Lessons For The European Passport-Grade Digital Identity
Survey on the failure of the public key infrastructure for 35 years

– *student project* –

Adrian-Tudor Dumitrescu
Delft University of Technology
Delft, The Netherlands
A.T.Dumitrescu@student.tudelft.nl

Johan Pouwelse
Delft University of Technology
Delft, The Netherlands
J.A.Pouwelse@tudelft.nl

***Abstract*—**

I. Introduction

Digital identity is a rapidly growing field, driven by the increasing need for secure and trustworthy online transactions, prompting even governments to take action towards the future of the population. This transition reflects the profound impact of technology on how individuals perceive and manage their identities in an increasingly interconnected and online world. While the adoption of digital identity has yielded mixed outcomes, it bears the potential to endow individuals with social and economic empowerment, with the capacity to unlock economic value estimated to range between 3 and 13 percent of GDP by the year 2030 [40].

Digital ID systems, despite being promoted for development purposes, pose serious human rights risks and often suffer from implementation failures. These risks are acknowledged even by proponents of such systems. Unfortunately, there is a lack of comprehensive evidence and monitoring of their human rights impacts. Activists, journalists, and researchers have played a crucial role in documenting these impacts, particularly in cases like Aadhaar in India. The evidence gathered so far reveals that digital ID systems can result in various urgent human rights issues, including violations of the right to nationality, restrictions on access to healthcare, food, and social security, and a range of other concerns [48].

Public key cryptography, a pivotal technological advancement articulated even more than 40 years ago [27], underpins the security of public networks, enabling global communication and commerce. To establish trust and identity in digital communication, public keys, and implicitly private keys, must be associated with specific identities. This necessity led to the development of Public Key Infrastructures (PKI), which facilitate the issuance and storage of digital certificates. These certificates verify that a public key corresponds to a particular entity. Certificate authorities (CAs), trusted third parties, publish these certificates, connecting public keys to users via a private key. Public key cryptography has played a crucial role in establishing online identity, from traditional PKI and CAs to experiments like PGP's web of trust, and more recently, the blockchain ecosystem [13] that needs to authenticate the nodes of the networks and use different PKI approaches such as Multi-Layered Approach, Instant Karma PKI or Guardtime Approach [41]. However, this relationship has its disadvantages in such that the shortcomings PKI brings can affect future digital ID infrastructures.

The interest of the European Union regarding the usage of digital ID has increased in recent periods, incorporating this vision in the EU developments and since 2021 drafting recommendations towards "a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework" [16]. As Europe advances toward seamless digital verification, caution must be taken not to create a surveillance state and a centralized 'digital identity' as it has the potential to erroneously label legitimate users as 'bad actors'. Accumulating sensitive digital information raises security concerns, and misidentification risks hindering legitimate users. Digital verification, like secure blockchain, offers advantages over paper documentation, reducing forgery and theft risks. To succeed, these digital systems must comply with the GDPR and align with the European Commission's 2020 data strategy, promoting secure and universally usable digital identities within common European data spaces as also stated by William Echikson in "Europe's Digital Identification Opportunity" [19].

This survey attempts to explore and reason the problems the PKI systems had and still exhibit after a long time from its introduction, alongside a history of possible alternatives ending with electronic ID implementations and failures from different countries. In section II we discuss the big problems

of PKI and what risk it presents in incorporating it in different domains. Next, in section III, we attempt to define a timeline of possible infrastructure alternatives that try to solve in part the PKI shortcomings presented. In section IV, we discuss how different countries in the world tried to implement digital identity and what point of failure they encountered, followed by conclusions.

II. PKI PROBLEMS

In recent years, Public Key Infrastructures (PKIs) have gained attention, with many organizations announcing their intention to provide certification services to the public. However, only a few have succeeded, and there are several reasons behind the failure of PKIs, which can be categorized into technical, economical, legal, and social factors [29].

