OneID

Trusted. Sovereign. Irrefutable.

Trusted Identity in Trustless Environments

(A Concept Paper)*

Akhilesh Damaraju† Anupam Gupta‡ Sri Yilapavanam§

January 2018

Abstract

We present a modern way to think of individual digital identities using proven techniques and recent advances in Information Security and Consensus Protocols in Distributed Systems. We show how *OneID*–the presented approach to identity, identity management, authentication and verification–solves the problems with the contemporary approaches, and is the way to go forward. We also look at how *OneID*'s decentralization approach opens up doors to more business opportunities and present some business use cases that we are developing.

Contents

*OneID, this whitepaper and additional technical papers are work in progress. This is version 0.5 of the concept whitepaper. For feedback, error reporting or possible collaborations on the project or research, please contact the second author.

†akhilesh@tsaasg.com
‡anupam@tsaasg.com
§sri@tsaasg.com

1 Introduction

Currently, there is no universally accepted digital equivalent of an individual's off-line identity such as a passport/driving license/social security number. The current model of digital identity is focused on service access, rather than true representation of an individual. The Internet misses an adequate identity layer. In the past, this has created considerable operational, opportunity and usability costs for the Internet economy, both for the corporations and and users.

Existing digital identity systems, as we know them, are centralized. Governments have built identity systems by making residents' identities on these systems a mandatory legal or statutory requirement. Business organizations like Google, Facebook or Microsoft have built them as an extension of the required identities for availing their services. However, as we shall see, such identity systems pose problems for users and businesses that require individual identities as a prerequisite to providing services, are prone to attacks through side channels and sometimes perimeter attacks leading to compromising large scales of identity data. In some cases, systems are compromised by insider attacks.

From a business view-point, centralized systems, wherein a private organization acts as a "trusted party", may lead to large corporations creating monopolies; there is no reason for an individual to place trust with her data in such a party, as evident in the past and in a recent example of a third-party exploiting a user-data-centric social network's APIs against the policies of that social networking business entity.

To this end, we use the widely proposed ideas of decentralized and distributed identity management in which the user is the owner of her identity, a.k.a., "self-sovereign identity" (Allen 2017), and build upon it using the recent advances in Cryptography research, to fulfill any imaginable use-case that bases itself on identity as the first requirement. Our framework, called **OneID**, works within the upcoming open standards proposed by the W3C Verifiable Claims Working Group and other standardization bodies. OneID is a distributed, privacy-preserving, secure, self-sovereign credential management and verification system. It is compliant with the EU General Data Protection Regulation (GDPR) **by design**. OneID is *built on* the requirements from the privacy and security point-of-view: selective disclosure by zero-knowledge proofs-of-knowledge, equality predicates, key-binding, carry-over attributes, revocation of credentials and its security properties are *provable*[1].

Identity management and verification is one of the hardest problems, and is as old as the networks of people and society. In the following, we try to understand, briefly, the associated problems, and why self-sovereign identity is the correct solution by glossing over the contemporary and past solutions for Digital Identity – a requirement that emerged with the advent of the modern computer networks. For a detailed historical treatment of the subject, please refer to (Allen 2017).

[1] A formal security model analysis of the protocols used in OneID is out of the scope of this document, and is presented in a separate "yellow paper".

1.1 Evolution of Digital Identity

Identity management has evolved over the years. Starting from late 1930s to now, there have been many attempts to formalize individual and organizational identities. These efforts over the years may be classified into four different phases and paradigms, broadly.

Up to 1990s, **Centralized Identity**: *administrative control by a single authority or hierarchy*, e.g., US Social Security (since 1930s), IANA (1980s) [2]

From late 1990s to early 2000, **Federated Identity**: *administrative control by multiple, federated authorities*, e.g., Microsoft Passport, Liberty Alliance by Sun Microsystems.

Early 2000s until now, **User-centric Identity**: *individual or administrative control across multiple authorities without requiring a federation*, e.g., ASN, OpenID, OpenID Connect (based on the variants of OAuth), FIDO, Facebook Connect etc.

From 2012 until now, **Self-Sovereign Identity**: *individual control across any number of authorities*, e.g., efforts by Request Network, W3C Verifiable Claims Task Force.

We argue that first three paradigms mentioned above are inadequate in addressing some of the fundamental privacy issues that an "identity owner" and other entities in the system face.

