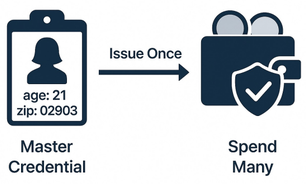
Smart Tokens: Attribute-Based Anonymous Tokens with Hidden Metadata Bit

Problem Statement and Goals

Problem:

Online services need to verify user eligibility *without tracking users:*

- CAPTCHAs
- Rate-limited APIs
- Metered paywalls



Goal:

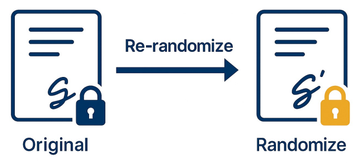
Create tokens that:

- Preserve anonymity
- Support selective attribute disclosure
- Carry a hidden metadata bit
- Require only one interaction with the issuer

Approach

We introduce **Smart Tokens**:

- We use **Zero Knowledge Proofs:**
  - To verify attributes (e.g., Age > 18) while keeping the actual data and user identity completely private.



- We use **Mercurial Signatures:**
  - That utilize equivalence class properties, so a user can transform a signature on a message into a new randomized valid signature.

Results

Properties

Total Privacy	Impossible to Counterfeit
No Framing	No Doubling Spending

Future Work

- Browser integration
- Public verification
- Post-quantum security

Related Work

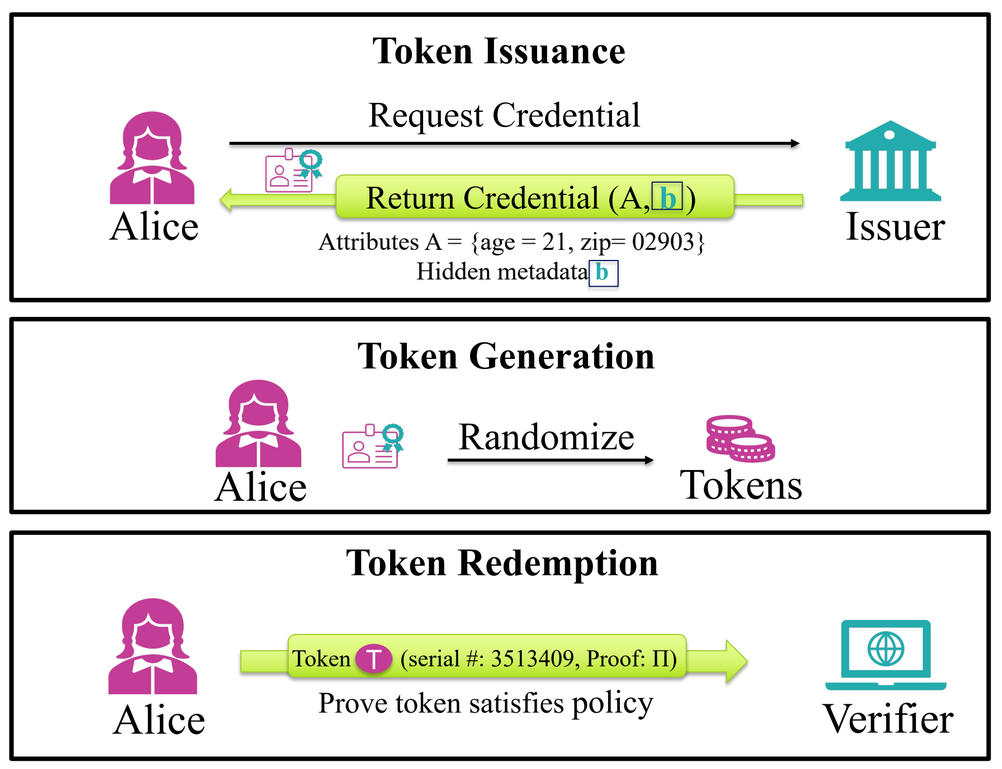
- Not attribute based
- Many online interactions
- Too revealing

References

1. Baldimtsi, F., Hanzlik, L., Nguyen, Q., Yadav, A.: Non-interactive anonymous tokens with private metadata bit. IACR Cryptol. ePrint Arch. p. 430 (2025), https://eprint.iacr.org 2025/430
2. Chairattana-Apirom, R., Dottling, N., Lysyanskaya, A., Tessaro, S.: Everlasting anonymous rate-limited tokens. In: Hanaoka, G., Yang, B. (eds.) Advances in Cryptology - ASIACRYPT 2025 - 31st International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, VIC, Australia, December 8-12, 2025, Proceedings, Part VI. Lecture Notes in Computer Science, vol. 16250, pp. 435–468. Springer (2025). https://doi.org 10.1007/978-981-95-5119-4_14, https://doi.org/10.1007/978-981-95-5119-4_14
3. Crites, E.C., Lysyanskaya, A.: Mercurial signatures for variable-length messages. Proc. Priv. Enhancing Technol. 2021(4), 441–463 (2021). https://doi.org/10. 2478/POPETS-2021-0079, https://doi.org/10.2478/popets-2021-0079

Acknowledgements. Thank you to my advisor Anna Lysyanskaya for her guidance and support ☺

Protocol



Proposed Protocol Overview

Eileen Nolan
Brown University

BROWN

Smart Tokens: Attribute-Based Anonymous Tokens with Hidden Metadata Bit

Abstract

In high-volume online services—such as privacy-preserving CAPTCHA bypass or metered paywalls—users need to prove eligibility without sacrificing anonymity. Anonymous tokens with a metadata bit allow users to do this, and additionally encode a bit of information that is hidden from the user; for example, whether there is reason to believe that the user is a bot.

Existing approaches to constructing anonymous tokens with a metadata bit require frequent, high-latency interactions with an issuer. This work solves this bottleneck by introducing a novel construction that leverages mercurial signatures.

Our core contribution is a protocol in which a user interacts with the issuer only once to obtain a master credential that also encodes the hidden metadata bit. By exploiting the equivalence class properties of mercurial signatures, the user can then locally re-randomize this single credential to generate up to N unlinkable, valid tokens without further online communication; each token encodes the hidden metadata bit from the master credential. This “issue once, spend N times” capability significantly reduces server load and network latency, making the scheme highly practical for real-time web applications.

Additionally, for the first time in the hidden-metadata context, our construction supports selective attribute disclosure.

Eileen Nolan
Brown University

BROWN