A Comprehensive Evaluation of the Identity Management Utility Sovrin

Dutch Blockchain Coalition

connect and create

www.dutchblockchaincoalition.org

Abstract

Self-sovereign identity (SSI) management is a crucial element of today's interconnected society. However, there are very few identity management solutions that are truly self-sovereign and are mature enough to be production-ready. Following DBC's initial assessment of the maturity of SSI solutions [10], in this work we focus on Sovrin and further evaluate this SSI utility from various perspectives, such as technical, legal and security. The aim of this evaluation is to determine whether or not Sovrin serves as a basis to continue building on by the DBC self-sovereign identity track. Following our evaluation, we conclude that Sovrin has proven to be a serious contender in the self-sovereign identity space, but it is not a clear winner at the moment, nor is it a mature product. With the existence and setup of the technical platform, many use cases could be built. However, for the platform to become production ready many open issues would have to be solved.

Preface

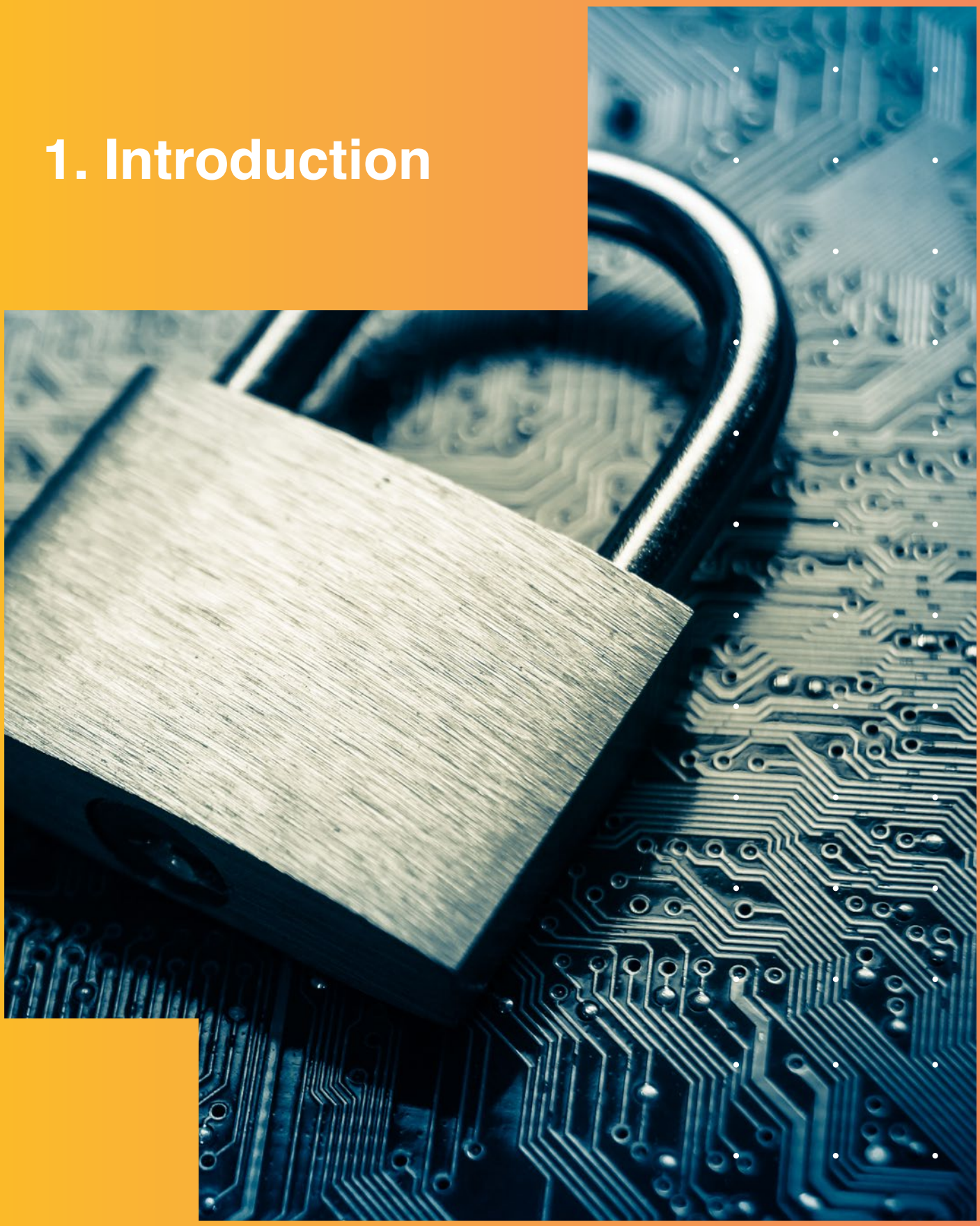
Digital identities are a crucial element of many applications in the digital world. The better we can trust who or what we work with on the other end of the digital connection, the more we can build important and relevant applications that serve people, business and society at large.
The Dutch Blockchain Coalition was established to build a strong foundation under blockchain applications. Digital identities are a key component in blockchain application and therefore it made sense to prioritize this topic.
The partners in the coalition consists of businesses, government and knowledge institutes who want to work in a pre-competitive environment. We believe in public private partnerships and in an open collaboration.
When choosing the topic of digital identities we earmarked a number of important to-do's. We needed an overview of what identity platforms are already available in the market place (report). Secondly, we wanted to get some real life experience with these platforms: Learning by doing.
Thirdly, we are experimenting with a use case that gives a perspective how these new identity systems can work in a concrete situation. For that purpose, we choose a mortgage case. We have built a working demo that gives a sense of what this will look like.
Finally, we want to aim for a digital identity that the government can agree to. Good work is ongoing at the TU Delft with Trustchain based on specifications of the Ministry of the Interior and Kingdom Relations.
In addition to the digital identities of people, we have started some initial work with identities of objects as well. This work has only recently started.

With regards to the first topic of identifying and selecting platforms, we believe in the concept of self-sovereign identities where the individual is at the center. Seven platforms emerged out of the long list we initially identified. Because of the international traction and the governance design, we chose to start experimenting with Sovrin.
This paper is the result of the work we have done with the Sovrin platform. To get a real view, reading white papers is not enough. We therefore devoted many hours on actual development and building a working Sovrin environment. That gave us the technical insights that are detailed further in this document.
In addition to the technology, we also looked at governance, legal and security aspects of the platform.
Although any evaluation is always bound to be limited and platforms change over time, we believe that this report will give a good sense of where Sovrin stands.

We want to thank everyone who has supported in creating these valuable insights. On and off there have been many contributors but in particular we would like to mention Peter Penning (ING), Tommy Koens (ING), Nicolas Castelon (CGI), Peter Nobels (Sogeti), Simon Sanders (CMS), Erik Jonkman (CMS) and Jacoba Sieders (ABN AMRO). And also the Tech Team: Ismenia Galvao (ING), Arturo Manzaneda (ING), Oleg Burundukov (ING), Jeroen van Megchelen (Ledger Leopard), Sergey Brazhnik (Ledger Leopard) and Artem Gorev (Ledger Leopard).

