Pioneering the Future of Electronic Identity: From Post-Quantum Cryptography to Fiduciary Principles

Frederico Schardong[1], **Ricardo Custódio**[1]

[1]Universidade Federal de Santa Catarina (UFSC)

frederico.schardong@ufsc.br, ricardo.custodio@ufsc.br

Abstract. *Electronic identity (e-ID) underpins online security and privacy, yet faces two threats: the cryptography behind today's protocols will fall to quantum computers, and concentrating identities in a few providers erodes privacy while overburdening users. This thesis advances e-ID on both fronts. It makes OAuth 2.0 and OpenID Connect resistant to the quantum threat under realistic networks, and charts a more private, usable path through a rigorous taxonomy of self-sovereign identity, tools to search and compare identity models, and the Fiduciary Identity model, which delegates decisions to accountable, auditable fiduciaries. Several results reached national scale: this work's technology signs every electronic birth, marriage, and death certificate issued in Brazil.*

Resumo. *A identidade eletrônica (e-ID) sustenta a segurança e a privacidade, mas enfrenta duas ameaças: a criptografia dos protocolos atuais cairá diante de computadores quânticos, e concentrá-la em poucos provedores corrói a privacidade e sobrecarrega os usuários. Esta tese avança a e-ID nas duas frentes. Torna o OAuth 2.0 e o OpenID Connect resistentes à ameaça quântica, e traça um caminho mais privado e usável com uma taxonomia de identidade autossoberana, ferramentas para buscar e comparar modelos, e o modelo de Identidade Fiduciária, que delega decisões a fiduciários auditáveis. Vários resultados alcançaram escala nacional: a tecnologia deste trabalho assina toda certidão eletrônica de nascimento, casamento e óbito do Brasil.*

1. Introduction

Proving that individuals are who they claim to be is fundamental to human interaction, online as much as in the physical world [ISO Central Secretary 2019]. Digitally, this proof takes the form of an *electronic identity* (e-ID): a collection of attributes through which a person is identified and authenticated. Corporations such as Google and Meta act as *identity providers* (IdPs) for billions of users on behalf of countless *service providers* (SPs) [Allen 2016], primarily through OAuth 2.0 [Hardt 2012] and OpenID Connect (OIDC) [Sakimura et al. 2014], the *de facto* standards of identity and access management (IAM).

This arrangement is pressured from two directions. First, the cryptography underpinning OAuth 2.0 and OIDC, together with the Transport Layer Security (TLS) and JSON Web Token (JWT) layers beneath them, is vulnerable to cryptographically relevant quantum computers [Shor 1994]. No such computer is known to exist, yet migration to post-quantum cryptography (PQC) [NIST 2016] is urgent rather than hypothetical: traffic intercepted today can be decrypted later, most experts surveyed for

the Quantum Threat Timeline put the odds of such a machine within 15 years above 5% [Mosca and Piani 2020], and NIST closed the standardization of the first PQC schemes in 2024 [NIST 2024]. Second, concentrating the e-IDs of billions of users in a handful of IdPs raises mounting privacy concerns, motivating the emergent Self-Sovereign Identity (SSI) paradigm, in which users, rather than intermediaries, control their own identities [Allen 2016].

The IAM literature had not kept pace with either pressure. On the post-quantum front, no practical evaluation of OAuth 2.0 or OIDC under realistic network conditions existed. On the SSI front, secondary studies either lacked methodological rigor or wrongly equated SSI with blockchain. The most consequential open problem, however, was usability: SSI shifts the burden of managing keys and credentials onto laypeople, frustrating the very users it intends to empower.

This thesis confronts both fronts. Its central claim is that *it is possible to secure today's identity protocols against the quantum threat while charting a more private and usable future for e-ID, grounded in a new model inspired by fiduciary legal principles*. To substantiate it, we make five contributions: (i) a post-quantum redesign and evaluation of OAuth 2.0 and OIDC; (ii) a rigorous systematic review, mapping, and taxonomy of SSI; (iii) a natural-language tool for matching identity metadata on blockchain; (iv) the Role-Artifact-Function framework for comparing e-ID models; and (v) the Fiduciary Identity model. The doctoral work also yielded a collaborative result outside the thesis that reached national-scale production: a one-time-certificate digital-signature technology, patented as BR102022012874 [Schardong et al. 2022b], that today underpins every electronic birth, marriage, and death certificate issued in Brazil, and the signing service RNP operates for the Brazilian academic community [Perottoni et al. 2023],[1] whose adoption UFRGS and UFCSPA report themselves [Soares et al. 2026, Moreira et al. 2026].

