Privacy-preserving Age Verification based on Improved Verifiable Credentials Framework*

Shuang Liu
Carnegie Mellon university
shuangl4@andrew.cmu.edu

Sarah Scheffler
Carnegie Mellon university
sscheffl@andrew.cmu.edu

***Abstract*—To enhance children's safety online, emerging legislation requires social media platforms to verify users' age. Current verification measures, such as submitting ID copies or presenting digital ID raise significant privacy concerns due to the significantly increased uploading, transmission, collection, and sharing of sensitive identity documentation and information. Privacy-preserving credentials such as Verifiable credentials (VCs), a tamper-evident and cryptographically verifiable mechanism for asserting claims, offer a promising solution to this challenge. However, existing implementations of VCs require issuers to run a special protocol to issue and sign new VCs and often rely distributed ledgers, introducing inefficiencies for some issuers.**

This work proposes a novel privacy-preserving framework with key features: (1) compatibility with existing ID systems to minimize the operational costs from issuers; (2) disclosure of only the verification result without revealing additional information; (3) support for blockchain but without reliance on it.

The main contributions of this work include: (1) designing an efficient and privacy-preserving VC framework that seamlessly integrates with existing ID systems (e.g. U.S. driver's licenses); (2) laying the foundation for future research into deploying VCs for various verification tasks that rely on government ID; and (3) addressing the tension between protecting children online and safeguarding user privacy.

1. Introduction

To enhance safety for minors, legislators have been seeking to mandate age verification for online platforms. As of 2025, 19 states in the US have implemented age verification laws [1]. For example, Tennessee requires the match of a real-time photo of the user with a photo from a valid ID [2], while Texas accepts digital identification for age verification [3]. All these measures trigger serious privacy concerns due to the increased collection, transmission, and storage of sensitive personal information [4] [5].

Digital ID, an electronic version of identity documents, can be verified through digital channels and stored in smart phones [6]. Unlike traditional paper IDs that require physical inspection or copying of the entire ID, digital IDs enable encrypted data exchanges and selective disclosure of attributes [7], enhancing security, reliability, and privacy. Despite these benefits, digital IDs pose challenges. First, disclosing an exact birthdate exceeds the requirements of age-verification laws, which only need confirmation that a user is over 18. Second, reliance on third-party digital ID software results in sharing sensitive information with those third parties which can pose privacy concerns. Third, storing digital IDs on mobile devices or in the cloud increases vulnerability to breaches.

These challenges call for a secure, privacy-preserving, and standardized verification method. Privacy-preserving credentials such as anonymous credentials offer a promising solution, enabling users to prove their eligibility without disclosing personal information [8]–[10]. The World Wide Web Consortium (W3C) also introduced a similar concept named Verifiable Credentials (VCs) leveraging decentralized identifiers (DIDs) and shared ledgers [11]. A VC, digitally signed by an issuer, contains claims [12], and can bundle multiple attributes, allowing users to disclose only what is necessary. Research highlights VCs' potential to enhance privacy and authentication by minimizing data exposure [13].

Under the W3C VC model, to use VCs for age verification, issuers, usually government agencies, would create VCs containing age-related claims and maintain a status list (to record whether a VC is revoked or suspended), and the holder will store the VC and make presentation to verifiers [11]. While the W3C's VC system offers flexibility and scalability, it has several limitations when applied to state-mandated age verification:

1) Compatibility issues. Some states use digital ID systems with unique encryption and signature methods that may not seamlessly integrate with the W3C VC model.
2) Issuer burden. For age verification, issuers like DMVs or government agencies must generate a VC for each holder, creating significant operational overhead and making the W3C model inefficient for mandatory age checks.
3) Limited governmental adoption. State and federal agencies are hesitant to adopt decentralized solutions due to concerns over transparency and regulatory oversight.

Work in progress. This project is funded in part by Carnegie Mellon University's CyLab.