- **Technical Reasons**:
  The technical landscape of PKIs is beset with complexities. Central to PKIs are public key (X.509) certificates, intricate and non-intuitive data structures. Their complexity poses substantial obstacles to deploying PKIs on a large scale, which is at odds with the direction of creating national or global digital identities. Furthermore, managing certificates, including tasks like key pair generation and certificate revocation, proves to be a daunting and error-prone undertaking. PKIs rely on globally unique X.500 Distinguished Names (DNs), which are often challenging to define and maintain resulting in death-by-complexity of its usage. Alternative models like SPKI and SDSI have struggled to gain widespread adoption. Additionally, cross-certification, the mutual recognition of Certificate Authorities (CAs), faces challenges due to variations in certification practices and a lack of incentives for cross-certification.
- **Economical Reasons**:
  Establishing and operating a PKI necessitates substantial investments in secure facilities, hardware, and personnel. Calculating the Return on Investment (ROI) for PKIs is intricate since they provide infrastructure rather than specific chargeable services. This intricacy makes building a sustainable business case for Certification Service Providers (CSPs) offering certificates a formidable task, given the high costs and limited revenue streams.
- **Legal Reasons**:
  PKIs raise questions about liability, with certificate providers potentially held accountable for damages resulting from misuse or technical failures. As further elaborated in the subsequent discussion of risks, the inability to repudiate digitally signed statements can lead to predicaments for certificate owners who may be unjustly held responsible for actions they did not authorize.
- **Social Reasons**:
  Certificates are sometimes misunderstood as a means to establish trust, but trust in digital relationships differs from real-world trust based on personal experiences with the level of trust we get from certificates often being overestimated. In addition, users often lack awareness of the vulnerabilities and risks associated with public key cryptography, accepting certificates without considering potential security implications.

As highlighted by Carl Ellison and Bruce Schneier in various risks associated with Public Key Infrastructure and the use of digital certificates, PKI is not a silver bullet for security and has potential pitfalls and challenges in its implementation [15]. These risks are presented as:

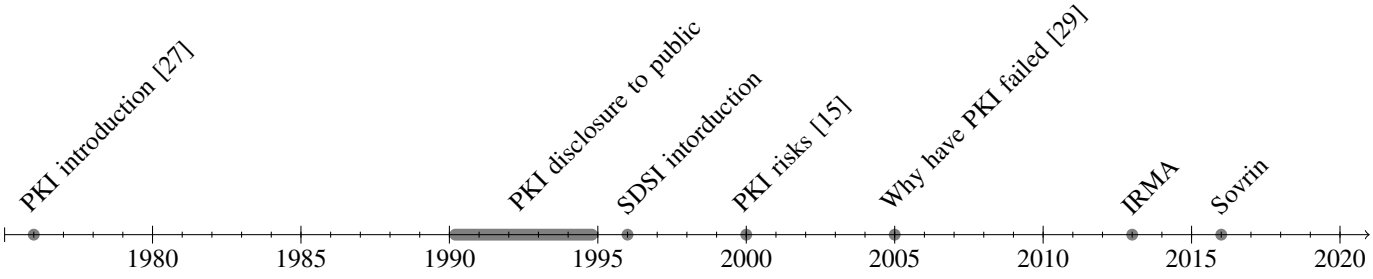
- **Trust in Certificates**
  The risk of misplaced trust in certificates issued by Certificate Authorities (CAs). Just because a CA is "trusted" doesn't mean you can necessarily trust a certificate for a specific purpose.
- **Identity Verification**
  Challenges in verifying the true identity of the certificate holder, particularly when relying on names or other identifiers.
- **Non-Repudiation**
  Legal issues surrounding non-repudiation, where individuals may be held legally responsible for actions taken with their private keys, even if those actions were not their own.
- **Security of Verifying Computers**
  The need to ensure the security of computers used to verify certificates, as compromising these computers can lead to security risks.
- **Certificate Authority Authority**
  Questions about the authority of CAs to grant specific authorizations in the certificates they issue.
- **User Involvement**
  The importance of considering users' understanding and actions when using certificates.
- **Registration Authorities**
  Risks associated with the use of Registration Authorities (RA) in addition to CAs in the certificate issuance process.
- **Certificate Holder Identification**
  Challenges in identifying the certificate holder, especially when relying on external sources like credit bureaus.
- **Certificate Practices**
  The importance of well-designed certificate practices and standards to ensure the proper use of certificates.
- **Single Sign-On**
  The need to consider how PKI integrates with other security practices, such as Single Sign-On (SSO), and the limitations of SSO in maintaining security.

