SpruceID

Provably Forgotten Signatures: Adding Privacy to Digital Identity

Presentation for NIST Workshop for Privacy-Enhancing Cryptography 2024

September 26th, 2024

Link to Blog Post:
https://blog.spruceid.com/provably-forgotten-signatures-adding-privacy-to-digital-identity/

Hi, I'm Wayne Chang.

Founder and CEO, SpruceID

- Background in engineering and product management.
- Advocate for utility, security, privacy, and interoperability.
- Working with public sector and institutional customers.
- Former Co-Chair of W3C CCG.
- **Implementer, not cryptographer.**

Why should you care?

- It's happening at rapid rate now. 11+ states.
- It's aligned with several ongoing NIST efforts.
- This is the mDL position supported by ACLU, EFF, and EPIC in 2021:

> **Unlinkable presentations**
>
> Standards and technologies should be designed so that the Issuer (or any of their agents or contractors) cannot know where or to whom a Holder is presenting their ID, and so that Verifiers cannot conspire with each other or with Issuers to compile records of presentations.

Intersection with Ongoing NIST Efforts: National Cybersecurity Center of Excellence (NCCoE)

The NCCoE track for Digital Identities (https://www.nccoe.nist.gov/projects/digital-identities-mdl) strongly intersects with technologies we reference in our work.

From the NCCoE website:

Our first use case will address ‘Know Your Customer/Customer Identification Program Onboarding and Access’ which will demonstrate the use of an **mDL and/or Verifiable Credentials (VC)** for establishing and accessing an online financial account.

Intersection with Ongoing NIST Efforts: SP 800-63-4

NIST SP 800-63-4 (2nd Public Draft published on Aug 21st, 2024) refers to verifiable credentials and mobile driver's licenses as being able to serve as superior evidence for identity verification use cases:

Under 2.5.1. Identity Verification Methods:

Authentication and Federation Protocols. The individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g., **verifiable credentials**) through the use of authentication or federation protocols. This may be done in person, through presentation of the credential to a device or reader, but can also be done during remote identity proofing sessions.

Under A.3. Superior Evidence Examples:

Mobile Driver's License (MDL)	State Issuance processes, AAMVA guidance, and Real ID Act	Validation of Mobile Security Object, revocation check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B.
Digital Permanent Resident Card (Verifiable Credential)	DHS issuance and eligibility process	Validation of stored verifiable credential, revocation check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B.
European Digital Identity Wallet (EUDI Wallet) Personal Identification (PID) Element	EC defined identity verification and issuance process; qualified issuer certified	Validation of stored verifiable credential or Mobile Security Object, revocation check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B.

Intersection with Ongoing NIST Efforts:
NIST AI 100-5: A Plan for Global Engagement on AI Standards

Especially:

Transparency among AI actors about system and data characteristics.

System deployers and users often need information from designers and developers about training data, performance testing results, areas of intended or unintended use, **AI systems' supply chains (the underlying software, data, and model components)**, and the like.

…

A Risk: Data Linkability via Collusion

Linkability can arise when traceable digital signatures or identifiers are used repeatedly.

This can allow different parties to correlate interactions back to the same individual, which can create surveillance potential across societies.

Use Case: Using a digital credential to access an age-restricted website

Why This Matters Now

The train has left the station.

ANDROID / GOOGLE / TECH

Google Wallet will let you make a digital ID from a US passport

TRAVEL NEWS TSA Add Topic +

TSA digital ID checkpoints: Travelers from these 11 states can use their Apple Wallet

Zach Wichter
USA TODAY

Published 11:57 a.m. ET Sept. 10, 2024 | **Updated 12:18 p.m. ET Sept. 10, 2024**

TECH

NIST takes next step in studying feasibility of mobile driver's licenses

Home / India / 99.9% adults in India have Aadhaar number and 'use it at least once a month', s...