Contents

1. Introduction



Introduction

Contributors: Tommy Koens, Stijn Meijer, and Peter Penning

The Dutch Blockchain Coalition (DBC) considers that 'reliable identification and authentication are basic conditions for virtually all applications of blockchain'[1]. However, currently most identity management solutions are under central governance. Examples can be found in most social media platforms such as Facebook and Google accounts. Additionally, this extends to real world examples, such as a passport or a driver's license provided by government. Although these solutions seem to work in practice, there is an essential issue. Namely, the owner of the identity is not in control of his/her identity. For example, a social media platform may decide to remove an account based on its own policy, leaving the identity owner with a virtual gap in its existence. Additionally, identifiers (such as a passport) provide a lot of -arguably too much- information about the identity holder, even though only a single attribute (e.g. the date of birth) needs to be known. Indeed, identity owners are no longer in control of their identity when using centralized identity management solutions.

To overcome this issue, Allen [7] introduced the concept of self-sovereign identity (SSI). The idea of a self-sovereign identity aims at putting the user back in control of its identity. Allen introduced ten SSI principles [8] that aim to provide a user control of its identity. These ten principles were used by Koens and Meijer [10] to analyze nearly 50 identity management solutions. From their work [10] the identity management utility Sovrin [5] was chosen to investigate further to determine if Sovrin is suitable for industry and government standard (self-sovereign) identity management. This work provides the analyses of various aspects of Sovrin, including technical, legal and security perspectives.

2. Evaluating the Technical Quality of Sovrin

Evaluating the Technical Quality of Sovrin

Contributors: Oleg Burundukov, Arturo Mandaneza, and Peter Penning

In this section we evaluate the quality of Sovrin's software from various angles, which includes a code review and an analysis of its developer community size.

2.1 Evaluation of the software quality of Sovrin

The Sovrin software is a Hyperledger Indy blockchain technology product. It comprises several components, where each component performs a specific function in the architecture of Sovrin. All components are open-sourced. The components were cloned from a known repository, built and deployed by the ING team into a test environment.

Sovrin is a public permissioned network and ledger designed as a self-sovereign identity network. At the same time Sovrin is the business model and the trust chain. The entire technology domain used in Sovrin can be used outside Sovrin business model network too, having the trademark preserved. Moreover, the domain has a space for extensions, such as user-defined ledgers and transaction types. Note that in this document we interchange Sovrin and Indy terms.

The Sovrin code has been analyzed by ING DLT team. The team has focused on key components only, and the coverage of analysis varies per component, therefore the total coverage ratio is not yet 100%. These are the system components:

- **Indy plenum** implements Redundant Byzantine Faulte Tolerant (RBFT) protocol with specific Indy extensions;
- **Indy node** implements validator's node, extends "Indy plenum" consensus protocol;
- **Indy crypto** implements advanced cryptography for revocable anonymous credentials;
- **Indy SDK** implements an API for the Sovrin business protocol.
- **Indy agent** implements a communication protocol between client and server end-points in Sovrin.

Sovrin is positioned as a mobile-centric architecture, but we could not find code designated for mobile platforms. This leads us to the conclusion that the project is rather far from full accomplishment.

2.2 Code maturity metrics

Below we present the code metrics results we found on Github.

- Indy node: 1344 Commits/ 11 branches/ 643 releases/ 46 contributors
- Indy plenum: 3200 commits/ 19 branches/ 516 releases/ 34 contributors
- Indy crypto: 372 commits/5 branches/ 0 releases/9 contributors
- Indy SDK: 5400 commits/8 branches/ 7 releases/52 contributors

These numbers suggest that all projects are relatively new. The first two show strong maturity. The SDK, which is a key component for developing business applications, is currently in development and it has not reached the same maturity level. The agent component has been introduced very recently, and it is in active development too.

2.3 Code review

The overall quality of the code varies from module to module, which is likely the result of developing components by people with very different skills and experiences. For example, we found that design of Indy node attempts to follow Object Oriented Programming (OOP) standards, but at same time fails to deliver code clarity. In contrast, Indy SDK is very well structured and it follows the paradigm of the used programming language very well.

One large problem, which is common across the components, is the lack of clearly defined error codes and error messages. These errors can be hardly interpreted correctly by the users, as different problems lead to same generic codes in API.

Sovrin is written in two programming languages, Python and Rust. Python is used for the node and plenum components, while Rust is used for the SDK and cryptography. Note that cryptography library is used by both the nodes and the plenum consensus protocol.

The choice of languages is rather unusual. Python has become recently a very popular language next to Java for large enterprise projects. While Python remains good choice for the prototyping, hardly any modern enterprise system uses Python nowadays. Rust is a relatively rare language, and it has a number of advantages compared to scripting Python: Rust is very good at the static type checking, application memory management, overall execution speed and the compactness of a code. Rust is much better for server applications, therefore the team would recommend to rewrite plenum and node components in Rust.

The interaction with Rust SDK requires a language wrapper. Rust supports foreign-function-interface standard and the integration with SDK is same as an integration with any other native library.

Wrappers are merely delegation layers or "mirrors", and they require quite a coding effort. They must be delivered and maintained by the Sovrin team. We found that the wrappers from Sovrin are not often functionally complete, marked as "not ready for the production" and "for the usage at own risk".

2.4 Android integration

We were rather surprised that the Android platform is currently not officially supported, see the response in [4]. Taking into account that Android devices currently occupy 85% of the mobile market led us to evaluate whether SDK can work on this platform.

The SDK code was forked and subjected to standard build for Arm7 and Arm8-64 architectures. Unfortunately, we discovered that the code can not be ported directly to Arm without several SDK code fixes and amendments in the build scripts, but we eventually managed to run test Java application with Indy SDK in a smartphone. The application was tested to be able to perform Sovrin on-boarding and attestation functions.

2.5 Vendor info and feedback

Sovrin is developed by Evernym [2], the company where the product portfolio consists of sole Sovrin project. Our specialists met the leaders and technical experts of the company at Sovrin design workshop, where both sides presented ideas and working solutions for the platform. Evernym specialists showed the product roadmap and delivered detailed answers on many questions. We could clearly see the large effort the company puts into Sovrin.

Summary. To summarize this technical assessment, we conclude that Sovrin:

- Implements advanced distributed ledger algorithms;
- Supports user-defined ledgers and transactions;

- Delivers cutting-edge cryptographic identity primitives;
- Is open for the community;
- Is open for the usage outside Sovrin business model;
- Has not yet fully implemented the network architecture;
- Should have considered another programming language for the node and plenum code;
- SDK does not integrate well with Java;
- The code is unstructured at various places;
- Lacks clarity in the documentation;
- Does not support mobile Android platform yet.

2.6 Community size and trend in momentum

One important factor in the decision making to continue with Sovrin will be the assessment of international uptake and growth in usage.
To make this specific:

- Facts and figures on experiments/proof of concepts from Q42017 to now, and do we see a trend (up, equal or down).
- Facts and figures on growth of the codebase/ functionality.
- Facts and figures on size and diversity of the developer community.
- Facts and figures on competitors, do we see trends with the competitors.