This article condenses the doctoral thesis, defended at the Federal University of Santa Catarina (UFSC) in July 2024 and available at `https://repositorio.ufsc.br/handle/123456789/262831`. Section 2 states the objectives; Section 3 details the five contributions and their results; Section 4 summarizes the scientific production; Section 5 reports the awards and real-world impact; and Section 6 concludes.

2. Objectives

The overarching goal is to advance e-ID management on two complementary fronts: hardening the protocols that secure identity today and conceiving a more private and usable model for identity tomorrow. We pursue it through two primary objectives:

- **Enhancement of authentication and authorization with post-quantum cryptography**: to design and empirically validate quantum-resistant variants of OAuth 2.0 and OIDC, and of their TLS and JWT layers, under realistic networks.
- **Introduction of the Fiduciary Identity model**: to define a new e-ID model that, inspired by fiduciary legal principles, minimizes the user's burden of managing credentials by automating consent and delegating decision-making to accountable entities.

[1] `https://cdd.icpedu.rnp.br/`

and three secondary ones: to characterize the state of SSI with methodological rigor, yielding a taxonomy and the open challenges that motivate the rest; to propose and evaluate a mechanism that matches identity metadata on blockchain more accurately when queries approach natural language; and to develop the Role-Artifact-Function framework for formally examining and contrasting e-ID models and the ontological structures underlying them.

3. Contributions and Results

3.1. Post-Quantum OAuth 2.0 and OIDC *primary*

OAuth 2.0 and OIDC, with the TLS and JWT layers they rely on, depend on classical public-key cryptography that a quantum computer would break. Chapter 3 addresses this in three steps. A reproducible systematic review found no prior practical, network-aware evaluation of post-quantum OAuth 2.0 or OIDC. We then proposed modifications that make the protocols quantum-safe, replacing the vulnerable primitives in their JWT and TLS foundations and doubling the symmetric parameters where Grover's algorithm applies. Finally, we implemented a post-quantum OIDC stack and ran each configuration a thousand times on Amazon EC2 instances across five locations.

Table 1 reports the bytes on the wire and the end-to-end time of every configuration. We compared ECDSA p256 and RSA 2048 against Dilithium, Falcon, and SPHINCS+, with Kyber512 for key exchange, the schemes NIST later standardized as ML-DSA, FN-DSA, SLH-DSA, and ML-KEM [NIST 2024]. Post-quantum algorithms match ECDSA at 30 ms, but their larger keys and signatures trigger extra TCP round trips as latency grows: at 325 ms the lattice configurations cost about a third more time, and SPHINCS+ 256 more than doubles it. Notably, the TLS handshake takes half of the total OIDC time under lattice settings and two thirds under SPHINCS+, against a third under classical cryptography, which identifies the handshake, rather than the tokens, as the primary target for optimization. The contribution is not a new primitive but the protocol-level redesign and the first network-aware measurement of its cost. The implementation and experimental setup were released under an open-source license.[2] This work was published at CANS 2022 [Schardong et al. 2022a] and was later extended by our group to the automated issuance of post-quantum certificates [Giron et al. 2024].

3.2. Systematic Review, Mapping and Taxonomy of SSI *secondary*

SSI had attracted attention, yet secondary studies either lacked methodological rigor or wrongly equated SSI with blockchain. We conducted the first rigorous systematic literature review of SSI, with a systematic mapping relating researchers and works,[3] as reported in Chapter 4. From it we derived a novel taxonomy of the conceptual and practical efforts in the field and identified the open challenges that shaped the rest of the thesis, among them the usability burden that SSI places on laypeople. Published in *Sensors* [Schardong and Custódio 2022], this review is the most cited contribution of the thesis.

[2] `https://github.com/fredericoschardong/post-quantum-oidc-oauth2`

[3] The per-stage screening and extraction results of the review are available as a supplementary spreadsheet: `https://docs.google.com/spreadsheets/d/1FzUJRqe3WUhtsNYV6PyMZO8F14iQO-DXnBHR9xUsaiw`.

Table 1. Cost of each configuration, as the mean of a thousand runs. TLS covers the 22 handshakes of the scenario; OIDC covers the whole exchange.