III. A HISTORY OF ALTERNATIVES

A. SDSI

SDSI, or A Simple Distributed Security Infrastructure, is an innovative framework designed to address the complexities of security in distributed computing environments [46] tackling the first PKI problem presented while offering a robust and flexible solution, a first step in direction of SPKI(Simple public key infrastructure).

Fig. 1: Timeline of alternatives and problem statements for PKI



One of the most important features of SDSI is its simplicity. It achieves this through clear and intuitive mechanisms that focus on fundamental aspects of security by defining and representing security principles, establishing naming and addressing conventions, and expressing security policies.

By providing a straightforward means to define who or what can access resources, SDSI simplifies the task of managing access control. This clarity extends to naming and addressing, enabling a seamless way to locate and identify entities within a distributed network. SDSI recognizes that trust is a foundational element in security, and its framework allows for the establishment of trust among various entities within the system.

While SDSI offers a good step towards a less problematic infrastructure in distributed environments, it's important to acknowledge that it may not be suitable for all use cases with an accent on digital identity. As state also by the creators of SDSI, "We feel [...] identity certificates must typically in the end be examined by people, to see if the name and other attributes given are consistent with the attributes known to the human reader" [46], the problem of trust is transferred to the issuer(country in our case).

Over the years after SDSI design, multiple attempts have been made to use it in more practical ways to be able to overcome the problem of economic reasons. For example, in 1997, one year after SDSI release, a C library was created [20] to pave the way for its usage in different scenarios alongside a Java implementation in 1998 [37] followed by an implementation of a secure web client using SPKI/SDSI certificates [36] in 2000, to meet the growing importance of the World Wide Web and with a case study on the effect on a company.

B. IRMA

IRMA stands for "I Reveal My Attributes" and is a project aimed at implementing attribute-based identity management that seeks to address issues related to attributes, their possibilities, and challenges [5].

The paper acknowledges the existence of cryptographic techniques for secure and privacy-friendly attribute-based authentication, noting that recent advancements in smart card technology have made it possible to deploy attributes in practical scenarios. The concept of attributes [6] is used broadly to describe the properties of individuals. These attributes may range from anonymous attributes (non-identifying), such as gender or age, to identifying attributes, like bank account or social security numbers. The paper highlights that while the underlying technology ensures full unlinkability, attribute values may allow for linkability expanding the range of application scenarios. It relies on the Idemix technology and uses personal smart cards as carriers of credentials and attributes

The extensive use of attributes within IRMA leads to dependencies between attributes, where the issuance of one attribute may depend on the verification of another. These dependencies give rise to a tree structure for attributes and raise questions about what should be considered "root" attributes that do not depend on others. These considerations have implications for societal identity structures, including pseudonym accounts.

The paper suggests the involvement of an independent, non-profit foundation to manage the IRMA scheme, set policy, and oversee certificate management for access to the card. This foundation would play a crucial role in addressing sensitive issues related to attribute management and policy solving perhaps the economic and legal problem of monopoly of a company on a scheme.