The following information is based on input kindly provided by IBM (Arnaud Le Hors). The best source of information is the quarterly report the Indy project produced for the Technical Steering Committee [3]. Here are some relevant highlights:

- "One year after being accepted into Hyperledger, Indy has earned significant interest and developer support. Community contribution continues to grow, with 1,000+ commits on the project, and several hundred members of the mailing list and chat channels."
- "The Indy project saw increased developer interest globally (US, Canada, Finland, Netherlands, UK)"
- "Teams working on / with Indy currently includes Evernym, BYU OIT, BC.gov, WIPRO - to which we can now add IBM"

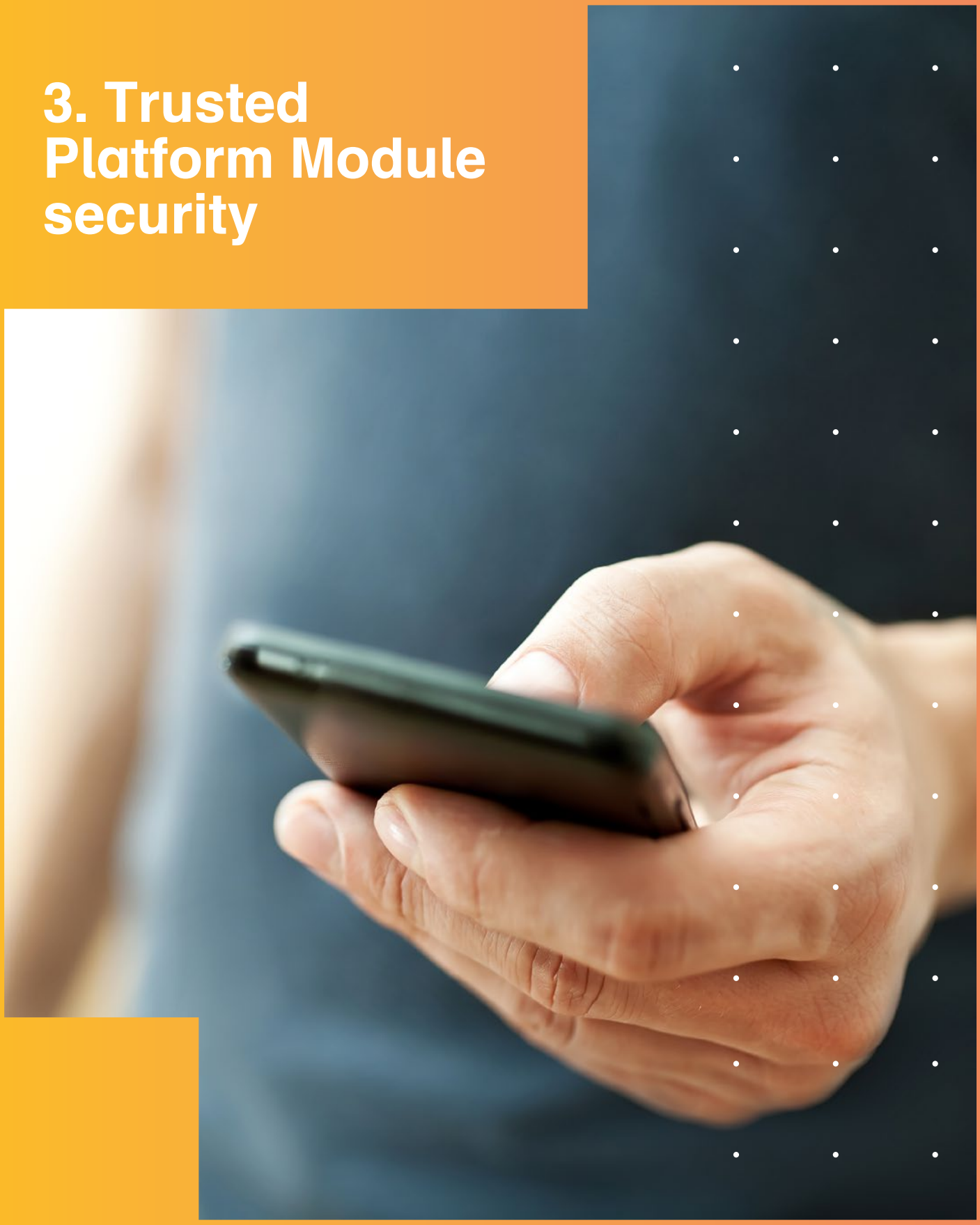
The Sovrin Trust Framework is currently "provisional". This means access is limited to allow for ramp-up testing. It should be finalized for full General Availability in Q3. Most of the activity for now is however on the test network which is starting to see some small amount of traffic. Nathan George (CTO of Sovrin) is working with many organizations that are saying they want to write to the live/production ledger right away (which means we won't see them on the test network beforehand), but many of them are still guring out POCs and integration schedules. So it could take them a while. A handful say they are starting soon, but it is up to them what that means. Fundamentally, there is little info on adoption that can be shared because:

1. They're seeing a lot of new development effort and organizations engaging with the system, but they are not sure which ones want to go public yet;
2. As a network trying to preserve privacy, they haven't tracked all adoption as much as perhaps they could.

Note that during the Sovrin workshop hosted by ING, more than 30 people from 10 companies attended.

In conclusion, there is a general sentiment that the momentum has increased in the first half year of 2018, but we cannot substantiate this impression with quantative facts in terms of e.g. developer community, PoCs or memberships. The trend seems up, but not exponential yet.

3. Trusted Platform Module security



Trusted Platform Module security

Contributor: Oleg Burundukov

Based on an extensive evaluation of Mobile Platform Security, we present here the conclusions of [9]. Gaining insight in the security of a trusted platform module allows us to determine how well the security of Sovrin attributes stored on smart phones is established.

The overall design of a system component Trusted Platform Module (TPM) is specified in several documents published by the Trusted Computer Group.TPM secures a memory where secret keys are stored, and it executes crypto-graphic algorithms while keys never leave the component. The specification is aligned with the mobile platform architecture of modern devices. The documents determine requirements and capabilities of a secure platform, so that a device equipped with a TPM should be able to withstand a wide range of attacks.

The specification does not particularize whether the TPM component should be implemented in ASIC or in software. A brief analysis of the differences between these options lead to the following conclusions:

- Tampering or reverse engineering of a hardware device leads to significant expenses conceivably unjustifiable by the value of hidden information;
- Hardware device can be manufactured to become invulnerable to side-channel attacks;
- Truly secure key storage should be implemented in hardware anyway, so that generated key never leave the device body;
- But the hardware solution has increased cost of implementation;
- Additionally, the hardware device body has to be replaced for algorithm updates, and stored keys must be transferred to new body.

These factors make software based solution significantly weaker but noticeably cheaper at the same time. Modern retail smart-phones do not have dedicated hardware TPM.

Currently, Android is taking approximately 85 percent of the market of smartphones, while IoS occupies the rest. The comparison of these two leads to following conclusions:

