JOHANNES KEPLER
UNIVERSITY LINZ

René Mayrhofer,
Michael Roland,
Tobias Höller,
Martin Schwaighofer
Institute of
Networks and Security

@ rm@ins.jku.at
https://www.digidow.eu/

April 2021

Towards Threat Modeling for Private Digital Authentication in the Physical World

Technical Report

Christian Doppler Laboratory for
Private Digital Authentication in the Physical World

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.

INSTITUTE
OF NETWORKS
AND SECURITY

DIGiDOW

JOHANNES KEPLER
UNIVERSITY LINZ
Altenberger Straße 69
4040 Linz, Austria
jku.at

Contents

Abstract

Various forms of digital identity increasingly act as the basis for interactions in the “real” physical world. While transactions such as unlocking physical doors, verifying an individual’s minimum age, or proving possession of a driving license or vaccination status without carrying any form of physical identity document or trusted mobile device could be easily facilitated through biometric records stored in centralized databases, this approach would also trivially enable mass surveillance, tracking, and censorship/denial of individual identities. Towards a vision of decentralized, mobile, private authentication for physical world transactions, we propose a threat model and requirements for future systems. Although it is yet unclear if all threats listed in this paper can be addressed in a single system design, we propose this first draft of a model to compare and contrast different future approaches and inform both the systematic academic analysis as well as a public opinion discussion on security and privacy requirements for upcoming digital identity systems.

1. Introduction

Digital identity is currently a highly active topic both in research and commercial implementations: frameworks like STORK [29] and FutureID [8], the eIDAS regulation [5], or Blockchain-based concepts like Blockstack [1], ID2020 [16], Evernym [6], or serto (formerly uPort, [26]) have explored or are working on the creation of digital ID; protocol standards like WebAuthn [11], OpenID 2.0 [25], OpenID Connect [23], Verifiable Credentials [28], MLS [22], or projects like SPRESSO [7] define specific ways to use digital ID in various digital services, each with its own threat model; and first international standards like ISO/IEC 18013-5 for mobile driving licenses [17] will be released soon.

We hypothesize that the next step will be transparent, background use of digital ID without explicit user interaction—that in the future, individuals will be supported by infrastructure components in validating those attributes of their identity required for each particular transaction without having to carry any other identifying documents, tokens, or devices. That is, that the current state-of-the-art of personal, trusted, mobile devices will be augmented by increased use of infrastructure devices such as wireless cameras, microphones, or other biometric sensors; a trend that has already started with the proliferation of shared voice assistant devices. General security and privacy requirements for such infrastructure based physical-world authentication are similar to previous work on digital ID on smart phones (e.g., [2, 9, 10, 12, 13, 14, 15, 19, 21, 24] among many others), but need to be extended to better hide meta data created by the verification of IDs when those verifications are performed on the global internet instead of local wireless links. To clarify this particular threat, we explicitly assume global passive adversaries capable of monitoring a significant subset of all internet traffic. On all layers of the networks stack (from MAC through IP up to application layers), unique identifiers therefore need to be avoided, which requires updated threat models and communication designs compared to close-range, local-only communication as assumed in many current standards.

In the following, our main contribution is the first step towards a complete threat model for this hypothesis of future decentralized, shared, global authentication systems. To better ground our threat model, we first define our terminology and a varied set of motivating scenarios we assume will need to be addressed. Note that our proposed threat model is independent of the specific system architecture and implementation, and can be applied to both centralized and decentralized approaches, wired as well as wireless.

1.1 Terminology and Context

We start by introducing stakeholders and clarifying terminology so that we can discuss our threat model in a well-defined context.

Individual: A subject for which digital identities are managed. This is the main group of users.

Identity: We directly re-use the definition from Opencreds [27]: "*An identity is a collection of attributes about an entity that distinguish it from other entities. Entities are anything with distinct existence, such as people, organizations, concepts, or devices. Some entities, such as people, are multifaceted, having multiple identities that they present to the world.*"

Attribute: A data item describing an aspect of an individual's identity, e.g., name, date of birth, template of a face or fingerprint, employee of X, license for Y, etc.

Claim: A statement about the value of an attribute.

Proof: Information enabling the verification of a claim in the context of a particular transaction.

Credential: A set of claims (and their proofs) in the context of a particular transaction.

Sensor: Devices sensing attributes about individuals, e.g., biometric sensors (fingerprint, camera), location (e.g., WiFi/BT devices in range), etc. Sensors are assumed to register in public directories for discovery and transparency.