In order to understand the issues, we need to address 1. the confusion that arises due to commonly used terms, clarifying what we mean by "identity", "authorization", "authentication" and "verification" and 2. formalization of the minimum requirements of modern identity systems.

Identity. A "Digital Identity" is a digital document that belongs to an entity, and it has a public identifier. Not all of the identity is public information. For example, a student's scholastic history is required by a university for her admission in higher studies, but the university does not require the knowledge of her choice of a mobile network operator or the mobile phone brand.

So far, the public identifiers have been seen to be unique, thereby creating a one-to-one mapping of a user and a set of services or a set of attributes enabling information leaks by correlation across different services. We claim that these public identifiers to an identity can be different to avail different services, while keeping a unique private identity (key).

There may be several agencies that may hold different or overlapping identity attributes of an identity.

Authorization. Authorization is a two-party or a multiparty process wherein a user holding an identity, authorizes a second party, independently or using a **trusted third-party** to use parts of her identity to avail a service.

Authentication. Authentication is a process that requires active participation by a user, who holds certain identity, to prove certain statements to be true about her identity.

[2] UIDAI's Aadhaar, in principle, is a Centralized Identity management system with biometric data and mobile phone numbers for 2 and 3-factor authentication.

Verification. Verification is the process that a notary or a trusted-party (in traditional sense) would carry out, i.e., ensure that an identity is valid and if someone needs it, can validate an identity or parts of it.

1.2 Basic Requirements of Identity Systems

Allen 2017 argues and proposes the 10 principles of identity, with which we largely agree. However, in order to provide realistic guarantees with the state-of-art in technology, we envision the identity as follows.

- A user must have an independent guaranteed digital existence without repudiation from any agency.
- A user must be in complete control of her identity, and this control should be limited only by well-understood and secure algorithms that ensure the continued validity and claims based on the identity. In addition, the user must have access to her whole ID data, wherever it resides.
- Identities must be persistent, but respecting the will or right (depending on the area of jurisdiction) to be forgotten.
- Identities should be as widely usable as possible, out of silos and proprietary formats, to limit replication, for optimal resource utilization.
- Users must agree to the use of their identity, or the parts of it. Any unauthorized use must be denied, and the user *may be* be alerted if her identity is in unauthorized use. Revocation of use of identity in case of unauthorized use must be possible.
- Disclosure of claims must be minimized. When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand.

1.3 Current Approaches

If the user manages her own identity for various digitally-enabled activities, she ends up with with multiple credentials. Multiple credentials expose the user to a variety of security issues. Moreover, such a scenario can not deal with the authenticity of one's assumed identity.

Among the approaches that can verify the authenticity, the most common approach works as a centralized identity management model[3]. The broad idea is depicted in Figure 1. There can be other components to add user's consent (authorization) and/or more security features, multifactor authentication, authentication using biometric records etc. We can't comment on the cryptographic and perimeter security properties of these approaches, and believe that there are strong security measures against possible threats. We have analyzed (internally at our organization) the security and privacy aspects of Aadhaar[4] (which we believe is one of the biggest enablers for financial and other services targeted at the populace of the second most populated country in the world) based

[3] E.g., UIDAI's Aadhaar in India.
[4] This research is available on request.

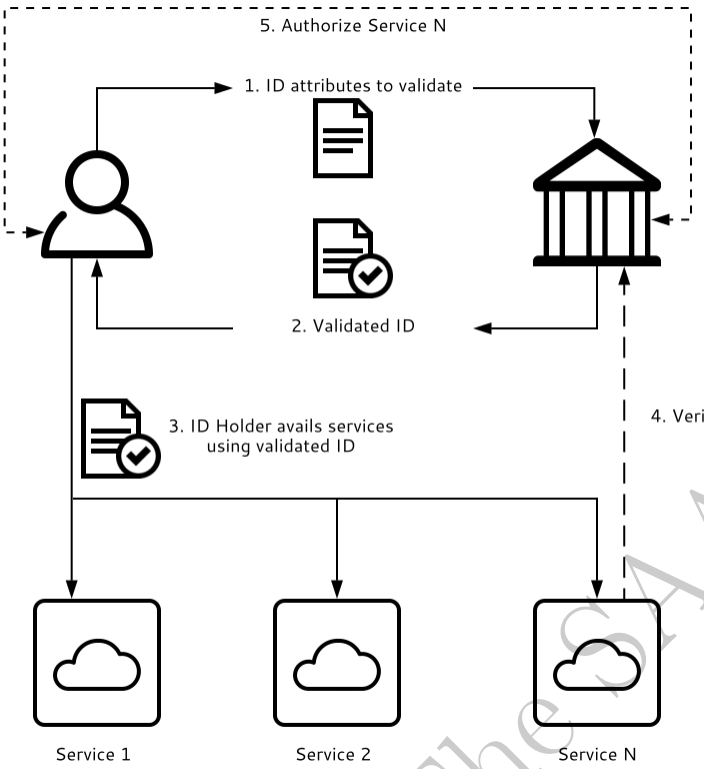


Figure 1: A simplified illustration of Centralized identity management

on the available public data and designs, as well as by consulting some prominent recent research by (Agrawal, Banerjee, and Sharma 2017) and (Rajput and Gopinath 2017).

OpenID (Recordon and Reed 2006) and OpenID Connect (Sakimura et al. 2014) are the user-centric solutions. For example, OpenID Connect (which is different from OpenID in design and architecture) is a protocol for delegated authentication in the web: A user can log into a service or a "relying party" (RP) by authenticating herself at a "trusted third-party", a.k.a. an identity issuer. For example, a user may sign into *Quora* by signing into *Google+ Sign-In* and authorizing *Quora*.

Both of these approaches use OAuth (E. Hammer-Lahav, Ed. 2010), OAuth 2.0 (D. Hardt, Ed. 2012) and some other variant with improvements and extensions (Denniss and Bradley 2017) to provide specific authorization flows for various digital applications. There has been a lot of research to from formal analysis to practical attacks on security of these flows over the years.

Very recently, the FIDO Alliance's Universal Authentication Framework (UAF) and Universal Second Factor (U2F) specifications "*to transparently leverage native security features of end-user computing devices for* ***strong user authentication*** *and to reduce the problems associated with creating and remembering many online credentials*" (The FIDO Alliance 2017). FIDO protocols complement federated frameworks (e.g., OpenID), as well as web authorization protocols (e.g., OAuth). It is important to stress here that some of the components used for OneID wallet subsystems are similar

to FIDO strong authentication components for one-time on-boarding, but without a trusted party.

However, these systems, centralized, federated or (more recently) user-centric, do not fulfill all the basic identity requirements that are commonly accepted guidelines, e.g., by the European Union's General Data Protection Regulation (GDPR), and pose serious privacy concerns evident from recent data breaches of the millions and billions of users at some of the organizations opting for these. Even though the data security arrangements may be of the highest standards, the federated and centralized identity managers have been known to be involved user-profiling, with or without the explicit consent of a user. There are scenarios where the ID attributes are not required, but the third parties ask for them, and those are stored by these third parties availing identity attributes from centralized or federated identity managers with or without proper security measures; either way, this may lead to correlation of identities across services and domains, and has been known to target many a Facebook users outside Facebook (for example). There have been instances when Facebook or other such agencies have disabled applications and services that indulge in "data stealing" and spamming activities, but this can't always be done.

Moreover, in trying to prevent unauthorized access, these identity managers may end up preventing the individuals (identity owners) from accessing their own data.

The only permanent solution is that we let the user be wholly in control of her identity attributes, do not store any such data in centralized storage or a distributed storage managed by one or a set of organizations.

1.4 Identity on Blockchain

At a very high-level, a blockchain is an append-only data store with decentralized consensus derived by incentives, providing strong immutability and transaction-order guarantees. The number of applications on blockchain has seen a growth explosion of late. Several proposals have come upon proposing the use of blockchain to store and manage identities and enabling identity-based, secure and irrefutable message-exchange protocols (that are at the core of almost all financial applications).

The reader would know that blockchain itself does not provide an "identity layer". Moreover, there are reasonable doubts on using blockchain (or a Distributed Ledger Technology) to solve the previously mentioned problems related to digital identities. These doubts closely relate to and sometimes stem from the applications and the scope of use of identities. Most use-cases can be fulfilled by the use of some cleverly (and of course carefully) designed cryptography protocols and some distributed storage mechanism (e.g., IPFS (Benet 2014)) and ensuring a total order on the timestamps of all operations. It just happens to be true that the blockchain, by virtue of its cryptocurrecies-oriented design goals, provides the mentioned properties.

However, if one to create an identity system at the scale of the people on the entire planet (and possibly providing identities to their assets), can we use a blockchain to be reasonably adequate to provide any kind of SLAs? Or is the solution such that the identities are maintained on a network of small networks? We have been puzzled with some of these questions, and trying to come up with

technical solutions[5]

2 OneID Identity

OneID and other self-sovereign identity projects give the user the control of her identity and attributes. Before diving deeper into OneID's approach, we describe a few terms that we will frequently use in rest of this note.

2.1 Glossary of Terms

ID attribute : An ID attribute is a validated component of an identity. For example, a university may issue an ID attribute to an individual and this ID attribute becomes part of an individual's identity.

ID attribute issuer : An agency that issues ID attributes. For example, a university will be an ID attribute issuer issuing a degree certificate for an individual.

ID claim : An ID claim is a statement about an identity, composed of claims using the ID attributes. A claim, for a clarity example, could be

"Public ID `6067054411837be873dadbae7f52ec891` is at least 18 years old and is a resident of India."

ID holder : An ID holder can be a person, a device or some asset. An ID holder has access to its own data, kept with it in encrypted form. We represent the identity data as a linked document. Such a document contains some meta-data and a set of ID Attributes. An ID holder may control other ID holders, in which case, the controlling ID holder is the "parent" and the controlled ID holder becomes a "child". For example, a car is an ID holder, however its ID information is controlled by an individual who is in possession of the car. Note that an ID holder or the parent of an ID holder is the "authenticator" (we are devising a self-authentication model).

ID validator : An ID validator is an entity (a service or an agency) that validates claims about identity attributes. Note that an ID validator is required to act only initially on a given ID attribute. In the longer run, the claims, along with some "metadata" can prove themselves. Think of ID validator as a digital noterizer.

ID verifier : An ID verifier is a service that needs an ID holders claims to avail some service. The ID verifier can be a service like a bank or it can be a third-party verifier whose truth-value is trusted by services.

Note that once we have the ID documents data structures *securely* stored with an ID holder, the future ID and ID attributes related transactions are only verification exchanges to avail services. Also

[5] An in-depth look at OneID R&D and technology is not in the scope of this high-level concept note, and is the subject of several papers that follow subsequently. Some of the research is patent-pending as well.

note that most privacy-preserving verification problems can be modeled as mostly conjunctive clause evaluation (assertion). These operations can be performed using semantically secure *homomorphic computation* in the ciphertext space.

2.2 Understanding OneID

OneID is being designed to provide the basic identity requirements (ref. Section 1.2). Broadly, OneID platform helps an ID holder to prove her identity issued by one or many ID attribute issuers without revealing any side-information, instantly in a non-repudiating way. Identities issued on Trust Net to individuals are a set of verifiable claims and attributes (e.g, Name, Age, Address, Registration Number, Photo) which are "validated" (signed) by ID attribute issuers. ID attribute issuer cannot track ID holders by correlating the services she avails.

ID verifiers (services) may ask (as per regulations and laws of the land) only verifiable blind claims or they may need partial information. OneID guarantees that any information other than required is not leaked.

Figure 2 is a high-level picture of OneID identities.

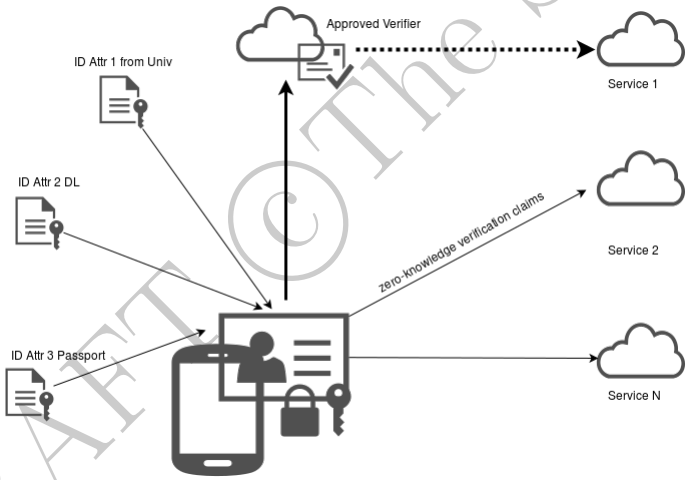
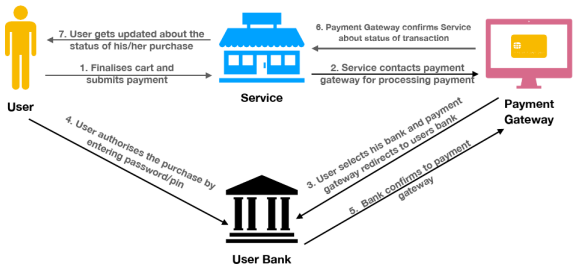