Problem Definition This paper proposes an efficient, privacy-preserving VC framework *compatible with existing digital ID systems*. It enables secure verification while achieving the following objectives:

1) Verify an ID property (e.g., the holder is over 18) without disclosing additional personal information, such as exact age or birthdate.
2) Minimize the operational burden on issuers. In particular, the issuer should only need to perform their existing functions: issuing IDs with a digital signature, they should not be required to change their systems to integrate with the VC protocol itself.
3) Ensure compatibility with existing digital ID systems by leveraging current signatures and digital attributes (e.g., barcode data on driver licenses) without requiring changes to their ID specifications.
4) Ensure compatibility with existing state DMV public keys by allowing verifiers to check signatures using keys in the American Association of Motor Vehicle Administrators' mDL Digital Trust Service [14]

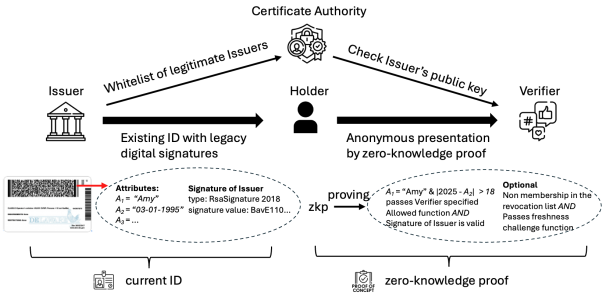
Certificate Authority
Whitelist of legitimate Issuers
Check Issuer's public key
Issuer
Holder
Verifier
Existing ID with legacy digital signatures
Anonymous presentation by zero-knowledge proof
Attributes:
A_1 = "Amy"
A_2 = "03-01-1995"
A_3 = ...
Signature of Issuer
type: RsaSignature 2018
signature value: BavE110...
zkp
proving
A_1 = "Amy" & |2025 - A_2| > 18 passes Verifier specified Allowed function *AND* Signature of Issuer is valid
Optional
Non membership in the revocation list *AND* Passes freshness challenge function
current ID
PROOF OF CONCEPT
zero-knowledge proof

Figure 1. Proposed Improved Framework for VCs

Improved VC Framework This paper proposes an efficient VC framework with no blockchain dependency in the W3C VC model, replacing it with traditional signature validation already supported by most IDs. In the W3C model, issuers—typically government entities—must issue and sign new VCs with age-related claims. In contrast, our proposed framework (Figure 1) integrates seamlessly with existing ID systems without requiring changes to current issuer practices in most cases. While compatible with blockchain, it does not rely on distributed ledgers or registries. Ultimately, this framework aims to achieve the following security properties:

1) Privacy: No party (especially a verifier, even if malicious) should get any information beyond the fact that the credential was accepted (or rejected).
2) Soundness: If a malicious holder presents a disallowed credential, it should not verify.
3) Completeness: All valid IDs can be verified. Valid IDs are those with attributes that make a verifier-chosen function return True.
4) *Optional:* Revocation should be possible by Issuers.
5) *Optional:* Freshness and security against replay.

2. Related Works

Anonymous credentials, a privacy-preserving form of VCs that allow users to prove that they have valid credentials without disclosing personal information (e.g. identity). The concept was first introduced by Chaum in 1985 [8]. Later, Camenisch and Lysyanskaya developed a fully realized anonymous credential scheme using CL-signatures based on RSA groups [15], [16]. Brands proposed an alternative method using pairing-free groups, with Baldimtsi and Lysyanskaya subsequently providing formal security proofs for this approach [9], [17]. *zk-creds*—an issuer-agnostic toolkit based on Merkle Trees—has been introduced to support flexible identity statements with zero-knowledge proofs [10]. More recently,, *CanDID*, a decentralized identity system, has introduced a more user-friendly approach to credential issuance through committee nodes [18].

A VC is a digitally stored set of claims and cryptographic proofs of identity or attributes, verified by third parties to ensure authenticity and prevent tampering [11]. W3C formalizes the workflows into three steps: (1) the issuer verifies the user's identity, signs on and issues VCs; (2) the user presents the VC to a verifier to prove eligibility, such as confirming they are over 18; and (3) the verifier checks the presentation against the registry and grants services upon successful verification [11].

In recent years, VCs have gained significant traction in both academia and industry, particularly within digital identity systems aligned with the self-sovereign identity (SSI) framework [19]. For instance, Microsoft's Entra Wallet Library provides tools for managing decentralized identifiers (DIDs) and VCs for secure access control [20].