More work has been added to the IRMA project, with an implementation for smartphones [7] in 2017 to facilitate its usage by ordinary people (with an app and QR codes) but also for service providers using standardized JSON Web Tokens. In 2019, solutions were proposed to contribute to ensuring the confidentiality and integrity of IRMA credentials in various scenarios. "Backup and Recovery of IRMA Credentials" [17] emphasizes that a recovery solution for IRMA should be designed as a backup and restore mechanism. To enhance portability and user-friendliness, the backup should be encrypted in a way that allows storage in any location without imposing a specific storage location on the user.

In this, key management is a crucial aspect of the design. The primary solution involves using a mnemonic phrase that can be written down on paper, an approach that does not require technical expertise and is understandable to users. Additionally, parts of the key are managed by trustees or a trusted institution as a second authentication factor to enhance security.

C. Soverin

Security requirements for digital identity systems mirror those of traditional paper credentials, encompassing compati-

bility, unforgeability, scalability, low latency, and revocation capabilities. Digital identity systems offer advantages like minimal dependencies, privacy/anonymity, unlinkability, and selective disclosure, providing a level of control impossible in paper-based systems.

Privacy-oriented digital identity schemes, such as U-Prove and Idemix, have been proposed but face challenges in widespread adoption due to issues like compatibility and scalability. For that, Sovrin is a system that integrates anonymous credentials with revocation, emphasizing privacy, unforgeability, performance, and unlinkability. The implementation incorporates a distributed ledger inspired by Ethereum and Byzantine Fault Tolerant (BFT) protocols for scalability [53].

Sovrin employs anonymous credentials based on zero-knowledge proofs, providing unlinkability and features like delegation and revocation. Privacy concerns are associated with revocation, but in [31] paper, attribute-based sharding are proposed to enhance privacy during the revocation process(and closing the gap to IRMA). The revocation methods involve cryptographic accumulators for efficiency.

Overall, Sovrin aims to address privacy and security concerns in digital identity systems through its innovative design and implementation and states from its requirements "self-sovereign identity, where every person, organization, or thing can have its own truly independent digital identity that no other person, company, or government can take away" [45]. Furthermore, the paper explains what most distinguishes Sovrin as a distributed identity system: it is the first public permissioned ledger. The stack of the technology has 3 important levels: Sovrin Ledger, Sovrin Agents and Sovrin Clients.

In a comparison between IRMA and Sovrin [38], adopting Sovrin is considered challenging for both service providers and credential users and, like the PKI, its commercial value can be overseen. At the same time, Sovrin is a complex project and still in progress with its documentation, being an open source, being somewhat scattered around. However, Sovrin has an advantage over IRMA in deployment in such that service providers do not need to host any server because of the Sovrin Ledger. Regarding the digital identity problem, Sovrin has been cited as a possible solution for the technology needed in such schemes [54].

IV. National digital identity implementations

In recent years, worldwide there have been multiple attempts to create a national digital identity for its citizens sometimes expanding to inter-state agreements and continental recognition such as the eID. The majority of these attempts incorporated the PKI and blockchain ecosystem and tried to strengthen security with interviews(Estonia) or biometric data. While using PKI in e-Gov is not a new idea, present since 2000 [12], even the latest implementations acknowledge the shortcomings of the PKI. For example, the UAE digital ID project was started based on such an infrastructure and even after its release and years of research the vulnerabilities presented in section II still persist [24] with the focus being on a lack of business value, business requirements and business integration issues alongside "much confusion about the full scope of this project" [4]. The risk in such systems may also explain the decrease in rapid adoption of digital identity solutions that started 'promising' like the EU nordic common eID [25] project started in 2015 with a set timeline that was not continued until 2023 yet. But these failures did not stop other countries from fully embracing forms of digital identity and the benefits of such adoptions have been studied more in recent years ([51], [49], [40]) to determine the financial impact. Here we present some cases in the world of a national electronic ID.