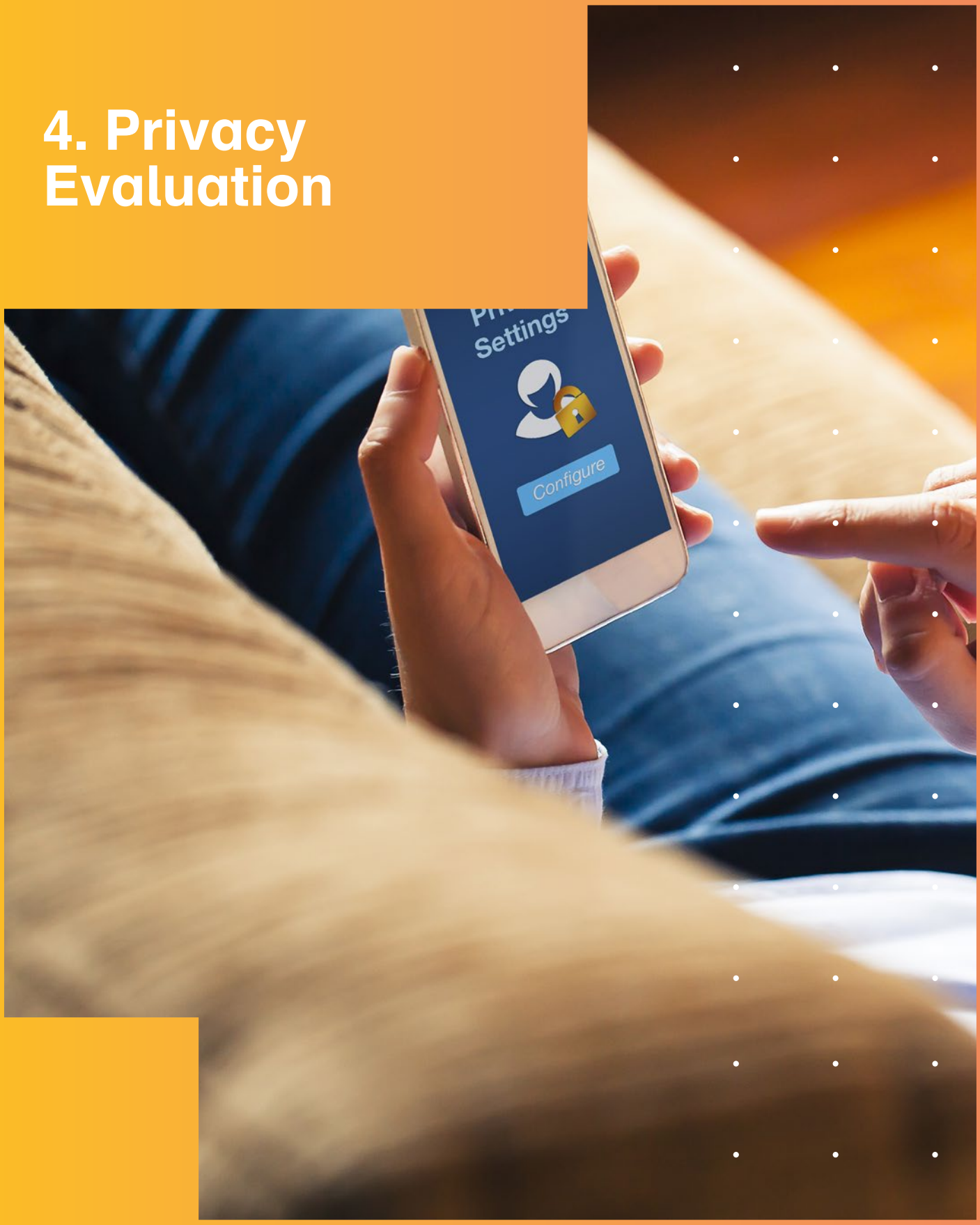
- Both IoS and Android OS use same CPU type and same ARM Trust-Zone technology, therefore they have same level of resistance to side-channel attacks. Dedicated crypto-processors used in laptops and servers are much more resistant to these attacks.
- Both mobile ecosystems execute users code in sandboxed environment, therefore they pose same threat level of application cross-talk attacks.
- Both systems support full disk encryption and the encryption per file. Both systems use disk encryption schema where single key may unlock entire device.
- Apple IoS uses proprietary CPU chip with hardware based key store, while Android phones use different chips across the ecosystem, and the key store may not be hardware backed.
- Android benefits from public attestation and acceptance of its open source implementation. IoS operation system seems to be better defended with its closed source code, but the risk of hacking is not entirely eliminated.
- Regarding the business models, Apple seems to invest generously into securing the devices. Disclosing a way of breaking into IoS is officially accepted and paid back with

substantial bounties. Android OS is not there yet, but Google made recently a lot of progress toward same level of protection.

The aforementioned facts lead to following summary:

- Both platforms deliver same level of overall security, where a device can be unlocked by single fingerprint or pin code;
- Keeping highly sensitive data in a smartphone requires another extra layer of encryption. The application-specific secret keys must be generated and they have to be independent from other keys in the system. For example, Samsung Knox works this way;
- Storing keys in a smartphone requires an additional hardware component to resist side-channel attacks. Such an additional chip is hardly an option in retail;
- These application-level keys have to be stored in an external hardware device. The device has to be kept in a sealed place and gets connected to the phone when necessary.

4. Privacy Evaluation



Privacy Evaluation

Contributors: Oleg Burundukov and Tommy Koens

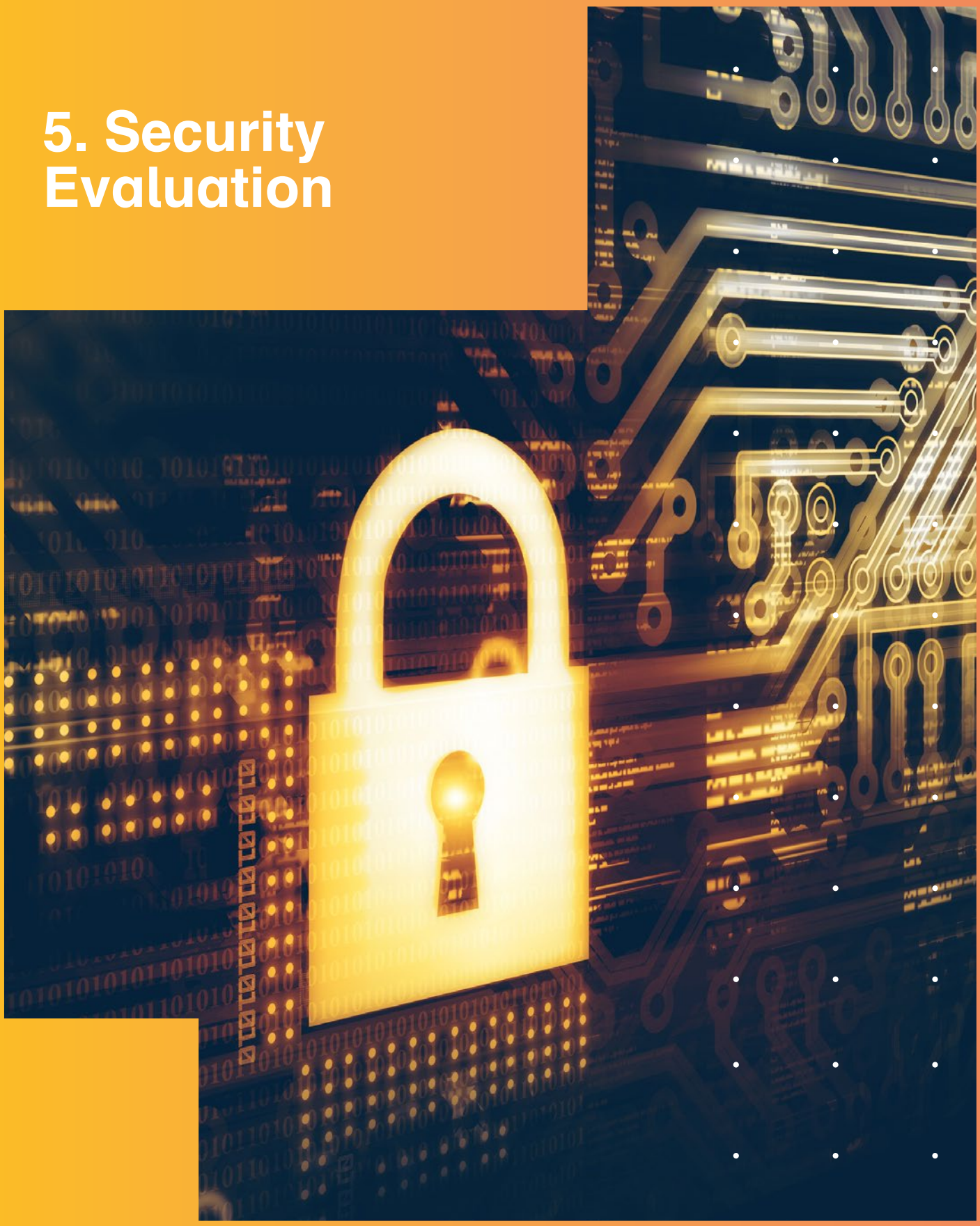
We evaluated the privacy regarding Sovrin based on the three claims made by Sovrin [6], these are:

1. Pseudonimity by default. Sovrin supports pairwise-unique DIDs and public keys.
2. Private by default. To prevent correlation, no private data is stored on the ledger, not even in encrypted form.
3. Selective disclosure by default. Sovrin verifiable claims use cryptographic zero-knowledge (ZK) proofs so they can automatically support data minimization.

During our analysis, we did not find any evidence that does not support these claims. Therefore, we assume that the claimed privacy aspects are correct. However, Sovrin's revocation technique is not fully disclosed by its current implementation nor its documentation. Therefore, we were unable to assess this mechanism.

Furthermore, due to time constrains we did not investigate the ZK components of Sovrin. In conclusion, Sovrin focuses on privacy which seems to hold, although we do acknowledge that our privacy assessment is limited to the three topics mentioned above. Further privacy evaluation is recommended, as privacy is an important subject in SSI solutions.

5. Security Evaluation



Security Evaluation

Contributor: Nicolas Castelon

In this section we evaluate the security of Sovrin and perform a business impact assessment.

5.1 Current landscape of blockchain security

There are currently no specific security standards that are directly tailored for blockchain technologies. Though this is the case, there are currently efforts by the Australian government along with panels of experts to produce an international standard for blockchain technologies. The ISO standard being developed is categorized under ISO/TC 307. This effort also includes the effort to determine security baselines, where two working groups are dedicated for that purpose. ISO/TC 307 SG3 focuses on Security and Privacy standards and ISO/TC 307 WG2 focuses on Security, Privacy and Identity. Without official standards and baselines, this report will address the security of blockchain technology taking into account the particularities that make a blockchain application different from conventional application. These differences refer more specifically to the decentralized design of the blockchain, the trust needed between the nodes to verify the transactions on the ledger, and the privacy of the users.

5.2 Current standards

As previously mentioned, the ISO standard ISO/TC307 addressing Blockchain and distributed ledger technologies is currently under development. The main standards taken within scope of this report are the ISO/IEC 27002:2013 and the General Data Protection Regulation (GDPR).

ISO/IEC 27002:2013 The ISO 27002 is the widely accepted standard for security of applications. This standard includes 14 chapters covering a wide range of security issues, including security baselines, compliance and security controls. For this blockchain application, we have paid particular concern to the following aspects: (9) access control, (10) cryptography, (12) operational security, and (13) communication security. All other chapters are equally important for the security of an application but are less relevant for the scope of this application as it is still in demo phase.

General Data Protection Regulation The General Data Protection Regulation (GDPR) is a major piece of legislation which came into effect on May 25th 2018. This EU directive is meant to ensure the privacy of EU Citizens across all digital applications storing or processing their data. The most pressing point will be in receiving consent from the users of this application, defining how the data will be used, and determining the relationship between the data controller, and the data processor.

5.3 General description of the application security

Blockchain applications are vulnerable to the full breadth of vulnerabilities and risks of conventional applications. Though this is the case, there are particular vulnerabilities that need more attention given the design of this technology. It is important to note that Sovrin, the architecture behind this application, has thus far not had any pressing security vulnerabilities disclosed. The following is a snapshot of the security controls that should be in place and evaluated once the technical white-paper is released by Sovrin.

User Authentication and End Point Security: Users accessing the application interface (API) should do so in a language such as C# as to prevent the source code to be directly accessed by the users. The application blockchain interface (ABCI) is to be hosted on a cloud provider. The security controls derived from a cloud environment are effectively outsourced to the cloud vendor.

Network and Node Security: The logging in, registration, data submission, and session storage should be done locally in every node. Every node should therefore be encrypted with AES 128 locally. This prevents nodes from having access to the original source code while being able to communicate with the other nodes.

Data Encryption: Once the user has been authenticated by a session hash, all further communication should be done in the AES 128 encryption standard.

Key Storage: After a session has been established, the ABCI and API should both contain an AES 128 key used to encrypt further communication. The key should be stored on the memory of both sides, meaning the key cannot be extracted from a node while both nodes are able to encrypt and decrypt the data.

5.4 IRAM risk assessment

The Information Risk Assessment Methodology (IRAM) is an Information Security Forum (ISF) template used to assess the risks surrounding an application. The IRAM consists of six different steps: scoping, business impact assessment, threat profiling, vulnerability assessment, risk evaluation, and risk treatment. As this application is still in demo phase, we will not be taking the last step of risk treatment into account. This step should be considered once the application is to be implemented in a production environment and the risk appetite of the application owner has been established. The IRAM framework has been chosen for this application as it is ISO 27002 compliant. As this application is in demo phase, the sections of the IRAM framework will be limited to tools current state. Applying this framework will provide a comprehensive snap-shot of the applications security posture in regards to ISO 27002 standard. The security posture will answer questions identifying the major vulnerabilities of the application, what security measures need to be in place, and the risk profiles of the vulnerabilities identified.

Scoping Scoping what will be included in the application is done to provide a business centric view of the risks that could be incurred. This phase is used to provide an integrated view of the risk by defining the technology infrastructure that will be analyzed. The scope of this analysis will cover the blockchain application in all of its estimated segments. As the technical whitepaper is currently not available, we have generalized the architecture to the following basic segments, which include the front-end, API, the different ABCI nodes, and the cloud environment.

Business Impact Assessment The business impact assessment will assess scenarios that affect the operation of the application. This phase is meant to determine impact of the application in terms of confidentiality, integrity, and availability of the service. We show our analyses in Table 1.

Table 1. Business Impact Assessment on Sovrin

	Assessment	Level of impact
Confidentiality	The communication with the API, communication between nodes, and the user authentication need to be secured through acceptable industry standards. The main impact of loss of condentiality would be for non-authenticated or legitimate users to also get access to the data in transit or in storage. This scenario could lead to violation of the GDPR, possibly incurring in high fines and additional financial losses derived from loss in user trust.	High. Signicant financial impact.
Integrity	The integrity of the information is at the core of using a blockchain application. As every node will need to verify the transaction and approve their validity, the integrity of the information is more dicult to falsify. Loss of integrity can lead to inaccurate representations of user identity, and therefore have an impact on the trust of the application and service.	Moderate impact on organization operations.
Availability	The availability of the data will depend on the availability of the nodes and the availability of the cloud environment hosting the API. In regards to the data, as every node will have a copy of the ledger, there will multiple backups of the information spread out across the network. This means the risk of losing the data is also spread out and thus reduced to a certain extent. In regards to the cloud environment, the issue of the availability has been outsourced to the supplier. The lack of availability of these resources can be assessed to have a high impact on its use given its reliance on the cloud environment.	High impact.

5.5 Threat profiling

Threat profiling entails understanding the threats that may affect the application. We show our resuts in Table 2.