Verifier: On an abstract level, an entity that verifies attributes about an individual for specific transactions (also called a relying party). In practical settings, we distinguish between: (i) a verifier *endpoint* that is a specific device/instance used in a particular transaction for verification purposes (e.g., a particular payment terminal); (ii) verifier *domains* that operate and rely on one or more endpoints (e.g., the store organization).

Issuing authority: A (third) party trusted by a verifier to define attributes of individuals (root of trust for verification of proofs).

Transaction: An interaction between an individual's digital identity, sensor(s), and a verifier.

The main stakeholders are individuals (whose privacy and data security need to be protected), verifiers (who need proof of identity attributes secured against fraud) assisted by sensors (to map individuals to attributes they present), and issuing authorities (who help individuals to prove certain identity attributes and are at least partially trusted by verifiers). We assume verifiers and sensors to be decentralized and not controlled by or dependent on any single point. Issuing authorities are assumed to be centralized in the sense that they are control points for certain domains of identities (such as citizenship), but that there exist multiple independent authorities per domain. Specific systems architecture may depend on various central components, which influences their resistance to the threats we try to structure in this paper.

Note on centralized vs. decentralized A clear definition of decentralization is difficult, as it depends upon which parts of the (trusted) infrastructure are considered to be part of the system under analysis. Our current draft definition of centralization within the scope of this model is loosely "a single point of control that could be abused for surveillance or censorship". If there are sufficient technical (in contrast to policy) safeguards that make such a point unabusable even if a single party controls it, we would consider this sufficiently censorship-resistant (one of the goals of a decentralized architecture); conversely, a distributed system that could still be easily taken over by a well-resourced adversary (governments and 51% attacks included) would be considered non-resistant and therefore unfit for some scenarios. Depending on the scenario, the notion of *federation* may be more useful or appropriate than a quest for strict decentralization (pending an agreed-upon definition): if individuals are able to easily transfer their digital identity services to another trusted provider, the threat of centralized control can already be mitigated to a certain extent (but not necessarily prevented if a single or small group of providers reach market dominance).

1.2 Example Scenarios

Based on an example described recently in [20], we suggest the following scenarios as thought experiments to span a wide range of use cases for digital authentication in physical-world transactions:

- *Physical access control* (opening doors and gates) is one of the simplest scenarios and often requires only proof of group membership as an attribute of an individual's ID (e.g., being an employee of a company).
- *Proof of age* is often needed e.g., to enter certain locations or for being eligible for purchases or services. This is also one of the outlined scenarios for privacy-preserving identification in the upcoming mobile driving license standard [17], as it requires only the age attribute and proof of association to the individual.
- *Time-based public transport tickets* such as monthly or yearly subscriptions do not require any further identification than possession of a valid ticket. This scenario is particularly challenging from a privacy point of view, as the verifier domain of the public transport organization might be able to associate start and end points of journeys over time if any meta data leakage occurs on any of the layers. Pseudonymization has long been shown not to be effective in such a scenario [18], and therefore true anonymization of every single transaction is required against the threat of linking transactions.
- *Physical ID checks* usually involve presenting a physical identity token to an authority. Typical examples would be driving license verification or crossing a border. In many cases a verifier does not require all the information on an identity token, but only a selected subset, which could easily be wrapped in a transaction-specific credential.
- *Vaccination status* verification is currently a contested political topic. Assuming that vaccination or other medical test results need to be presented for certain activities, proof of safety is the primary attribute, and transmission of other personally identifiable attributes should ideally be avoided.
- *Enrollment at a public university* is the most complex scenario we are currently considering, as it requires a mix of attributes from many issuing authorities (e.g., the last school), but only proof of possession of some att-

ributes (e.g., having passed the university entrance diploma, but without details on grades).

2. Threat Model

For authenticating individuals in a distributed system, many different parties have to interact, often with minimal mutual trust and partially conflicting interests. Therefore, we group the threat model by those parties and list threats to each. Note that some of the threats are based on our hypothesis of future infrastructure based authentication (as opposed to personal, trusted, mobile devices as are currently assumed for the mobile driving license standardization) while others apply more generally to digital authentication and identity systems.

2.1 Threats

2.1.1 Threats Against Individuals

We define threats against individuals as issues that affect an individual in the physical world. We found that all threats against components of digital authentication ultimately lead to a threat against either the individual or the verifier.

I1 *Privacy loss:* Data has proven to be one of the most valuable resources of this century. If private information becomes available to unauthorized parties, they could use it for manipulative marketing, blackmail, etc.