A. India

The Indian digital ID scheme, 'Aadhaar' [52], was first introduced in 2010 and has been linked to almost all states within the country [10]. The project aims to provide a single, unique identifier that captures all the demographic and biometric details of every resident of India and is close to issuing Aadhaar digital ID cards at the same time as birth certificates. Even though the system tried to pass the risks and problems of the PKI, the biometric implementation of Aadhaar raised privacy concerns from the start and is regarded as a failure in the citizen-government relationship [18]. This example shows that implementing a biometric ID scheme can be very delicate and comes with its risks as well that may balance the benefits, reported to be in 2018 at almost 10 million euros [44]. In this type of ID scheme, privacy and integrity of the data is critical, a weakness that the indian system encountered in leakage of critical information [47]. Aadhaar is the world's largest biometric identity database in the world, so it is vital that the privacy of individuals is not breached and the data is used only for the purpose for which it has been approved. Even after years of use the problem and skepticism still exists [2], with a big accent on availing welfare benefits, governmentalism, authentication without consent and dependency on connectivity.

B. Canada

In contrast to the Aadhaar, Canada had a different strategy in adopting a general digital identity scheme. Rather like countries where there is a single centralized government agency that assumes the role of identity authority, Canada opted that no single federal government organization can provide digital identity for all persons within the jurisdiction but there are 14 different "roots of identity" [3] through which persons can establish who they are. In the paper "Building Trust: Lessons from Canada's Approach to digital identity", the Canadian approach is described as being bold in terms of making friendly overtures to technological implementations of the latest development in solutions—self-sovereign identity, where there might not be a need for Web PKI but a more decentralized infrastructure. While self-sovereign identity has not been taken seriously by many other governments, two standards are being considered components: Verifiable Credentials and Decentralized Identifiers. The scheme for the national Canadian ID is seen as an improvement for the

TABLE I: Overview of the ranking countries eID.

Year	Country	Technology	Managing entity	Mistakes made	Mistakes to avoid
2007	Estonia	KSI blockchain	Information System Authority - coordinated with police and border guard	-	-
2010	India	PKI/HSM	UIDAI, an autonomous government agency	-	-
2010	Germany	PKI blockchain		-	-
2013	Peru	PKI blockchain	RENIEC - autonomous public agency	-	-

public and private sectors and has well-defined principles such as No Centralized Authority, Secured Blinded Infrastructure, Decentralized, Secured, and Private Data Architecture, Privacy and Controls and Book Keeping, Audit, and Billing [9]. The development of a modern digital ID system is accelerated by the use case on the financial side, like open banking, with an estimation of a profit of 3 billion euros [32] in its first year. The attempts to create such as system have already been made in the country with the Verified.me application by SecureKey Technologies Inc which is set to expand its use to multiple public/private institutions [11].

C. Germany

Germany had one of the first [39] officially declared eID schemes for eIDAS, following the User-centric model. It is based on the German national identity card and electronic residence permit. Due to the use of Extended Access Control (EAC), each SP requires an authorization certificate and either an own eID server or a corresponding eID service. In order to obtain such an authorization certificate, SPs usually need to apply first, including a substantial service fee. Public bodies are excluded from this rule, since every municipality is required to provide its services online by law. To make things more complicated, every federal state can have its own digital identity system, leading to a rather complex mostly SAML-based federation. For this, multiple projects have been proposed to experiment [50] like project OPTIMOS 2.0 which provides the ecosystem for the mobile eID, while the project Digital Identities tries to optimize the app. The mobile app AusweisApp2 can be used as long as the smartphone is equipped with near-field communication (NFC) capabilities and runs on either iOS or Android [42]. In the end, after the experiments, German citizens are able to securely store their national ID on a SIM card in their smartphone and the mobile eID could be used to open a bank account, use eGovernment services and other online services. As such, the need for a card reader or a physical card to identify and authenticate citizens online was removed [1]. However, one problem identified within the country was the very low usage of the eID in transactions and interactions even with a high adoption rate of the population [33] some inhibitors being other identification and authentication methods, and involvement of the private sector. One important use will no longer be possible with the new ID card because the holder can no longer be forced to deposit the ID card or give up custody of it. With the new card entailing both the electronic proof of identity and a private cryptographic key for the generation of qualified electronic signatures, the sole ownership of it represents indispensable security. Thus, to prevent abuse, "it is no longer allowed to demand the ID card to be handed over at the front desk or gate of a building or used as a deposit when borrowing an object" [28].