Table 2. Threat profiling in Sovrin

Potential Threats	Description	Threat Level
Session Hijacking	An attacker taking over a legitimate user's session and having access to data and modifying data.	Medium
Social Engineering	An attacker getting access by soliciting authorized user through email, call or in person. The legitimate user discloses information intendedly or downloads malware that grants access to application or account.	High
User Authentication	User is incorrectly authenticated and gets access to API by intercepting session or hash.	Medium
Key Storage	Key storage is compromised and keys are revealed to unauthorized user.	Medium

5.6 Vulnerability assessment

The vulnerability assessment provides an overview of the controls needed to counter the threats identified in the previous section. We provide our results in Table 3.

Table 3. Vulnerability assessment of Sovrin

Potential Threats	Control	Description
Session Hijacking	SSL Security	"SSL security while it is actually TLS is a cryptographic standard for web browsers."
Social Engineering	Staff Awareness	All users using the application should take a mandatory training on social engineering and the do's and don'ts of safe online behavior.
User Authentication	SHA 256	SHA 256 is a cryptographic function used to run one-way algorithms to determine the integrity of the data. User should be authenticated through a hash function such as SHA 256.
Key Storage	AES 128	Advanced Encryption Standard (AES) 128 is an industry standard for encryption. All user communication and storage of keys should be done in AES 128.

5.7 Security as an enabler of trust

As it has been shown by applying the IRAM framework, the biggest risks faced by this application are session hijacking, social engineering, user authentication and key storage. With the exception of user awareness sessions, all risks have control measures implemented in the architecture of the application. User awareness sessions should be encouraged once the application is in full production. As stated earlier, the security of this application should be considered a label of excellence to ensure its trustworthiness to its users.

6. Governance Assessment

Governance Assessment

Contributor: Peter Nobels

The assignment for assessing Sovrin's governance raises the issue 'against which benchmark? Because Sovrin wants to realize a global solution for self-sovereign identity (SSI), the stakes are high. After all, a globally adopted SSI solution will become a vital component in all digital traffic for everyone! (this issue retains its relevance in the context of several globally used SSI solutions). This puts a great responsibility on those who are governing this vital component. The assessment framework should therefore help to answer the question: "What makes stake-holders such as users, public authorities and providers of connecting services can be confident that the governance of this vital SSI solution is in good hands".

6.1 Assessment Approach

We studied and evaluated the following material:

- Sovrin-Protocol-and-Token-White-Paper; Version 1.0 - January 2018
- The-Inevitable-Rise-of-Self-Sovereign-Identity; First released 29th September 2016; Updated 28th March 2017
- Sovrin-Provisional-Trust-Framework; 28 June 2017

6.2 Conclusion

The conclusions have been formulated at the level of the main questions. These conclusions are the result of the 'rolling up' of conclusions on the subquestions. In turn, these conclusions are based on the findings at the level of attributes (see the sections 'Assessment framework' and 'Findings').

1. Does Sovrin's governance offer confidence?
- The Sovrin Foundation identities the issues that need to be addressed in order to offer confidence in governance;
- Many good ideas and intentions which are in line with good governance;
- Too little protocolized;
- Too little transparency. For example, who are the members? Do they have proven expertise? What are their interests? How were decisions made? Where do the nodes run?

2. Is Sovrin's governance in line with the distributed ideology?
- Many good ideas and intentions. These are heading in the direction of a decentralized administration/organization;
- Too little autonomously running code (algocratic governance);
- Too little is irrefutable recorded.

6.3 Assessment Framework

The assessment framework is containing two parts: research questions and attributes.

Research questions

1. Does Sovrin's governance offer confidence?
   (a) Is there a sustainable balance of governance power
   (b) Is there sustainable transparency in governance?
   (c) Does the governance have operational checks & balances?
   (d) Is governance accessible, now and in the long term?
   (e) Is governance based on knowledge, skills & facts?

2. Is Sovrin's governance in line with the distributed ideology?
   (a) Is governance organized in a distributed/ decentralized way?
   (b) Is governance partially autonomous?
   (c) Are governance results irrefutably recorded?

6.4 Attributes

To be able to answer the sub research questions, attributes have been specified:

1. Balanced share of stakeholder groups in decision-making
2. Transparent governance processes
3. Transparent decisions and how they have been taken
4. Decisions are irrefutably recorded
5. Democratic and effective decision-making mechanisms
6. Distributed/decentralized (partially autonomous) governing bodies
7. Transparent objectives
8. Transparent governing bodies, including members, with tasks, powers, responsibilities
9. Transparent roles, and who fulfills them, with tasks, powers, responsibilities
10. Transparent accountability structures
11. Effectively organized supervision
12. Transparent rules on accessible membership
13. Transparent rules on ownership
14. Actors are experts
15. A level governance playing field
16. Transparent, complete and correct registers
17. Sound governance incentives and sanctions
18. Transparent standards (technical, semantics and ontology)
19. Open source & suitable technology
20. Nodes are well distributed over several parties.
21. Easy off boarding (data portability)
22. DOA (Decentralized Autonomous Organization): Governance is automated

Table 4 shows the multiple relationship between attributes sub research questions: In Table 5 we present our conclusions on the governance of Sovrin.