I2 *Identity theft:* Digital identity information has to be linked to individuals. If that link is compromised, attackers acquire the capability to impersonate other individuals.

I3 *Identity loss:* Individuals depend on their digital identities for various purposes. If they lose the ability to prove that a digital identity is linked to them, they lose access to granted rights and paid-for services.

2.1.2 Threats Against Individual's Digital Proxy

Individuals' attributes are digitally represented by proxies (also called "holder" devices) in various forms, e.g., on their mobile device or on a hosted cloud instance. Those representations are also subject to specific threats:

P1 *Attribute disclosure:* The main function of the digital representation is to provide attributes to other actors. If any actors can receive attributes they are not authorized to know, the individual faces threat *I1*. Since an individual should remain in control over their personal data, the disclosure of attributes to an *authorized* individual is explicitly not considered a threat.
Note: Disclosure or modification of any data based on coercion and other pressures is not a threat against the digital proxy itself (because the commands would be issued by a correctly authenticated individual), but a direct threat to *I1* and *I2*.

P2 *Denial of service:* Any disruption of either the operation or the network necessary to reach the digital representation leads to *I3*.

P3 *Data modification:* Individuals and their identities change over time and so must their digital representation. Malicious use of that capability could cause storage of wrong attributes or modification of existing ones leading to *I2* or *I3*.

2.1.3 Threats Against Operators of Verifiers (Verifier Domains)

Entities that rely on verifiers to trigger actions in the physical world also face threats:

O1 *Fake identities:* If a verifier can be tricked into accepting a forged credential, operators can no longer rely on the identification made by their verifiers. This would give all users a possibility to deny their actions.

O2 *Denial of service:* If organizations rely on verifiers for their business model, any circumstances that render their systems unavailable causes immediate financial loss.

2.1.4 Threats Against Verifier Endpoints

V1 *Denial of service:* Any circumstances that make it impossible for individuals to successfully interact with a verifier impacts both the operator (*O2*) and the individual (*I3*).

V2 *Forging/modifying attributes:* Due to incomplete or otherwise insecure verification of issued attributes, it might be possible to trick a verifier into accepting attributes that have not been issued by a trustworthy issuing authority leading to *O1*.

V3 *Combining cross-identity attributes:* Multiple individuals could combine attributes to trick a verifier into assuming all those attributes belong to a single individual (*O1*).

V4 *Internal compromise:* Attackers could gain access to information used by the verifier to identify itself (such as private signing keys), allowing them to operate a rogue verifier (*Adv3*).

2.1.5 Threats Against Issuing Authorities

A1 *Spoofing of identities:* If an issuing authority wrongly identifies an individual, a valid link between one person's digital identity and another person's real world interactions can be created, leading to *I2* or *O1*.

A2 *Modification of attributes:* An issuing authority could be tricked into updating an individual's attributes incorrectly, for example by leveraging methods of social engineering, leading to either *I2*, *I3*, or *O1*.

A3 *Re-use of outdated/revoked attributes:* If an attacker got hold of such attributes, they could still try to use them in order to be identified as another individual by an issuing authority, leading to *I2* or *O1*.

A4 *Leakage of attributes:* Issuing authorities have to store and process private attributes of individuals. Consequently, there is a possibility that an issuing authority is tricked into revealing these attributes to attackers, leading to *I1*.

A5 *Internal compromise:* Malicious actors can gain control over the issuing authority infrastructure resulting in a rogue issuing authority (*Adv4*).

2.1.6 Threats Against Sensors

S1 *Spoofing/manipulation of sensor input:* Attackers could attempt to fool the sensor into reading wrong biometric data – for example by creating a fingerprint dummy or a face mask – leading to *I2* or *O1*.

S2 *Spoofing/manipulation of sensor output:* A man-in-the-middle attack could intercept, modify, or replay information transmitted by the sensor, leading to *I2*, *I3*, *O1*, or *O2*.

S3 *Denial of service:* If a sensor is unable to communicate with the rest of the infrastructure, individuals cannot use them to authenticate to verifiers (*I3* and *O2*).

S4 *Internal compromise:* Physical (or otherwise remote) access to sensors could be abused to take full control over a sensor without other transaction participants noticing. This effectively turns the sensor into a rogue sensor (*Adv1*).

2.1.7 Threats Against Sensor Directories

We assume that sensors are registered in a public directory. We expect this to be public, because in our vision, privacy should be reserved for individuals, while infrastructure is designed to be as transparent as possible to generate trust.