Figure 2: OneID identities

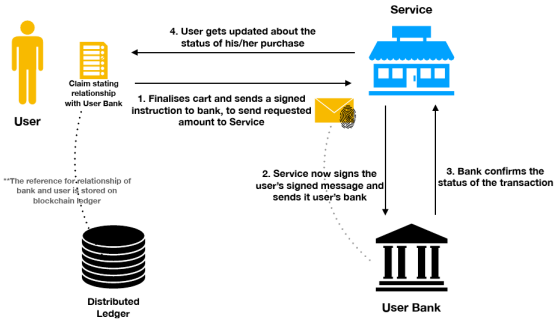
3 Use Cases

With an ID Holder able to completely control and prove her identity almost instantly using OneID (mostly) without the need of third-party verifier, there are numerous business opportunities that arise.

Payments : OneID has the potential to *disrupt* the current P2P payments operations. Figure 3a depicts the typical high-level information flow to make payments by a user to a service or product. The same scenario within OneID is depicted in Figure 3b.



(a) Traditional Payments



(b) Payments with OneID

Following is how payments work in OneID (also depicted in Figure 3b): Imagine there is a goods/payment transaction between a user and (say) an online marketplace. The core assumption here is that all three entities are part of OneID.

- The user finalizes the cart and sends a signed instruction (contract) to the marketplace. This contract asks the bank to pay a certain amount to the marketplace service.
- Marketplace service verifies the contract, signs it and sends it for clearing the payment to the user's bank.
- Bank confirms the status of the transaction.
- The user and service both get updated.
- All the parties participating in a transaction can know the state of the transaction at any given point of time.

We emphasize that all the participants using OneID are benefited: banks can banks can directly handle the instructions from users and enable payment services to anyone on OneID. Thereby with significant reduction in processing charges ($\approx 0.7\%$) charged by the payment gateways), banks can create a business model beneficial for both banks, who now become payment enablers, and services. Also, services which are part of OneID are directly benefited with the significant reduction on TDR (Transaction Discount Rate), and thereby increasing profit margins. The number of steps a user has to perform is significantly reduced, thereby improving overall user experience. And finally, by using DLT, all the parties participating in a transaction can know the state of the transaction at any given point of time.

KYC and AML Due Diligence : With constant change in global and local regulations to perform KYC/AML, both time and cost for organizations to satisfy these regulations cause a lot of overhead. Global surveys reveal a clear message: the costs and complexity of KYC are rising, continuing to weigh heavily on financial institutions. Another major concern with the organizations is relying on their existing clients to update their KYC information regarding any material changes.

Aadhaar and CKYC registry are welcome steps to reduce the KYC burden; in fact, the KYC

costs have come down by almost 90+% using Aadhaar and CKYC in India. OneID can do what Aadhaar and CKYC registries avail without the problems that centralized identities face. OneID does it more seamlessly and transparently to the user.

P2P Lending : P2P lending is growing exponentially globally, and the total value of loans issued on these platforms is expected to grow to US$150 billion by end of 2025 (PwC 2017). Leading companies in this space (e.g., Lending Club, Upstart, Prosper) charge the borrowers a fee in the range 0.5% to 26% based on the grade of loan. A major component of such high fees charged by the platforms for customer due-diligence they need to perform in order to reduce defaults.

Existing P2P lending platforms also cannot request collateral on their digital platforms. However, on ETHLend and Salt like lending platforms the users use cryptocurrencies as collateral to receive loans, thereby reducing the possibilities of defaulters.

OneID enables P2P lending platforms for easy due-diligence, and to make sure that all claims submitted by a borrower are true. Moreover, since any real world asset's identity can be managed by its owner (parent ID holder) and registered on OneID, the asset can be put as a collateral if required in the loan-contract between investor and borrower. All participating parties are always updated in case the previously-known state of loan specific attributes are changed.