99.9% adults in India have Aadhaar number and 'use it at least once a month', says UIDAI

Government & Policy

The EU Digital Identity Wallet: Everything you need to know about the EU's plans for a universal digital identity system

Natasha Lomas / 10:00 AM PDT • June 23, 2024 Comment

Why This Matters Now

Cryptographers' Feedback on the EU Digital Identity's ARF #200

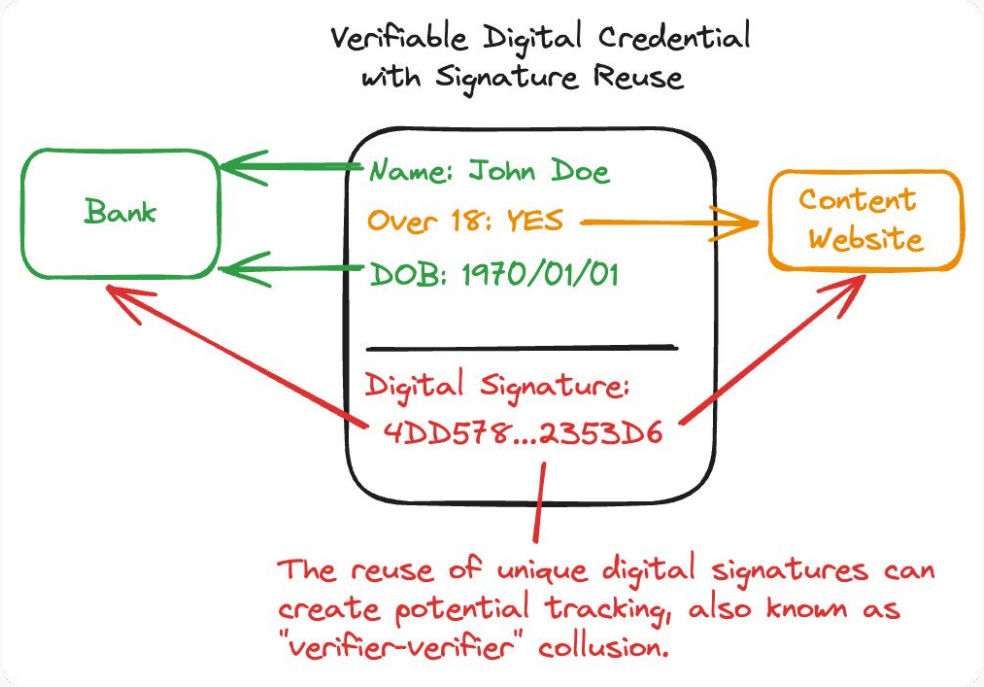
Closed **alysyans** opened this issue on Jun 19 · 41 comments

alysyans commented on Jun 19

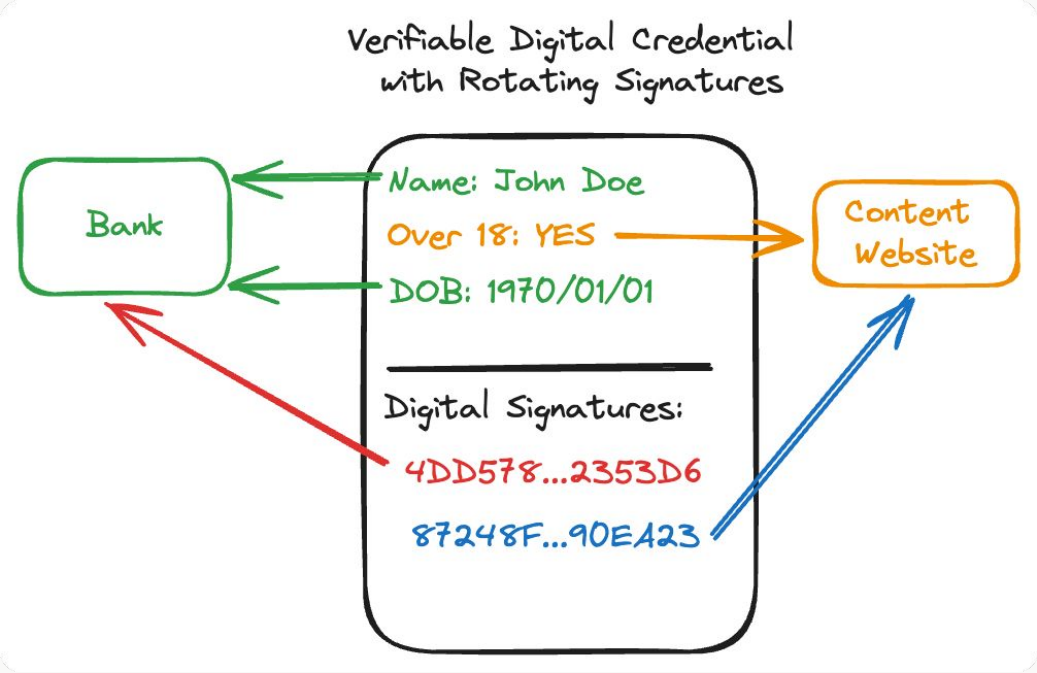
The EUDI Wallet Team of the European Commission invited subject-matter experts (i.e. cryptographers) to participate in a Webex meeting on June 5th or 6th, 2024, in which the team presented their current design of the EUDIW (ARF version 1.4.0), and requested feedback. They specifically requested feedback concerning attestations and zero-knowledge proofs. Our feedback is in this document: cryptographers-feedback.pdf