3. Contributions

1) We design and present a novel, efficient VC framework and protocol for online verification. Our protocol always reveals *only* the result of the verification check (i.e. whether the holder has sufficient credentials or not) and reveals no other information.
2) Our approach seamlessly integrates with existing digital identity systems (e.g. the ISO standards) and signature schemes used by issuers, without requiring changes to current practices by government agencies.
3) Unlike other anonymous credential approaches for age verificaiton like zk-creds [10], our framework eliminates reliance on blockchain technology, significantly improving efficiency while maintaining the same privacy and security guarantees.
4) Beyond age verification, our approach has broader applications for government-related and ID-based verification scenarios. This work lays the foundation for future research into deploying VCs for various government-related verification tasks.

References

[1] F. A. Center. (2025, Apr.) Age verification: The complicated effort to protect youth online. [Online]. Available: https://action.freespeechcoalition.com/age-verification-resources/state-avs-laws/

[2] T. S.B.1792, 2024.

[3] T. H.B.1181, 2023.

[4] S. Scheffler, "Age verification systems will be a personal identifiable information nightmare," *Communications of the ACM*, vol. 67, pp. 31–33, 07 2024.

[5] CNIL. (2022) Online age verification: balancing privacy and the protection of minors. [Online]. Available: https://cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[6] J. M. D. M. J. B. M. M. Olivia White, Anu Madgavkar and O. Sperling. (2019) Digital identification: A key to inclusive growth. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#section-header-1

[7] D. Slamanig, K. Stranacher, and B. Zwattendorfer, "User-centric identity as a service-architecture for eids with selective attribute disclosure," in *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 153–164. [Online]. Available: https://doi.org/10.1145/2613087.2613093

[8] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, p. 1030–1044, Oct. 1985. [Online]. Available: https://doi.org/10.1145/4372.4373

[14] AAMVA, "Mobile driver license digital trust service," https://www.aamva.org/identity/mobile-driver-license-digital-trust-service.

[15] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, ser. EUROCRYPT '01. Berlin, Heidelberg: Springer-Verlag, 2001, p. 93–118.

[16] ——, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, ser. Lecture Notes in Computer Science, vol. 3152. Springer, 2004, pp. 56–72. [Online]. Available: https://iacr.org/archive/crypto2004/31520055/cl04.pdf

[9] S. Brands, "A technical overview of digital credentials," 2002. [Online]. Available: https://api.semanticscholar.org/CorpusID:18284690

[10] M. Rosenberg, J. White, C. Garman, and I. Miers, "zk-creds: Flexible anonymous credentials from zkSNARKs and existing identity infrastructure," Cryptology ePrint Archive, Paper 2022/878, 2022. [Online]. Available: https://eprint.iacr.org/2022/878

[11] D. C. I. H. Manu Sporny, Dave Longley. (2025, Feb.) Verifiable credentials data model v2.0. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/#dfn-verifiable-credential

[12] S. A. Kakvi, K. M. Martin, C. Putman, and E. A. Quaglia, "Sok: Anonymous credentials," in *Security Standardisation Research: 8th International Conference, SSR 2023, Lyon, France, April 22-23, 2023, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2023, p. 129–151. [Online]. Available: https://doi.org/10.1007/978-3-031-30731-7_6

[13] L. Hanzlik and D. Slamanig, "With a little help from my friends: Constructing practical anonymous credentials," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 2004–2023. [Online]. Available: https://doi.org/10.1145/3460120.3484582

[17] F. Baldimtsi and A. Lysyanskaya, "Anonymous credentials light," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 1087–1098. [Online]. Available: https://doi.org/10.1145/2508859.2516687

[18] D. Maram, H. Malvai, F. Zhang, N. Jean-Louis, A. Frolov, T. Kell, T. Lobban, C. Moy, A. Juels, and A. Miller, "Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1348–1366.

[19] M. Richter, M. Bertram, J. Seidensticker, and M. Margraf, "Cryptographic requirements of verifiable credentials for digital identification documents," in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2023, pp. 1663–1668.

[20] M. Entra. (2025) Introduction to microsoft entra verified id. [Online]. Available: https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview