture to implement this and other scenarios.

II. Scenario: Physical Access Control

The first scenario is intentionally simple from a conceptual point of view: opening doors (in the future including other kinds of barriers like public transit entrance or even country border control) with minimal explicit interaction and protecting individual's privacy by only transmitting those attributes strictly necessary to determine relevant access. As actors, we initially assume:

- *Individual*: A user of the system with identity attributes (such as name, date of birth, face picture, em-

[1]The same purposes are served by physical cash, other license documents, or physical keys.

[2]Recently, personal data from 500 Mio. Marriott guests has become available to third parties (c.f. https://marriott.gcs-web.com/node/28301/html).

ployed by, student at, citizen of, etc.) from potentially multiple different issuing authorities. In this scenario, the important attribute is *member-of* (an organization or group) to ascertain that the individual should have permission to open this door.

- *Personal Identity Agent (PIA)*: The active software component mediating the individual's interactions by managing their digital credentials.
- *Verifier*: For this scenario, a door lock controller verifying the attributes of a digital identity and – if access should be granted – triggering an actuator to open the respective door.
- *Sensors*: Different trusted sensors available in the infrastructure or carried by the individual to derive proof of their identity and – in this scenario – their location in front of the respective door. Specific examples are location and biometric sensors embedded in smart phones, smart card readers, fingerprint sensors, or cameras. Sensors are assumed to be registered in a public registry or otherwise known to both the verifier and PIA interacting in a particular transaction.

These actors will require at least the following interactions to open a specific door:

1) *Individual* $\rightarrow$ *Sensor*: The user is detected by the sensor (e.g. by stepping in front of the camera or carrying their personal smart phone into the defined area).
2) *Verifier* $\rightarrow$ *Sensor*: This is an optional step for the verifier to send a pre-selected list of potential PIA contact endpoints and/or identifiers to sensors to prime them for faster detection of users. Such preselection is only possible for defined subsets of users.
3) *Sensor* $\leftrightarrow$ *PIA*: PIA queries local and potentially global registries for sensor(s) to interact with for the particular transaction, requests remote attestation for the validity of all candidate sensors, and queries relevant lists for sensor revocations.
4) *PIA* $\rightarrow$ *Verifier*: PIA selects which verifier to interact with (which verifier is responsible for the current door to open), provides a credential as claim of access for the user, and cryptographic proof for the attributes in this claim. The verifier then queries relevant sensor, identity, and attribute revocation lists and, upon successful verification of all proofs, opens the door.

We are working towards a first prototype implementation of this and another scenario in a living lab setting at our institute.

III. Proposed Architecture

On the poster, we will present first details of our proposed solution in the form of an extended block diagram covering both the main architecture with the actors identified above, but detailed with additional actors required in other phases of using the system (e.g. identity issuing authorities, a directory for sensors, or device certification authorities).

This architecture is based on hardware roots of trust for sensors, external issuing authorities for creating signed attribute statements, and cryptographic zero-knowledge proofs for verifying claims made on (a combination of) such attributes while guaranteeing unlinkability under the assumption of collusion between multiple verifiers, global passive eavesdropping on the connection level, and potentially honest-but-curious issuing authorities. A more formal definition of the threat model is subject to future work, and we will explicitly solicit feedback from readers and conversation partners during the poster session concerning additional attack scenarios.

Acknowledgment

This work has been carried out within the scope of Digidow, the Christian Doppler Laboratory for Private Digital Authentication in the Physical World, funded by the Christian Doppler Forschungsgesellschaft, 3 Banken IT GmbH, Kepler Universitätsklinikum GmbH, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH and has partially been supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria.

References

[1] European Commission, "Electronic identification and trust services (eIDAS): regulatory environment and beyond."

[2] European Union, "Charter of the Fundamental Rights," *Official Journal of the European Communities*, no. 364/01, 2000.

[3] R. D. Findling, M. Hölzl, and R. Mayrhofer, "Mobile match-on-card authentication using offline-simplified models with gait and face biometrics," *IEEE Transactions on Mobile Computing*, vol. 17, no. 11, pp. 2578–2590, Nov 2018.

[4] FutureID Consortium, "FutureID project."

[5] D. Hintze, R. D. Findling, M. Muaaz, E. Koch, and R. Mayrhofer, "CORMORANT: Towards continuous risk-aware multi-modal cross-device authentication," in *ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp 2015)*. Osaka, Japan: ACM, Sep 2015, pp. 169–172.

[6] D. Hintze, M. Muaaz, R. D. Findling, S. Scholz, E. Koch, and R. Mayrhofer, "Confidence and Risk Estimation Plugins for Multi-Modal Authentication on Mobile Devices using CORMORANT," in *13th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2015)*. Brussels, Belgium: ACM, Dec 2015, pp. 384–388.

[7] M. Hölzl, R. Mayrhofer, and M. Roland, "Requirements for an Open Ecosystem for Embedded Tamper Resistant Hardware on Mobile Devices," in *11th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2013)*. Vienna, Austria: ACM, 2013, pp. 249–252.

[8] M. Hölzl, M. Roland, and R. Mayrhofer, "Real-World Identification: Towards a Privacy-Aware Mobile eID for Physical and Offline Verification," in *14th International Conference on Advances in Mobile Computing and Multimedia (MoMM 2016)*. Singapore: ACM, Nov 2016, pp. 280–283.

[9] M. Hölzl, M. Roland, and R. Mayrhofer, "Real-world Identification for an Extensible and Privacy-preserving Mobile eID," in *Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017*, ser. IFIP AICT. Ispra, Italy: Springer, Sep 2017, vol. 526/2018, pp. 354–370.

[10] M. Hölzl, M. Roland, O. Mir, and R. Mayrhofer, "Bridging the Gap in Privacy-Preserving Revocation: Practical and Scalable Revocation of Mobile eIDs," in *SAC 2018: Symposium on Applied Computing*. Pau, France: ACM, Apr 2018.

[11] Italian Parliament, "Declaration of Internet Rights," Jul. 2015.

[12] T. Nyman, J.-E. Ekberg, and N. Asokan, "Citizen Electronic Identities using TPM 2.0," Computing Research Repository (CoRR), arXiv:1409.1023, Sep. 2014. [Online]. Available: http://arxiv.org/abs/1409.1023

[13] STORK Consortium, "Stork project."

DIGIDOW
Towards an Architecture for Private Digital Authentication in the Physical World

JOHANNES KEPLER UNIVERSITY LINZ

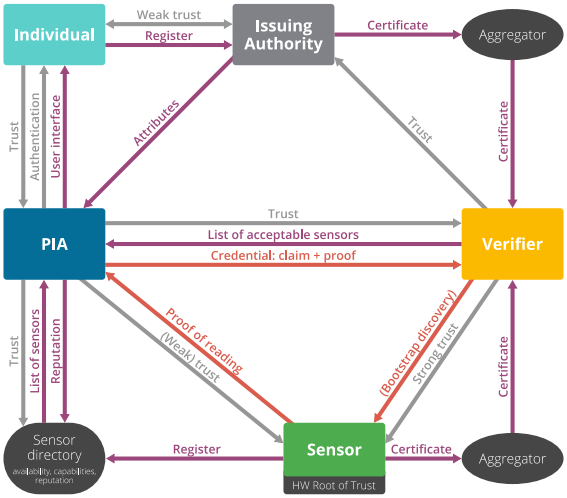
INSTITUTE OF NETWORKS AND SECURITY

Vision

The Digidow projects aims to support using digital identities for authentication in the physical world without compromising user privacy.

It strives to achieve this goal without requiring users to carry any physical identity document or trusted electronic device. Implementing such a token free approach would be relatively easy using centralized databases holding biometric information.

However, we consider the tracking enabled by such databases as a violation of the human right to data privacy. Therefore, we propose a decentralized approach, giving each individual better control over their data.



Sensor

The sensor is responsible for translating a physical world action into a reaction in the digital world.

It achieves that by providing the Personal Identity Agent (PIA) holding the detected biometric template with a proof that the individual represented by the PIA has interacted with a certain sensor at a certain time.

Based on this information verifiers can take actions.

PIA

The PIA acts as the representative of an individual in the digital world.

It employs biometric authentication to confirm that its owner has really interacted with the sensor. It decides if it trusts the verifier involved in the transaction. It uses the data provided and signed by the sensor to create a proof for the verifier that shows its owner actually is the one in front of the sensor and allowed to do what he or she is trying to do.

Verifier

The verifier translates an action in the digital world – the information provided by the PIA – into a reaction in the physical world.

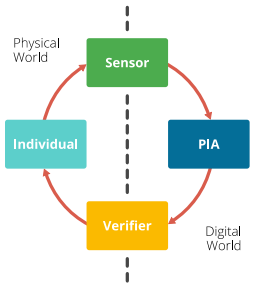
It has to verify the information provided by the PIA and also needs to verify that the provided sensor data originates from a trusted sensor.

Finally, it can trigger an appropriate physical world reaction for the identified individual.

Scenario: Physical Access Control

Assume an individual standing in front of a locked door, with a biometric sensor in front of it, and a verifier connected to the lock. Authorized users could easily gain access via the following steps:

1. User interacts with sensor, which generates biometric template.
2. Sensor searches for PIA responsible for the extracted template.
3. One PIA proves responsibility (and also trusts the verifier).
4. PIA creates and sends cryptographic proof that it is authorized to open door.
5. Verifier verifies the claim made by the PIA.
6. Verifier opens lock and user can enter room.



Authors

René Mayrhofer, Michael Roland, and Tobias Höller
Johannes Kepler University Linz, Institute of Networks and Security

rm@ins.jku.at • roland@ins.jku.at • hoeller@ins.jku.at
https://digidow.eu/ • https://ins.jku.at/