The attached document was co-authored by and thus represents the **consensus opinion** of the following cryptographers who were present on one of the two calls:

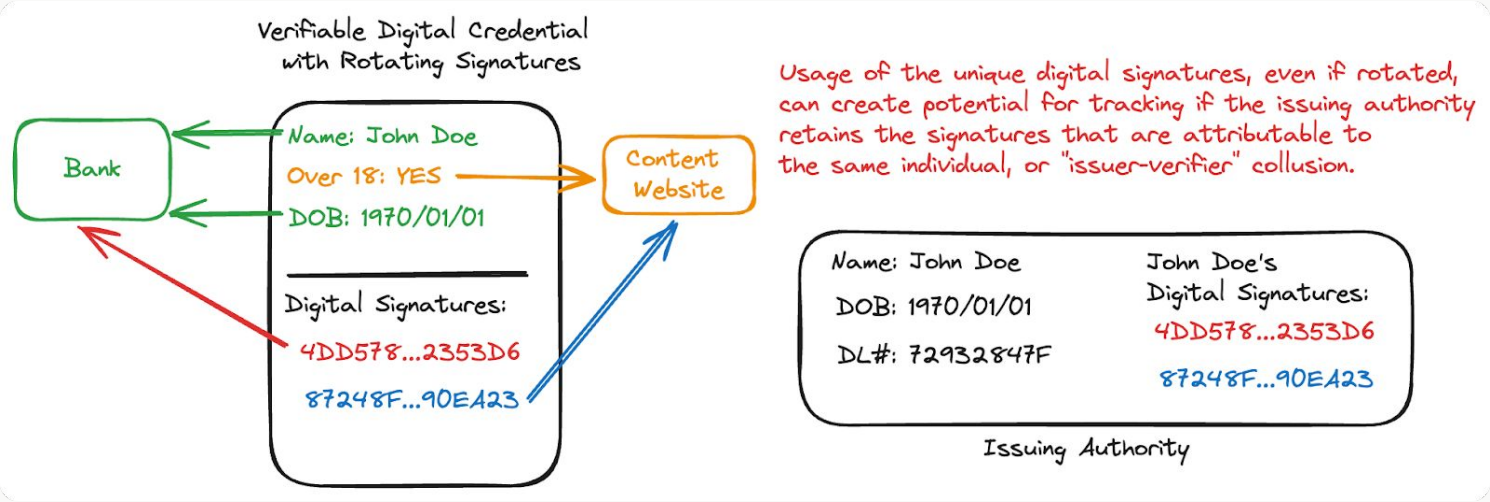
Verifier-Verifier Collusion



Cycling Signatures to Prevent Verifier-Verifier Collusion



Issuer-Verifier Collusion