KEX / signature	TLS (kB)	OIDC (MB)	30 ms	325 ms	TLS time share
ECDHE / ECDSA p256	48	1.02	2.6 s	16 s	33%
ECDHE / RSA 2048	87	1.02	2.5 s	16 s	33%
Kyber512 / Falcon-512	209	1.03	2.5 s	21 s	50%
Kyber512 / Falcon-1024	350	1.03	2.5 s	21 s	50%
Kyber512 / Dilithium 2	471	1.04	2.5 s	21 s	50%
Kyber512 / Dilithium 3	628	1.06	2.5 s	21 s	50%
Kyber512 / Dilithium 5	842	1.07	2.6 s	21 s	50%
Kyber512 / SPHINCS+ 128	2322	1.86	4.8 s	32 s	62%
Kyber512 / SPHINCS+ 192	4777	2.18	4.9 s	37 s	68%
Kyber512 / SPHINCS+ 256	7015	2.31	5.1 s	38 s	68%

3.3. Matching Identity Metadata on Blockchain *secondary*

Blockchain-based SSI implementations register credential schemas on the ledger, but locating the right one is difficult when a query does not match the registered terms verbatim. Chapter 5 proposes a tool that applies natural-language processing, through pretrained word vectors, to match queries against schemas on the Sovrin ledger by semantic similarity rather than exact wording. Our review identified three competing tools, all based on full-text search: von-x and Indyscan, which we evaluated, and that of Lux et al. [Lux et al. 2019], which is not publicly available. Over three queries against the 149 schemas of the Sovrin live ledger, our tool reaches a mean weighted f-score of 0.70, against 0.66 for von-x and 0.59 for Indyscan. The advantage lies in queries approaching natural language: for *first name*, whose correct schemas often omit the words *first* and *name*, it scores 0.76 against 0.66 and 0.48; for *company job*, on which both competitors matched nothing, it scores 0.55. We also report where it is weaker, such as the single-word query *address*. The tool and its experiments are publicly available,[4] and the work appeared at the BPM workshops [Schardong et al. 2021].

3.4. The Role-Artifact-Function Framework *secondary*

The literature lacked a formal instrument for describing and comparing e-ID models. Chapter 6 introduces the Role-Artifact-Function (RAF) framework, a meta-metamodel and a metamodel that express an e-ID model as a set of roles, computational artifacts, and functions. We instantiated it for the major e-ID models and proved by construction that each instantiation satisfies real-world properties, exposing the ontological structures underlying these models and where they diverge. RAF is the instrument with which we positioned the Fiduciary Identity model against its predecessors. It was published at the International Conference on Conceptual Modeling [Schardong and Custódio 2024b].

3.5. The Fiduciary Identity Model *primary*

The usability burden surfaced by our review is the most consequential challenge: SSI empowers users, but asks them to manage keys and credentials and to judge every request for their private data. Chapter 7 answers it with the Fiduciary Identity model, the capstone contribution. Drawing on the legal notion of the information fiduciary [Balkin 2015], it

[4] `https://github.com/fredericoschardong/sovrin-schema-matching`

interposes a *fiduciary*: an entity the user chooses and may replace at will, bound by duties of loyalty and care to act in the user's interest, which automates consent and relieves users of low-level credential management.

Introducing an actor invites the objection that it reinstates the intermediary SSI set out to remove. Three commitments separate the two. First, the fiduciary is independent of IdPs and SPs and is chosen by the user, who may hold several and revoke consent at any time, so it does not inherit the position of an IdP users cannot refuse. Second, consent is architectural rather than a per-request dialog: the user states policies *a priori*, and the model obliges the fiduciary to retain evidence of every decision, which the user retrieves through an audit function that is part of the formal specification. Third, the verifier's program may execute inside the fiduciary's computing environment, so a verifier can learn the result of a predicate over the user's attributes without receiving the attributes. What the fiduciary gains over an IdP is not more data, but accountability for how it is used.

We are explicit about what the thesis does not deliver. The model is specified formally and compared analytically against the centralized, outsourced-IdP, and SSI models, but has no reference implementation, no controlled study of the claimed reduction in cognitive load, and no threat model covering compromise, collusion with verifiers, or recovery from an adversarial fiduciary; Section 6 states how we are addressing them. It appeared at the ACM Symposium on Applied Computing [Schardong and Custódio 2024a].

4. Scientific Production

Table 2 lists the publications that directly support the thesis, separating core results (first-authored and mapped to a thesis chapter) from collaborations.

Table 2. Publications supporting the thesis, with venue, CAPES Qualis stratum, and Google Scholar citations.