D1 *Flooding:* If the public sensor directory is filled with fraudulent entries, it can no longer serve it's function of supporting discovery effectively causing *I3* and *O2*.

D2 *Denial of service:* The sensor directory could be prevented from answering requests, for example by disrupting network traffic, leading to *I3* and *O2*.

D3 *Loss of control:* If a malicious actor can fool users into distrusting valid sensors (see *S3*, and in turn, *I3* and *O2*), or can gain control over the sensor directory, the directory becomes a rogue sensor directory (*Adv2*).

2.2 Threat Actors

Here we define adversaries that are responsible for the identified threats.

Adv1 *Rogue sensors* can send incorrect biometric measurements or (see *I2*, *O1*) steal biometric information. Either by logging measured biometrics or by tricking PIAs into revealing information about their internal biometric data (*I1*).

Adv2 *Rogue sensor directories* can aggregate data about which sensors are used by whom (*I1*) and can control which sensors are trusted, potentially causing *I2*, *I3*, *O1*, or *O2*.

Adv3 *Rogue verifiers* can try to request attributes without actually needing them (*I1*) or can deny access to authorized individuals (*I3*).

Adv4 *Rogue issuing authorities* can issue new or modified attributes for an individual (including coercion e.g., by legal or governmental action), which can lead to *I2* or *I3*.

Adv5 *Active local adversaries* have direct physical access to the digital infrastructure involved in a transaction. Some of the threats they pose must be tolerated (for example the fact that they can deny service by disabling or damaging the infrastructure).

Adv6 *Active remote adversaries* have only remote access to the authentication infrastructure. They try to exploit both the protocols and their implementations used by sensors, verifiers, digital representations, etc.

Adv7 *Active network adversaries* have full access to one or several network links used during transactions. They try to capture, replay, insert, or drop parts of a transaction.

Adv8 *Passive global adversaries* are assumed to have access to all Internet communication but not the internal state of other parties. They can use any identifiers in network communication to link interactions leading to *I1*.

2.3 Preliminary Evaluation

Many of these threats are not new in themselves, and many have already been solved for particular contexts. E.g.:

- Cryptographic techniques such as attribute based credentials (ABCs) [4] can provide selective disclosure of attributes together with unlinkability of signers (and thus anonymity for individuals as attribute holders) — if applied correctly (and in a usable way, which is still a largely unsolved side issue), this can (at least partially) address *I1*, *P1*, *O1*, and *V2*.
- The digital proxy being transparent about its actions on behalf of the individual can be used for obtaining informed user consent to continued participation and enable informed public discourse.
- The possibility for users to delete specific data their digital proxy stores mitigates threats of coercion and other pressures to disclose data about interactions that is stored for transparency. This protects *I1* at some cost to transparency.
- Local biometric authentication, e.g., fingerprint sensors in smartphones or human personnel at the verifier end as assumed in the upcoming mobile driving license standard [17], addresses binding identity attributes to individuals (*I2*, *O1*, *A1*, and *S1*). However, once those sensors become integrated into the environment and are no longer fully trusted by either the individual or the verifier, existing methods fall short of practical solutions.
- Network privacy technologies such as Tor onion routing can address confidentiality threats posed by passive (or active) global adversaries (*Adv8*) at the cost of increased latency and decreased availability and scalability.
- Hardware root of trust approaches such as secure/measured boot schemes with remote attestation (e.g., based on DAA [3]) – if and only if coupled with transparency on running software stacks – are a step towards addressing insider threats against distributed devices such as sensors (*S4*), but do not currently help against internal attacks at semi-trusted organizational entities like issuers (*Adv4*) leading to data abuse (*A4* and *A5*).

Unfortunately, supporting a combination of attributes from different issuers without the risk of forging the mix (*V3*) seems practically unsolved, similarly to the practical necessity of updating attribute values due to changed individual circumstances and corresponding threats *P3*, *A2*, *A3*.

We are also unaware of practical mitigations against the different denial-of-service threats *I3*, *P2*, *O2*, *S3*, *D1*, *D2* and many approaches seem to be less suited for scaling to a global population of individuals and to an open-ended set of issuing authorities and verifiers from a performance point of view, explicitly including network communication latency for interactive protocols.