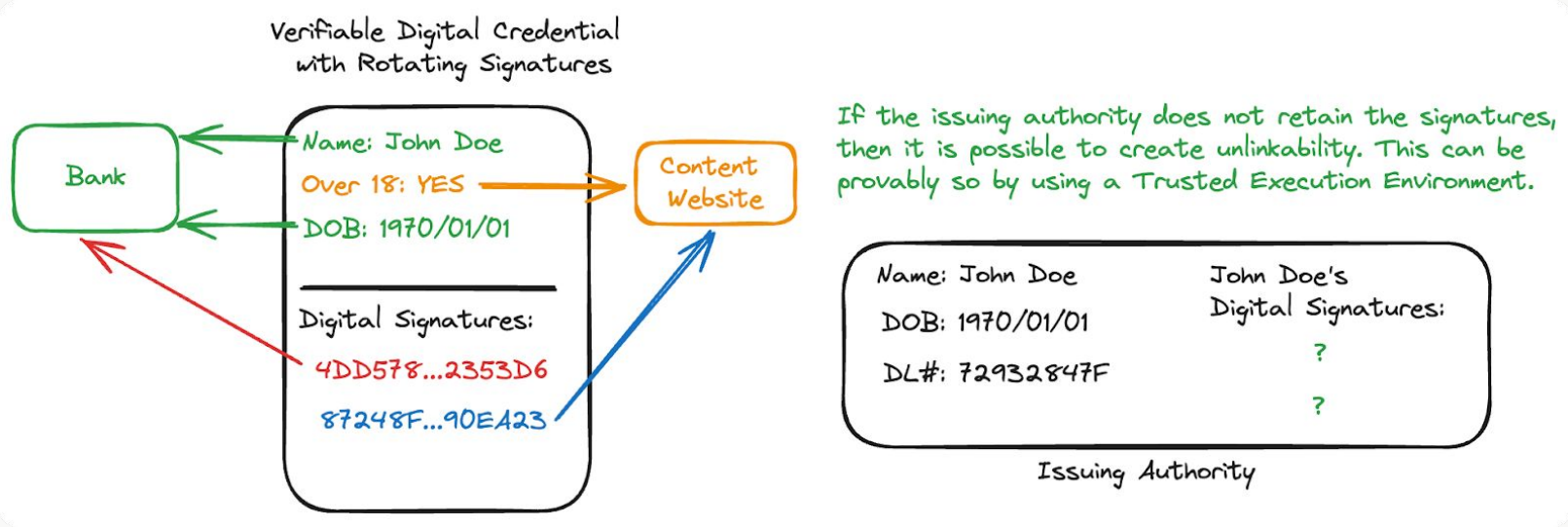


Approaches Using Zero-Knowledge Proofs

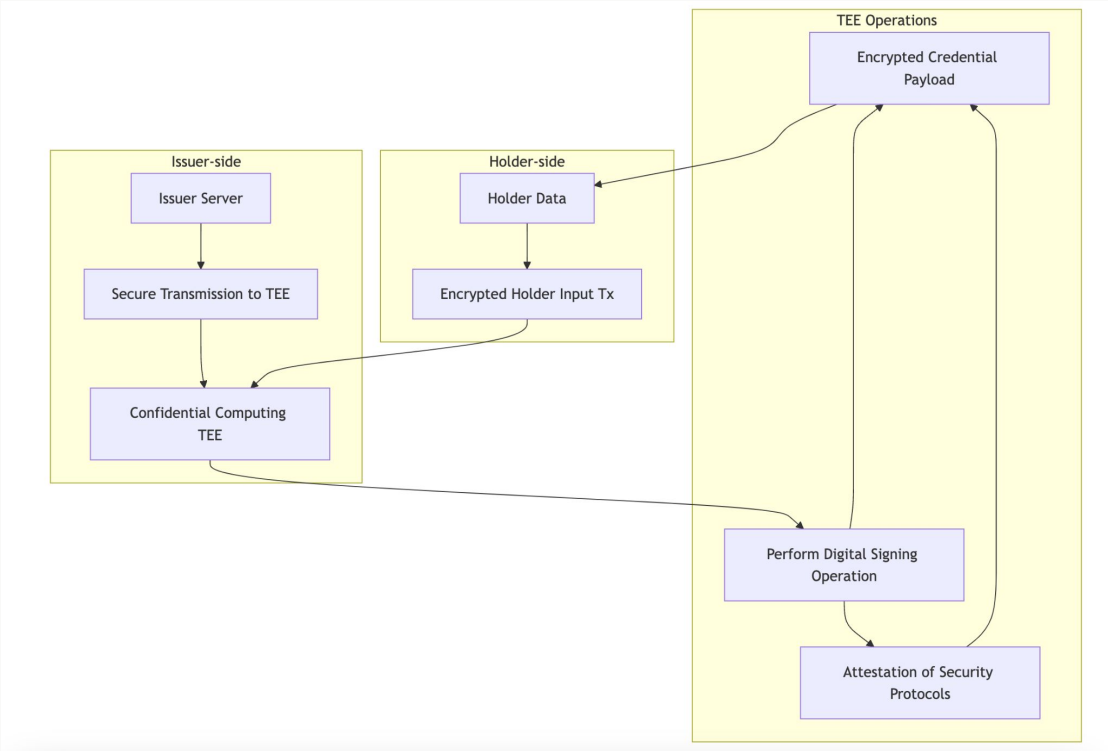
Integrating cryptographic approaches, such as BBS signatures, AnonCreds, U-Prove, zk-SNARKs, and zk-STARKs pose challenges when integrating into **production systems with rigorous security standards.**