Ref.	Venue	Year	Qualis	Cit.	Role	Type
[Schardong and Custódio 2022]	Sensors	2022	A2	175	C	Survey
[Schardong et al. 2021]	BPM (SPBP)	2021	–	15	C	Method
[Schardong et al. 2022a]	CANS	2022	A4	11	C	Method
[Schardong and Custódio 2024b]	ER	2024	A3	0	C	Theory
[Schardong and Custódio 2024a]	ACM SAC	2024	A1	1	C	Theory
[Giron et al. 2024]	ACNS	2024	A2	10	Co	Method
[Giron et al. 2022]	SBSeg (SF)	2022	–	4	Co	Tool
[Vale et al. 2022]	CBMS	2022	A2	3	Co	Method
[Silva et al. 2023]	SBSeg (WGID)	2023	–	4	Co	Method
[Perottoni et al. 2023]	SBSeg (WGID)	2023	–	4	Co	Tool

Role: C (core), Co (collaboration). Qualis strata from CAPES (Eventos 2025; *Sensors* from Periódicos); "–" marks workshop or tool tracks with no separate stratum; citations from Google Scholar, June 2026. SPBP: Security and Privacy-enhanced BPM; SF: Salão de Ferramentas; WGID: Workshop em Gestão de Identidades Digitais.

The five core publications appeared in established venues, the strongest being the ACM Symposium on Applied Computing (Qualis A1) and the journal *Sensors* (A2). Together they have gathered more than 220 citations, 175 of them for the systematic review

of SSI. The doctoral work also contributed to a patent on one-time-certificate digital signatures (BR102022012874 [Schardong et al. 2022b]), co-invented with colleagues, whose national-scale deployment we discuss in Section 5, and the post-quantum line was later extended by the research group [Giron et al. 2024], evidence of its influence beyond the thesis.

The doctoral period also involved supervising three undergraduate final projects, three co-advised master's theses, and fourteen mentored undergraduates. One of these collaborations, on the electronic authentication of health professionals during COVID-19, led to a published study on touchless authentication factors [Vale et al. 2022].

5. Awards and Real-World Impact

Two international awards recognized the work conducted during this doctorate. In 2022, the author received the inaugural Kim Cameron Award from the OpenID Foundation, granted to one of four early-career researchers working on identity standards that prioritize security, interoperability, and privacy.[5] In 2024, the author was among the three recipients of the first Vittorio Bertocci Award from the Digital Identity Advancement Foundation.[6] Both were decided by independent international juries, providing external validation of the thesis's relevance to the identity community.

Several results moved from research into production. The patented one-time-certificate digital-signature technology [Schardong et al. 2022b] now underpins two national-scale systems: in Brazil it signs the electronic birth, marriage, and death certificates issued by the Civil Registry[7], and it powers the digital signer RNP operates across an academic federation of more than one million users [Perottoni et al. 2023]. The same technology reached Mozambique, where, with the national agency INTIC, we built an e-ID and public-key infrastructure used daily to sign the country's official journal[8].

We also proposed and led the development of a national e-ID issued by Brazil's Civil Registry [Silva et al. 2023], the authority that issues birth certificates. Anchored in the judiciary branch, it curbs executive-branch surveillance, consolidates data fragmented across agencies, and is reachable by service providers through OIDC and OAuth 2.0.

6. Final Remarks

This thesis advanced electronic identity on two fronts. It hardened the protocols that secure identity today, making OAuth 2.0 and OIDC resistant to the quantum threat, and it charted a more private and usable path for identity tomorrow, through a rigorous study of SSI, a tool that makes blockchain-based identity searchable, the Role-Artifact-Function framework, and the Fiduciary Identity model. Several are already in national-scale production.

The work continues. The Civil Registry e-ID is being broadened to reach more service providers, and the digital-signature infrastructure that already serves the Civil

[5] https://openid.net/2022-openid-foundation-kim-cameron-award-recipients-announced/

[6] https://diaf.org/news/celebrating-excellence-meet-the-first-vittorio-bertocci-award-winners/

[7] https://onrcpn.org.br/icp-idrc/

[8] https://assinadoravancado.gov.mz/

Registry, RNP, and Mozambique is reaching further institutions. The most ambitious line ahead, and our current focus, is to carry the Fiduciary Identity model beyond its formal specification. Three steps are required, in order: a reference implementation of the fiduciary, extending an existing SSI wallet; a threat model stating the fiduciary's capabilities and goals and analysing compromise, collusion with verifiers, and recovery, which is what an accountability-based model must withstand to be trusted; and a controlled study of cognitive load against an SSI wallet on the same tasks, the only way to settle whether the usability gain we argue for is real.

The thesis is at `https://repositorio.ufsc.br/handle/123456789/262831` and the first author's publications at `https://frederico.phd`.

Acknowledgments

The author thanks IFRS for the leave that made this doctorate possible, and RNP, the Arpen-Brasil and ON-RCPN civil-registry organizations, and Mozambique's INTIC for supporting the deployments reported here. Generative artificial-intelligence tools (Anthropic's Claude) assisted in drafting this article; the authors reviewed all content and take full responsibility for it.