D. Estonia

The Estonian digital identity scheme is one of the only ones that distance itself from the original PKI infrastructure. It uses the Keyless Signatures Infrastructure (KSI) a globally distributed system for providing time-stamping and server-supported digital signature services that have a different architecture from PKI, incorporating an Aggregation Network, Core Cluster and Gateway [14]. Started as a project for electronic access to healthcare and residency systems, the case expanded to a full digital ID infrastructure, with the main reasons for implementing the Digital Signature Act and provide means for digital signing for Estonian residents [35]. Since its introduction, the Estonian eID scheme has been praised ([8], [26]) for its adoption rate within both private and public sectors, but Estonia's digital success is not about other "digital offerings such as digital democracy, citizen engagement, or digitally transforming public services such as the welfare state" [30] and disconnect between technological infrastructure and degree of digital penetration alongside the small size of the population(and of the data) are often overlooked. Also from the policymaker perspective, there are identified challenges related to issues like implementation, (national) legislation, interpretation, compliance and communication. A crucial eIDAS implementation barrier is the lack of the EU common identifier and Estonia's scheme seems to further away even more [34]. Estonia is one of the first countries that enabled E-Voting with the help of the digital ID [22] with data stored in a decentralized fashion in over 360 databases in which all information from local hosts is linked through a specific infrastructure, X-Road, that, however, presents a single point of failure for the whole eGov data transfer to stop.

E. Peru

The National Electronic ID Card (DNIe) of Peru, issued by the National Registry of Identification and Civil Status (RENIEC), was recognized as the top ID card in Latin America at the 2015 High Security Printing Latin American Conference held in Lima. RENIEC, functioning autonomously and responsible for civil registration, identification, and digital signatures, has distributed 30 million eIDs, covering nearly the entire population of the country. The DNIe grants Peruvian citizens a digital identity that can be verified both physically and virtually. It incorporates two digital certificates, enabling the cardholder to electronically sign documents with the same legal weight as a handwritten signature. Peru's eID adheres to

the ISO/IEC-7816 standard, and its biometrics system aligns with ISO/IEC 19794 [23]. It implements the cryptographic methods and X.509 digital certificates defined by the Public Key Infrastructure (PKI) and comes with its known risks. First introduced in 2013, the specifications are being analyzed for a new form in terms of the card, hardware (subdivided into the antenna, chip, and memory), and software (subdivided into the operating system, applications, middleware, and complements [43]. Similar to the Indian scheme, Peru's digital ID can be used for biometric identification but in this case is not a requirement and not used at large and even though the adoption rate for the population is almost 99% there is still lack of a remote access of the e-ID [21]. In the analysis, there are also presented possible risks for the future of the Peruvian digital car, such as making ID enrollment a prerequisite in areas with low coverage.

V. Conclusion

References

[1] Overview of the german identity card project and lessons learned, 2020.

[2] K Abhijeet. Decrypting aadhaar. 2021.

[3] Sunil Abraham. Building trust: Lessons from canada's approach to digital identity. *ORF Issue Brief No. 367, Observer Research Foundation*, 2020.

[4] Ali M Al-Khouri. Pki in government digital identity management systems. *European Journal of ePractice*, 4(4), 2012.

[5] Gergely Alpár and Bart Jacobs. Towards practical attribute-based identity management: The irma trajectory. In *Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013. Proceedings 3*, pages 1–3. Springer, 2013.