3. Position on Future Work

Tackling all these threats in a single, distributed systems architecture is hard. Ideally, we would be able to construct a zero-trust cryptographic protocol to prove that a sensor has taken a reading that matches a (e.g., biometric) template stored at the individual's digital proxy to a third party (the verifier) without any of those parties learning more than they need:

- the sensor should not learn more than the current reading, i.e., not which identity it is matching, and not where this statement of a match is used (at which service it is presented);
- the verifier should learn neither about the biometric template nor the current sensor reading, but should receive unforgeable proof that the individual wishing to consume a service possesses the required identity attributes (without necessarily learning the exact value of the attribute itself); and
- the individual's digital proxy (where the template is stored) will learn where the identity is used (and knows all their digital identity attributes, of course) but should not learn anything about raw sensor readings referring to *other* individuals.

We argue that, considering all the threats discussed above, the minimally disclosing, secure statement provided by an individual (but effectively issued from an individual's digital proxy) to a verifier should be something like:

> "I have a valid credential signed by an authority you trust, and this particular statement about the credential[1] holds **and** I have a statement signed by a sensor you trust that it verified that I am currently there, matching another attribute of that same credential[2]."

That is, one ZKP (zero-knowledge proof) on the credential (without necessarily revealing any unique ID) and another ZKP on being recently authenticated by the sensor (again without a unique ID) uniquely linked together, but only within the scope of the current transaction and not generating linkable meta data that could be correlated in past or future transactions (even between the same pair of individual and verifier and under the assumption of collusion between issuing authorities and verifiers). Unfortunately, we are unaware of a protocol construction with these properties that does not imply hardware root of trust assumptions at this time, and propose that the search for such a protocol would be worthwhile for future digital identity systems.

4. Conclusions

We proposed a first threat model specifically for the upcoming, increased use of digital identity for physical-world transactions. We envisage a decentralized, distributed biometric authentication system to support individuals in their daily interactions without carrying physical identification documents or devices. While no such system exists globally at the time of this writing, we urge future systems designs to address as many of these threats as possible.

We specifically note that various threats are in conflict with each other based on different parties' interests (e.g., security against spoofing biometric authentication through multi-factor authentication vs. unlinkability of transactions),

[1] E.g., "I am over 18" or "I have a valid travel pass for this month".

[2] E.g., face detection passed with a certain threshold.

and completely mitigating all of them at once may not be possible in a single construction; systems designers will have to balance these conflicting interests or decide to accept some threats—possibly only for some scenarios—in favor of mitigating others. Our proposed threat model can potentially be used to declare how future systems choose those balances.

References

[1] Muneeb Ali. 2015. Introducing the Blockstack Identity System. Blockstack, (May 2015). https://blog.blockstack.org/introducing-the-blockstack-identity-system/.

[2] Siddhartha Arora. 2008. National e-ID card schemes: A European overview. *Information Security Technical Report*, 13, 2, 46–53. ISSN: 1363-4127. DOI: https://doi.org/10.1016/j.istr.2008.08.002.

[3] Ernie Brickell, Jan Camenisch, and Liqun Chen. 2004. Direct Anonymous Attestation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security* (*CCS '04*). ACM, New York, NY, USA, 132–145. DOI: 10.1145/1030083.1030103.

[4] Jan Camenisch and Thomas Groß. 2008. Efficient Attributes for Anonymous Credentials. In *Proceedings of the 15th ACM Conference on Computer and Communications Security* (*CCS '08*). ACM, Alexandria, VA, USA, 345–356. DOI: 10.1145/1455770.1455814.

[5] European Union. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (2014). http://data.europa.eu/eli/reg/2014/910/oj.

[6] Evernym Inc. 2020. Evernym – The Self-Sovereign Identity Company. (2020). https://www.evernym.com/.

[7] Daniel Fett, Ralf Küsters, and Guido Schmitz. 2015. SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (*CCS '15*). ACM, Denver, CO, USA, 1358–1369. DOI: 10.1145/2810103.2813726.

[8] FutureID Consortium. 2012. FutureID. (2012). https://cordis.europa.eu/project/id/318424.

[9] Daniel Hintze, Rainhard D. Findling, Muhammad Muaaz, Eckhard Koch, and René Mayrhofer. 2015. CORMORANT: Towards Continuous Risk-aware Multi-modal Cross-device Authentication. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers* (*UbiComp '15*). ACM, Osaka, Japan, 169–172. DOI: 10.1145/2800835.2800906.

[10] Daniel Hintze, Muhammad Muaaz, Rainhard Dieter Findling, Sebastian Scholz, Eckhard Koch, and René Mayrhofer. 2015. 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 '15*). ACM, Brussels, Belgium, (December 2015), 384–388. DOI: 10.1145/2837126.2843845.