Table 4. Relationship between attributes sub research questions

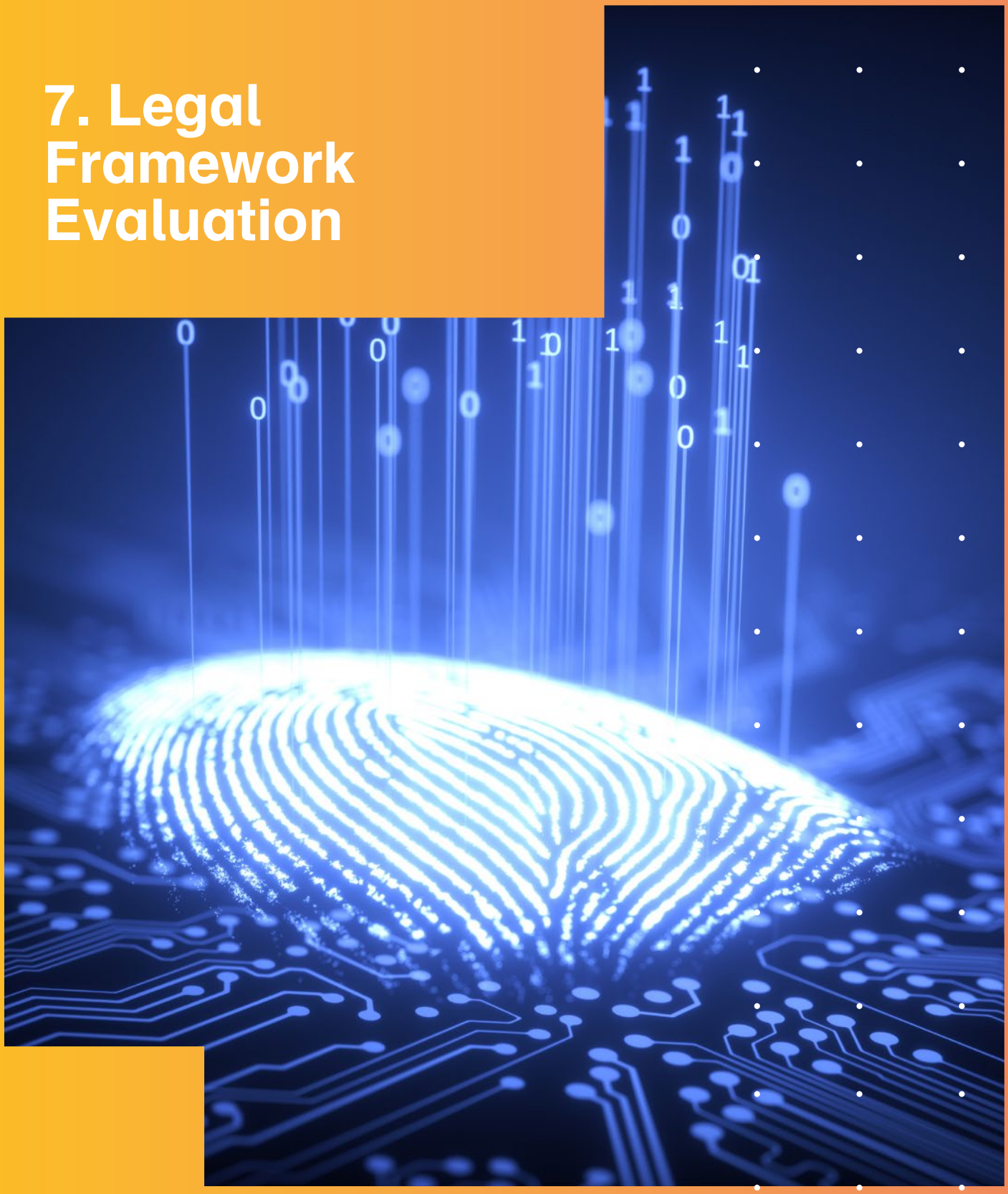
	1a. Balance of power	1b. Transparency	1c. Checks & Balances	1d. Accessibility	1e. Knowledge, skills & facts	2a. Decentralized / Distributed governance	2b. Autonomous executable governance	2c. Irrefutable governance results
1. Balanced share of stakeholder groups	X							
2. Transparent governance processes		X	X					
3. Transparent decisions	X	X	X					
4. Irrefutably recorded decisions		X			X			X
5. Democratic and effective decision-making	X	X		X				
6. Distributed/decentralized governing bodies						X		
7. Transparent objectives		X	X					
8. Transparent governing bodies		X	X					
9. Transparent roles		X	X					
10. Transparent accountability structures		X	X					
11. Effectively organized supervision			X					
12. Membership: transparent & accessible		X						
13. Transparent rules on ownership		X						
14. Actors are experts					X			
15. Governance: level playing field	X				X			
16. Transparent, complete and correct registers		X	X					
17. Sound governance incentives and sanctions	X							
18. Transparent standards		X						
19. Open source suitable technology		X	X					
20. Nodes are well distributed (several parties)	X				X			
21. Easy off boarding (data portability)	X							
22. Governance is automated		X			X	X	X	

Table 5. Governance findings

Nr.	Attribute	Findings (concise)
1	Balanced share of stakeholder groups	The Sovrin Foundation is working towards a balanced share of parties in its governance. The number of members is still limited and the occupancy rate is not yet balanced.The Sovrin Foundation has not clearly specified what it means by balanced stakeholder participation.
2	Transparent governance processes	A number of processes still need to be designed (protocolized) and installed. Dispute handling: where do you go as an identity owner if the system has been hacked and your identity has been revealed, violated (mutated) or stolen?
3	Transparent decisions	There is reporting of RFC-handling. It is not sufficiently clear to me, on a broad spectrum of subjects, what decisions have been taken within the Sovrin foundation and how they were made.
4	Irrefutably recorded decisions	Lack of recording of the Sovrin Foundation's decisions in a Distributed Ledger System (DLS).
5	Democratic and effective decision-making	Its not transparent whether decisions within the Sovrin foundation are taken democratically.
6	Distributed/ decentralized governing bodies	It is not yet clear to me how Sovrin's governance is organized decentral/distributed.
7	Transparent objectives	The objectives (duties) of the Sovrin Foundation are clear.
8	Transparent governing bodies	The governing bodies have been described in an elaborate way.
9	Transparent roles	There are templates for identity owners agreements and steward agreements.
10	Transparent accountability structures	It is not yet clear to me how the various bodies and parties are accountable to each other.
11	Effectively organized supervision	The Sovrin Foundation describes its plans to set up a monitoring system. How, is not yet clear.

12 Membership: transparent & accessible	Transparency: There are templates for identity owners agreements and steward agreements.It is not yet clear to me how the allocation of persons/actors to the different roles has been arranged.
13 Transparent rules on ownership	Who does the Sovrin code belong to (open source does not equal 'it belongs to everyone')? To the Sovrin Foundation?
14 Actors are experts	More openness about the expertise and interests of the members is paramount. Just saying that experts are independent experts is not enough.
15 Governance: level playing field	There is no evidence that actors with the same role can assert their rights to a greater or lesser extent.
16 Transparent, complete and correct registers	There is no irrefutable public register of actors that can be trusted to be correct and complete.
17 Sound governance incentives and sanctions	Are coins and premium claims a good idea? Is there the risk of violating the interests identity owners? For example, what if a relying party does not want to pay the amount? And: are unsound incentives introduced?
18 Transparent standards	Sufficient transparency.
19 Open source & suitable technology	How large and how active is the developers community around Hyperledger Indy? What are Evernym's interests? What interest does IBM have in Hyperledger Indy?
20 Nodes are well distributed (several parties)	Which stewards are running the nodes and where are these nodes located?
21 Easy off boarding (data portability)	How easy can an identity owner off board and take his/her data to another SSI solution?
22 Governance is automated	Sovrin does not have a governance DLS in which data is irrefutably recorded and in which processes are captured as algorithms (smart contracts).

7. Legal Framework Evaluation



Legal Framework Evaluation

Contributor: Simon Sanders and Erik Jonkman

In this section we explore the viability of Sovrin as a means for digital identification from a legal perspective.

Identity and identification are governed by several areas of law, not only with respect to the creation, but also with respect to the further use and processing of identity. In this chapter we will explore the relevant legal aspects of digital identity which are relevant to the potential use of Sovrin as a means for digital identification.

7.1 Identity

Identity, a concept which touches the very essence of who we are, is studied as part of inter alia philosophy, sociology and law. Who we are and what we do has become a disconcerting development in the digital arena, with potential far reaching impact on individuals and society. Individuals who have created online identities which they are no longer in control of, inter alia by virtue of the enormous volume of personal data processed.

The basis of these identities is usually the data provided by individuals, like Facebook or LinkedIn profiles and can be considered informal identities. These identities should be distinguished from the what is referred to in this contribution as formal identification means e.g. those means issued by government (e.g. passport) or regulated professional bodies. Formal identities are commonly based on administrative law or public law, whereas the informal identities are usually created by individuals themselves.

When evaluating identity from a legal perspective, the origin is one of the elements that is relevant for the legal basis and thus (legal) effect of identity, inter alia relevant for the evidence value / level of trust of the identity provided.

For this contribution we will assume that the origin of the identity / means of identification determines the potential scope, and therefore suitability as means of (formal) identification.

7.2 Digital identity (or DID)

Digital identity is in many aspects closely related to identity as we know it now. One of the most commonly used form of formal identity, is based on the process set out in administrative law, based on the registration of persons in a centralized register. This register also serves as a basis to create enhanced and physical forms or evidence of identity, the Dutch ID-Card or Passport, which also contains further (biometric) personal data.

DID is also closely related to the digital signature and authentication, which already exists in many forms. The distinction between DID and digital signature and authentication is not always clear cut, as both may serve a similar purpose. Broadly speaking one could say that the purpose of identity is identification, which by its very nature means the presentation of personal data, whereas with the digital signature and authentication, the presentation of actual personal data is not required.