[6] Gergely Alpár and BPF Jacobs. Credential design in attribute-based identity management. 2013.

[7] Gergely Alpár, Fabian Van Den Broek, Brinda Hampiholi, Bart Jacobs, Wouter Lueks, and Sietse Ringers. Irma: practical, decentralized and privacy-friendly identity management using smartphones. In *10th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2017)*, pages 1–2, 2017.

[8] Gary Anthes. Estonia: a model for e-government. *Communications of the ACM*, 58(6):18–20, 2015.

[9] Canadian Bankers Association et al. Canada's digital id future-a federated approach. *Canadian Bankers Association, Tech. Rep*, 2018.

[10] Shweta Banerjee. Aadhaar: Digital inclusion and public services in india. *World Development Report*, pages 81–92, 2016.

[11] Andre Boysen. Decentralized, self-sovereign, consortium: The future of digital identity in canada. *Frontiers in Blockchain*, page 11, 2021.

[12] Stefan Brands. *Rethinking public key infrastructures and digital certificates: building in privacy*. Mit Press, 2000.

[13] Garrison Breckenridge. A brief history of digital identity, June 2018.

[14] Ahto Buldas, Andres Kroonmaa, and Risto Laanoja. Keyless signatures' infrastructure: How to build global distributed hash-trees. In *Nordic Conference on Secure IT Systems*, pages 313–320. Springer, 2013.

[15] Bruce Schneier Carl Ellison. Ten risks of pki: What you're not being told about public key infrastructure. *Computer Security Journal*, 16(1):1–7, 2000.

[16] THE EUROPEAN COMMISSION. Commission recommendation (eu) on a common union toolbox for a coordinated approach towards a european digital identity framework. *Official Journal of the European Union*, June 2021.

[17] Ivar Derksen, Bart Jacobs, Hanna Schraffenberger, and Timen Olthof. *Backup and Recovery of IRMA Credentials*. PhD thesis, Master's thesis, Radboud University Nijmegen, 2019.

[18] Pam Dixon. A failure to "do no harm"–india's aadhaar biometric id program and its inability to protect privacy in relation to measures in europe and the us. *Health and technology*, 7(4):539–567, 2017.

[19] William Echikson. Europe's digital identification opportunity, 2020.

[20] Matthew Henry Fredette. *An implementation of SDSI: the simple distributed security infrastructure*. PhD thesis, Massachusetts Institute of Technology, 1997.

[21] Alan Gelb and Anna Diofasi Metz. *Identification revolution: Can digital ID be harnessed for development?* Brookings Institution Press, 2018.

[22] Miguel Goede. E-estonia: The e-government cases of estonia, singapore, and curaao. *Archives of Business Research*, 7(2), 2019.

[23] Paul A Grassi, Michael E Garcia, and James L Fenton. Draft nist special publication 800-63-3 digital identity guidelines. *World Bank*, 2017.

[24] Eman Hableel, Young-Ji Byon, and Joonsang Beak. Public key infrastructure for uae: A case study. In *Proceedings of the 6th international conference on security of information and networks*, pages 336–340, 2013.

[25] Kjell Hansteen, Jon Ølnes, and Tor Alvik. *Nordic digital identification (eID)*. Nordic Council of Ministers, 2016.

[26] Nathan Heller. Estonia, the digital republic. *The New Yorker*, 18, 2017.

[27] Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[28] Gerrit Hornung and Alexander Roßnagel. An id card for the internet–the new german id card with "electronic proof of identity". *Computer Law & Security Review*, 26(2):151–157, 2010.

[29] Gunther Pernul Javier Lopez, Rolf Oppliger. Why have public key infrastructures failed so far? *Internet Research*, 15(5):544–556, 2005.

[30] Rainer Kattel and Ines Mergel. Estonia's digital transformation: Mission mystique and the hiding hand, 2019.