References

Allen, C. (2016). The path to self-sovereign identity.

Balkin, J. M. (2015). Information fiduciaries and the first amendment. *U.C. Davis Law Review*, 49:1183. https://dx.doi.org/20.500.13051/4692.

Giron, A. A., Schardong, F., and Custódio, R. (2022). TLS 1.3 Handshake Analyzer. In *Extended Proceedings of XXII SBSeg*, pages 63–70. SBC.

Giron, A. A., Schardong, F., Perin, L. P., Custódio, R., Valle, V., and Mateu, V. (2024). Automated issuance of post-quantum certificates: A new challenge. In *Applied Cryptography and Network Security*, pages 3–23. Springer Nature Switzerland.

Hardt, D. (2012). The OAuth 2.0 Authorization Framework. https://dx.doi.org/10.17487/RFC6749.

ISO Central Secretary (2019). IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts. Standard, International Organization for Standardization, Geneva, CH. `https://www.iso.org/standard/77582.html`.

Lux, Z. A., Beierle, F., Zickau, S., and Göndör, S. (2019). Full-text search for verifiable credential metadata on distributed ledgers. In *Int. Conf. on Internet of Things: Systems, Management and Security*, pages 519–528. IEEE.

Moreira, D., Lima, C. L., Fallavena, A. B., Araujo, R. d. S., da Silva, C. A., and Rocha, L. (2026). Modernização e integridade na gestão acadêmica: a implantação de assinaturas eletrônicas da icpedu para planos de ensino na ufcspa. In *Anais do XVIII WTICIFES*.

Mosca, M. and Piani, M. (2020). Quantum threat timeline report 2020. Global Risk Institute. `https://globalriskinstitute.org/publications/`.

NIST (2016). Post-quantum cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

NIST (2024). Module-lattice-based key-encapsulation mechanism, digital signature, and stateless hash-based digital signature standards. FIPS 203, 204 and 205. https://csrc.nist.gov/pubs/fips/203/final.

Perottoni, E. D., Costa, B. P., Müller, F. L., dos Santos Camargo, V., Schardong, F., Silvano, W., Mayr, L., Custódio, R., Rocha, L., Lyra, C., Matushima, R., and Rieckmann, N. (2023). Menos certificação digital e mais identidade eletrônica: Icpedu e cafe em um assinador digital inclusivo. In *Anais Estendidos do XXIII SBSeg*, pages 93–96. SBC.

Sakimura, N., Bradley, J., Jones, M., De Medeiros, B., and Mortimore, C. (2014). Openid connect core 1.0. Technical report, The OpenID Foundation. https://openid.net/specs/openid-connect-core-1_0.html.

Schardong, F. and Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors*, 22(15):5641.

Schardong, F. and Custódio, R. (2024a). From self-sovereign identity to fiduciary identity: A journey towards greater user privacy and usability. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, pages 687–694. ACM.

Schardong, F. and Custódio, R. (2024b). The role-artifact-function framework for understanding digital identity models. In *Conceptual Modeling*, number 1, pages 377–395. Springer-Verlag.

Schardong, F., Custódio, R., Pioli, L., and Meyer, J. (2021). Matching metadata on blockchain for self-sovereign identity. In *Business Process Management Workshops*, pages 421–433. Springer International Publishing.

Schardong, F., Giron, A., Müller, F., and Custódio, R. (2022a). Post-quantum electronic identity: Adapting openid connect and oauth 2.0 to the post-quantum era. In *Cryptology and Network Security*, pages 371–390. Springer International Publishing.

Schardong, F., Mayr, L., and Custódio, R. (2022b). Processos de verificação e assinatura digital de documentos eletrônicos baseado em identidade eletrônica, certificado digital de uso único e blockchain.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE.

Silva, B., Schardong, F., Junior, L. C. V., and Custódio, R. (2023). Identificaçao eletrônica do registro civil do brasil. In *Anais Estendidos do XXIII SBSeg*, pages 89–92. SBC.

Soares, D. D. S., da Silva, R. P., das Neves, R. M., Vieira, R., Ribeiro, R. d. Q., and Rocha, L. (2026). Assinador rnp: experiência de uso no sistema de documentos eletrônicos da ufrgs. In *Anais do XVIII WTICIFES*.

Vale, C. A., Schardong, F., Barros, M., and Custódio, R. (2022). Touchless authentication for health professionals: Analyzing the risks and proposing alternatives to dirty interfaces. In *IEEE 35th Int. Symp. on Computer-Based Medical Systems*, pages 459–464. IEEE.