- Compliance hurdles for adopting newer cryptographic algorithms, such as the BLS 12-381 Curve used in BBS and many zk-SNARK implementations.
- Requirements for high assurance systems
- Growing industry shift away from RSA signatures

A Pragmatic Approach for Today: Provably Forgotten Signatures



How It Works



1. Unique values, including digital signatures, are processed in the TEE of confidential computing on the issuer's server-side infrastructure.
2. Issuer-provided data required for credential issuance undergoes secure transmission to the TEE.
3. Sensitive user inputs, such as unique device keys, are encrypted before being transmitted to the TEE.
4. Within the TEE, assembled values from both the issuer and user are used to perform digital signing operations.
5. Resulting digital credential payload is encrypted using the user's device key and securely stored within the device's hardware.
6. Upon completion, an attestation accompanies the credential, verifying that the entire process adhered to stringent security protocols.

The Benefits

Protection Against Collusion
By employing confidential computing and strict segregation of cryptographic operations within a TEE, the risk of verifier-verifier and issuer-verifier collusion is mitigated.

Privacy and Security
User data remains safeguarded throughout the credential issuance process, with sensitive information encrypted and managed securely within trusted hardware environments.

Compliance and Implementation
Leveraging existing hardware security mechanisms supports seamless integration into high-assurance environments, aligning with stringent regulatory and security requirements.

The Considerations

1. **TEEs as Part of a Defense Strategy:** TEEs are not foolproof and have been compromised before; they work best as part of a layered defense-in-depth strategy with strict environmental controls by the credential issuer (see sgx.fail and TrustZone CVEs for examples).
2. **Shift in Trust Model:** The trust model shifts from the issuing authority to the hardware (TEE manufacturer), offering more isolation and security in controlled environments.
3. **Retention Periods and Auditability:** Digital credential guidelines may require retention periods. TEEs can enforce these with deterministic regeneration or prioritize unlinkability over auditability, depending on implementation choices.
4. **Key Compromise Detection:** Using cryptographic structures allows verification of issued signatures without linking to source data, while encryption ensures only authorized access to signature contents.

The Road Ahead

The future of digital identity lies in zero-knowledge proofs (ZKPs) that support post-quantum cryptography, enabling enhanced privacy and selective disclosure. To get there we must:

- Upgrade existing systems with new privacy guarantees
- Keep in line with current protocols and requirements for cryptographic modules
- Leave the door open for future zero-knowledge-based systems
- Show policymakers the art of the possible with an example of a pragmatic implementation
- Collaborate with industries, including standards bodies (IETF, NIST, W3C, ISO)

Let's Collaborate

- Enumerated requirements for TEEs around scalability, costs, and complexity to implement this approach, so that commercial products can be considered against those requirements.
- A formal paper with rigorous evaluation of the security model using data flows, correctness proofs, protocol fuzzers, and formal analysis.
- Prototyping using real-world credential formats, such as ISO/IEC 18013-5/23220-* mdocs, W3C Verifiable Credentials, IMS OpenBadges, or SD-JWTs.
- Evaluation of how this approach meets requirements for post-quantum cryptography.
- Drafting concise policy language that can be incorporated into model legislation or agency rulemaking to create the requirement for unlinkability where deemed appropriate.

SpruceID

Wayne Chang

Founder and CEO, SpruceID

wayne@spruceid.com

www.spruceid.com

https://www.linkedin.com/in/waynebuilds

Thank you.