Marketplaces : marketplaces face a big challenge of having sellers listing fake products. Another big challenge is fake reviews on the marketplaces. Existing marketplaces like Amazon have put some checks and balances but cannot completely stop them. Amazon.in, for example, promises to penalize sellers after the product sold is reported and confirmed to be fake. Because physical things and people have identities on OneID, the provenance problem becomes less severe. Figure 4 depicts the high-level view.

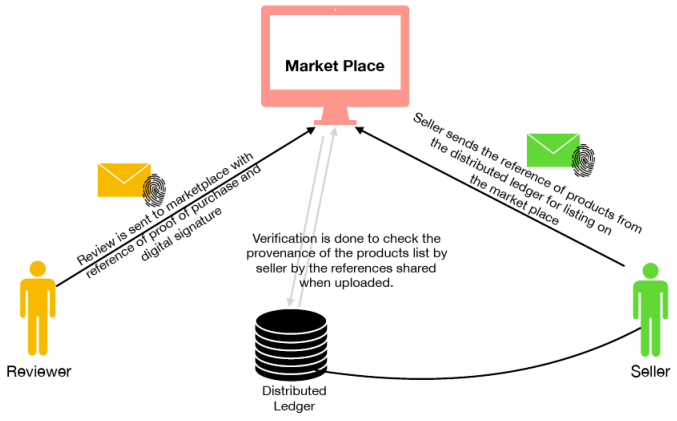


Figure 4: Easing of Marketplace operations

4 References

[1] Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma. "Privacy and Security of Aadhaar". In: *Economic and Political Weekly* Vol. 52.Issue No. 37 (Sept. 2017).

[2] Christopher Allen. *The Path to Self Sovereign Identity*. Mar. 2017. URL: https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md.

[3] Juan Benet. "IPFS - Content Addressed, Versioned, P2P File System". In: *CoRR* abs/1407.3561 (2014). arXiv: 1407.3561. URL: http://arxiv.org/abs/1407.3561.

[4] D. Hardt, Ed. *The OAuth 2.0 Authorization Framework*. RFC 6749. Internet Engineering Task Force, Oct. 2012, pp. 1–75. URL: https://tools.ietf.org/html/rfc6749.

[5] W. Denniss and J. Bradley. *OAuth 2.0 for Native Apps*. RFC 8252. Internet Engineering Task Force, Oct. 2017, pp. 1–21. URL: https://tools.ietf.org/html/rfc8252.

[6] E. Hammer-Lahav, Ed. *The OAuth 1.0 Protocol*. RFC 5849. Internet Engineering Task Force, Apr. 2010, pp. 1–38. URL: https://tools.ietf.org/html/rfc5849.

[7] PwC. *P2P Lending in India: A New Wave*. Whitepaper. July 2017. URL: https://www.pwc.in/assets/pdfs/ras/financial-services/compliance-cco-advisory-services/banking/featured-publications/p2p-lending-in-india-a-new-wave.pdf.

[8] Ajinkya Rajput and K. Gopinath. "Towards a More Secure Aadhaar". In: *Information Systems Security - 13th International Conference, ICISS 2017, Mumbai, India, December 16-20, 2017, Proceedings*. Ed. by Rudrapatna K. Shyamasundar, Virendra Singh, and Jaideep Vaidya. Vol. 10717. Lecture Notes in Computer Science. Springer, 2017, pp. 283–300. ISBN: 978-3-319-72597-0. DOI: 10.1007/978-3-319-72598-7_17. URL: https://doi.org/10.1007/978-3-319-72598-7_17.

[9] David Recordon and Drummond Reed. "OpenID 2.0: A Platform for User-centric Identity Management". In: *Proceedings of the Second ACM Workshop on Digital Identity Management*. DIM '06. Alexandria, Virginia, USA: ACM, 2006, pp. 11–16. ISBN: 1-59593-547-9. DOI: 10.1145/1179529.1179532. URL: http://doi.acm.org/10.1145/1179529.1179532.

[10] N. Sakimura et al. *OpenID Connect Core 1.0*. Specification. Feb. 2014. URL: https://openid.net/specs/openid-connect-core-1_0-final.html.

[11] The FIDO Alliance. *FIDO UAF Architectural Overview*. Whitepaper. Nov. 2017. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-uaf-overview-v1.2-rd-20171128.html.