[11] Jeff Hodges, J. C. Jones, Michael B. Jones, Akshay Kumar, Emil Lundberg, Dirk Balfanz, Vijay Bharadwaj, Arnar Birgisson, Alexei Czeskis, Hubert Le Van Gong, Angelo Liao, and Rolf Lindemann. 2021. Web Authentication: An API for accessing Public Key Credentials Level 2. (February 2021). https://www.w3.org/TR/webauthn-2/.

[12] Michael Hölzl, René Mayrhofer, and Michael Roland. 2013. 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 '13*). ACM, Vienna, Austria, 249–252. DOI: 10.1145/2536853.2536947.

[13] Michael Hölzl, Michael Roland, and René Mayrhofer. 2017. Real-world Identification for an Extensible and Privacy-preserving Mobile eID. In *Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017*. IFIP AICT. Volume 526/2018. Springer, Ispra, Italy, (September 2017), 354–370. DOI: 10.1007/978-3-319-92925-5_24.

[14] Michael Hölzl, Michael Roland, and René Mayrhofer. 2016. 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 '16*). ACM, Singapore, (November 2016), 280–283. DOI: 10.1145/3007120.3007158.

[15] Michael Hölzl, Michael Roland, Omid Mir, and René Mayrhofer. 2018. Bridging the Gap in Privacy-Preserving Revocation: Practical and Scalable Revocation of Mobile eIDs. In *Proceedings of the ACM SAC Conference*. ACM, Pau, France, (April 2018), 1601–1609. DOI: 10.1145/3167132.3167303.

[16] Identity2020 Systems, Inc. 2020. ID2020 Digital Identity Alliance. (2020). https://id2020.org/.

[17] ISO/IEC DIS 18013-5. 2021. Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application. Draft International Standard. (February 2021).

[18] John Krumm. 2007. Inference Attacks on Location Tracks. In *Pervasive Computing. Pervasive 2007*. LNCS. Volume 4480. Springer, Berlin, Heidelberg, 127–143. DOI: 10.1007/978-3-540-72037-9_8.

[19] Marian Margraf. 2011. The New German ID Card. In *ISSE 2010 Securing Electronic Business Processes*. Vieweg+Teubner, 367–373. DOI: 10.1007/978-3-8348-9788-6_35.

[20] René Mayrhofer, Michael Roland, and Tobias Höller. 2020. Poster: Towards an Architecture for Private Digital Authentication in the Physical World. In *Network and Distributed System Security Symposium (NDSS Symposium 2020), Posters*. (February 2020). https://www.mroland.at/uploads/2020/02/Mayrhofer_2020_NDSS2020posters_Digidow.pdf.

[21] Thomas Nyman, Jan-Erik Ekberg, and N. Asokan. 2014. Citizen Electronic Identities using TPM 2.0, (September 2014). arXiv: 1409.1023 [cs.CR].

[22] E. Omara, B. Beurdouche, E. Rescorla, S. Inguva, A. Kwon, and A. Duric. 2020. The Messaging Layer Security (MLS) Architecture. Internet-Draft, Network Working Group, IETF. (2020). https://tools.ietf.org/html/draft-ietf-mls-architecture-04.

[23] OpenID AB/Connect Working Group. 2014. OpenID Connect 1.0. (2014). https://openid.net/connect/.

[24] Florian Otterbein, Tim Ohlendorf, and Marian Margraf. 2017. The German eID as an Authentication Token on Android Devices. arXiv: 1701.04013 [cs.CR].

[25] David Recordon and Drummond Reed. 2006. OpenID 2.0: A Platform for User-Centric Identity Management. In *Proceedings of the second ACM Workshop on Digital Identity Management* (*DIM '06*). ACM, Alexandria, Virginia, USA, 11–15. DOI: 10.1145/1179529.1179532.

[26] Serto. 2021. serto – Data meets identity. (2021). https://www.serto.id/.

[27] Manu Sporny and Dave Longley. 2019. Identity Credentials 1.0. Draft Community Group Report, W3C. (2019). https://opencreds.org/specs/source/identity-credentials/.

[28] Manu Sporny, Grant Noble, Dave Longley, Daniel C. Burnett, and Brent Zundel. 2019. Verifiable Credentials Data Model 1.0. W3C Recommendation. (November 2019). https://www.w3.org/TR/vc-data-model/.

[29] STORK Consortium. 2008. Secure Identity Across Borders Linked (STORK). (2008). https://www.eid-stork.eu/.