[31] Dmitry Khovratovich and Jason Law. Sovrin: digital identities in the blockchain era. *Github Commit by jasonalaw October*, 17:38–99, 2017.

[32] Thorsten V Koeppl and Jeremy Kronick. Open banking in canada–the path to implementation. *CD Howe Institute Commentary*, 579, 2020.

[33] Philipp Liesbrock. The giant is lagging behind how the german electronic id fails to reap its potential. Degree project at the master's level, Stockholm University, November 2022.

[34] Silvia Lips, Nitesh Bharosa, and Dirk Draheim. eidas implementation challenges: the case of estonia and the netherlands. In *International conference on electronic governance and open society: challenges in Eurasia*, pages 75–89. Springer, 2020.

[35] Tarvi Martens. Electronic identity management in estonia between market and state governance. *Identity in the Information Society*, 3(1):213–233, 2010.

[36] Andrew Maywah, L. Rivest, and J. Maywah. An implementation of a secure web client using spki/sdsi certificates. 07 2000.

[37] Alexander Morcos. *A java implementation of simple distributed security infrastructure*. PhD thesis, Massachusetts Institute of Technology, 1998.

[38] Jelle C Nauta and Rieks Joosten. Self-sovereign identity: A comparison of irma and sovrin. *Technical Report TNO2019R11011, Tech. Rep*, 2019.

[39] Torsten Noack and Herbert Kubicek. The introduction of online authentication as part of the new electronic national identity card in germany. *Identity in the Information Society*, 3:87–110, 2010.

[40] James Manyika Deepa Mahajan Jacques Bughin Michael McCarthy Owen Sperling Olivia White, Anu Madgavkar. *Digital identification: A key to inclusive growth*. McKinsey Global Institute, April 2019.

[41] Om Pal, Bashir Alam, Vinay Thakur, and Surendra Singh. Key management for blockchain technology. *ICT express*, 7(1):76–80, 2021.

[42] Daniela Pöhn, Michael Grabatin, and Wolfgang Hommel. eid and self-sovereign identity usage: an overview. *Electronics*, 10(22):2811, 2021.

[43] Erik Papa Quiroz, Alvaro Cuno, Edgar Sarmiento, and Ever Cruzado. Requirements for a new peruvian electronic identity card. In *2020 IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pages 1–4. IEEE, 2020.

[44] Ursula Rao and Vijayanka Nair. Aadhaar: governing with biometrics, 2019.

[45] Drummond Reed, Jason Law, and Daniel Hardman. The technical foundations of sovrin. *The Technical Foundations of Sovrin*, 2016.

[46] Ronald Rivest and Butler Lampson. Sdsi – a simple distributed security infrastructure. *See the SDSI web page at http://theory.lcs.mit.edu/ cis/sdsi.html*, 08 1996.

[47] Srijoni Sen. A decade of aadhaar: Lessons in implementing a foundational id system. *ORF Issue Brief No*, 292, 2019.

[48] Digital Welfare State and Human Rights Project. *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID*. Center for Human Rights and Global Justice, June 2022.

[49] Clare Sullivan and Eric Burger. Blockchain, digital identity, e-government. *Business Transformation through Blockchain: Volume II*, pages 233–258, 2019.

[50] Digital Technologies. Showcase programme “secure digital identities”, 2023.

[51] Allan Third, Kevin Quick, M Bachler, and John Domingue. Government services and digital identity. *Knowledge Media Institute of the Open University*, 2018.

[52] Amit Kumar Tyagi, Terrance Frederick Fernandez, and SU Aswathy. Blockchain and aadhaar based electronic voting system. In *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pages 498–504. IEEE, 2020.

[53] Phillip Windley. How sovrin works. *Sovrin Foundation*, pages 1–10, 2016.

[54] Phillip J Windley. Sovrin: An identity metasystem for self-sovereign identity. *Frontiers in Blockchain*, 4:626726, 2021.