DID is not merely a digital concept, but will require a carrier, enabling communication or visualization in a way that is reliable and complies with the standards described in the previous chapters.

When we refer to DID in this chapter, we not only mean the concept of digital identity, but also its application on the basis of the Sovrin Platform.

7.3 Creation of Basic Formal Identity

As a starting point for evaluating the legal aspects of DID, we have worked from the assumption that there will always exist a basic formal identity, which is derived from the initial (and central) registration of formal identity. We will hereinafter refer to this basic formal identity as the basic formal identity (BFI), which will consist of a limited set of personal data which will not change during the life time of a person. We will assume that the self-sovereign aspects (other than shielding) are by the very nature of the personal information processed in all probability very limited.

The BFI is derived from the registration of a new-born, which is an obligation which exists under Dutch administrative law. In this contribution we will not discuss the BVV and SKDB. Currently no other means of registration exist in the Netherlands.

For this evaluation, we will also assume that any further enhancement or processing of BFI will be based on attributes, which are validated on the basis of attestations, and that for certain (official) attributes, an indefeasible link to the underlying BFI is established on the basis of e.g. blockchain technology. For many of these layers of additional identity, we believe these will be self-sovereign, but some of them may still be dependent on third party approval and may be subject to revocation.

We will assume that any formal DID will have to be derived from an officially recognized form of identification.

7.4 BFI, legal basis and use

Proof of identity up to the age of 14 is not required under Dutch law, and as children up to the age of 14 have limited legal standing for which identification is required. Therefore, proof of formal identity is usually not a barrier to social participation. As from the age of 14, evidence of identity is required by law. The form of evidence is limited: only those means defined in article 1 of the Wet op de Identificatieplicht (WID), are accepted as formal proof of identity, which in practice means any individual under the age of 18 should either apply for a passport or other official (Dutch) recognized ID. No form of digital ID is currently recognized as official (Dutch) recognized ID, therefore Sovrin without further regulation, would not be a valid formal means of identification in certain circumstances prescribed by law. However, this does not necessarily mean Sovrin cannot be used for any form of formal identification. The articles 2:13, 2:14 and 2:15 of the Dutch Administrative Law Act provide for digital communication with decentralized government, to the extent such communication has been agreed and sufficiently secure and does not cause undue burden.

Furthermore, art. 2 of the WID does not require identity papers to be carried by an individual, but an individual should be able to demonstrate evidence of such ID (the so called toonplicht). In addition, the WID allows for the additional or certain documents on the basis of a ministerial decree.

Therefore in administrative law, or on the basis of a ministerial decree, certain proofed digital copies of an official (Dutch) recognized ID, could be used as evidence of identity. Such DID would probable be derived from an official (Dutch) recognized ID, and the process of creating a DID should be integer / supervised. This means that the both

creation of the DID and the DID itself, will need to comply with certain (technical and procedural) standards. With respect to such standards we refer to the previous chapters of this report.

As with both current legislation on e.g. DigiD and the eIDAS regulation, such standards are imbedded in law and could serve as guidance for the implementation of Sovrin as means of DID, more in particular the standards as set out in 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.

Note that according to the Sovrin foundation, the Sovrin Trust Framework is not by itself an identity assurance framework as referred to in the eIDAS regulation. However it can apparently interoperate with identity assurance frameworks such as those based on NIST 800-63 or eIDAS source: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Provisional-Trust-Framework-2017-06-28.pdf). Thus it may qualify as a Platform for creating a DID, but for actual transacting with governmental bodies will depend on recognized identity assurance frameworks.

7.5 BFI, SSI and the GDPR framework

This section is restricted to the processing of personal data under the GDPR. Processing of other information (e.g. Financial information) an any specific regulation with respect to such transactions is not included in this section. For a technical evaluation of Sovrin we refer to the previous chapters.

As discussed above, personal data is processed both at the moment of creation of the DID, and any subsequent transaction with a DID. The GDPR in summary allows the processing of personal data, subject to there being a valid ground for such processing and subject to the safeguards as set out in the GDPR. Those safeguards can be summarized as safeguards with respect to security, restrictions on sharing and the validation rights and the right to be forgotten. Thus, the DID solution as proposed within the Sovrin framework, has to comply with these safeguards as provided for in the GDPR. We refer to the previous chapters for such assessment. Depending on how DID is implemented with the Sovrin framework, DID may run into constraints, as the use of certain technologies and network infrastructure may restrict the exercise of certain fundamental rights of data subjects under the GDPR, like the right to be forgotten or the right to have certain data erased or rectified. These right pose technical challenges for which several solutions are being explored. Considering the initial phase of the project, these (and other topics) will require further discussion and will impact design of the design of any DID solution.

8. Further Evaluation

Further Evaluation

Due to time constraints we were not able to evaluate the following topics:

- Cryptographic quality and maintainability
- In-depth privacy evaluation
- Legal framework
    - Processing grounds, use of DID
    - Processing grounds, safeguards
    - Right to be forgotten
    - Right to information processed
    - General safeguards
    - Destruction and Back-up

9. Conclusion

Conclusion

Contributers: Dutch Blockchain Coalition

From a technical perspective the maturity and quality reflects the startup nature of the founders, Evernym. It shows high quality of individual contributors, and lesser quality from other contributors. In particular, the functionality to run on Android was painfully missing. The total number of contributors is, however, growing, which is positive. Furthermore, we do not see an exponential uptake of the platform in the first half year of 2018.

Following the technical analysis of Sovrin, we conclude that its cryptography seems robust. From a privacy perspective, however, many more aspects have to be addressed before a conclusion can be drawn, most notably on the solution for storage of personal data.

The security aspects are not fundamentally different from standard solutions, as the blockchain technology is only a small part of the total solution. This implies that many of the regular threats and vulnerabilities will exist and must be addressed.

From a Legal perspective, if Sovrin-based Digital Identities were to be recognized as legally valid for government services, attestations by parties currently having this authority by law (government, notary, Chamber of Commerce) would be required.

All in all, Sovrin has proven to be a serious contender in the self-sovereign identity space, but it is not a clear winner at the moment, nor is it a mature product. With the existence and setup of the technical platform, many use cases could be built. However, for the platform to become production ready many open issues would have to be solved.

References

1. Dutch Digital Delta. Actielijn 1 - Digital Identities. https://www.dutchdigitaldelta.nl/en/blockchain/actielijn-1.
2. Evernym. https://www.evernym.com/.
3. Hyperledger wiki. https://wiki.hyperledger.org/groups/tsc/project-updates/indy-2018-may.
4. The lack of support for Android existed at the time of building the software. In July 2018 Android support has been added. History can be found at https://jira.hyperledger.org/browse/IS-582.
5. Sovrin. https://sovrin.org/#row_2.
6. Sovrin: A Protocol and Token for SelfSovereign Identity and Decentralized Trust. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf.
7. Christopher Allen. The path to self sovereign identity. https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md.
8. Christopher Allen. Self sovereign identity principles. https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md.
9. Oleg Burundukov. Mobile Platform Security. To be published.
10. Tommy Koens and Stijn Meijer. Matching identity management solutions to self-sovereign identity principles. https://www.linkedin.com/pulse/matching-identity-management-solutions-self-sovereign-tommy-koens/.

Dutch Blockchain Coalition

connect and create

info@dutchblockchaincoalition.org

www.dutchblockchaincoalition.org