Passkeys and Verifiable Digital Credentials: A Harmonized Path to Secure Digital Identity

September 2025

Editors:

Christine Owen, 1Kosmos
Teresa Wu, IDEMIA Public Security

Abstract

Around the world, government entities are currently working to create and implement their digital identity strategies, which includes issuing verifiable digital credentials (VDCs) to their citizens. As a result of these initiatives, organizations are also beginning to discuss using VDCs as a primary form of authentication. VDCs are an important part of verifying a user's identity that can be used alongside FIDO's passkeys, which provide a primary authentication mechanism that is fast, safe, and reliable. Passkeys should be issued after a citizen's VDC is presented for identity verification. This paper will discuss how VDCs and passkeys should coexist when implementing authentication for citizens.

We anticipate a growing confusion in recognizing the differences between the use of digital ID to ascertain identity attributes and allowing users to authenticate themselves online as solutions that follow digital ID standards for online use cases (such as **ISO/IEC 18013-7**, **W3C**, **IETF**, or **SD-JWT**) are deployed.

This paper aims to clarify misperceptions and avoid confusion by discussing the coexistence of passkeys and digital ID/VDCs, including best practices for using these technologies.

Audience

Government entities, policy makers, relying parties

Table of Contents

1 Verifiable digital credentials (VDCs) and passkeys

As new technologies continue to emerge, experts are finding new ways to use these solutions together. This paper discusses how verifiable digital credentials (VDCs) and passkeys should coexist when implementing authentication for citizens. VDCs and passkeys were both developed to secure identities in the digital world. However, they have different yet intersecting roles for end users. The following sections introduce VDCs and passkeys.

1.1 VDCs

A VDC can contain an electronic version of identity attributes or can be a digital representation of physical credentials (for example, driver licenses, passports, other identifiable information) that can be cryptographically verified. Typically, a VDC follows the **W3C Verifiable Credentials Data Model**, **Internet Engineering Task Force (IETF) Selective Disclosure for JWTs (SD-JWT)**, or **ISO/IEC 18013-5/7** (mobile driver's license) standards, which require cryptographic signatures to prove authenticity. Because these standard models use digital wallets, a secure, portable, and instant verification mechanism is created that can preserve privacy by requiring user approval prior to disclosure of sensitive information.

Deployment of VDCs is currently prolific in multiple regions around the world. For example, Asia-Pacific countries are embracing the idea of a VDC. Countries such as Japan, South Korea, and Australia are working together to ensure interoperability amongst their VDCs. Australia's 2024 Digital ID Act created accreditation requirements for digital IDs and enhanced the trust framework between different providers. In the United States, the mobile driver's license (mDL) movement is gaining momentum, and several states have already implemented or are piloting mDL programs. For a more detailed look at how government agencies are deploying VDCs, refer to the Appendix.

VDCs can be either a Person ID (PID) that represents a physical person or Attested Attributes which are documents that present properties of a person such as a driver license, age in a certain range, or educational degrees. The validity of VDCs can be expressed by Identity Assurance Levels (IAL) or Levels of Assurance (LOA) (depending on a country's digital identity standards). In cases where a PID is used, a government entity may determine the types of verified information that are necessary to establish the identity of a person. In most cases, information about a person's name, address, date of birth, place of birth, official government document number, phone number, and other attributes such as name of parents, gives a strong base for properly identifying a person through the controls available to government or private entities that perform verification on behalf of organizations. Modern technology may add records of biometrics such as fingerprints or face capture to further strengthen identity assurance. The European

Digital Identity Wallet (EUDI Wallet) requires that PID be a high level of assurance (LoA), in accordance with the principles used by member states for their civil registration process. Refer to section 5.3 EU VDC Efforts for more information on EUDI Wallets. Similarly, the **United States Digital Identity Guidelines**[1] require remote identity vetting to be performed at an IAL2 for government use.

VDCs hold a digital representation of a document by defining the syntax of the issuer's URL, the category of the document, and other standardized syntax such as a trust list (where government entities issue a certificate that guarantees that the URL is what it claims to be), then creating a cryptographic *seal* that guarantees the authenticity of the document when presented to a relying party (also known as a verifier). Under this **W3C Verified Credentials Data Model**, the URL serves as a trust model.

Because government entities are also building digital identity wallet schemes based on clear identity standards and mutual recognition mechanisms across different jurisdictions, the adoption of digital identity wallets internationally will facilitate the acceptance of VDCs by traffic police to validate a driver's license from another country or for a bank to provide the proper checks and balances (for example, know your customer) during transactions.

1.2 Passkeys

Passkeys, a passwordless and phishing-resistant authentication mechanism, represent a significant advancement in privacy-preserving authentication and are designed to replace traditional passwords with a more secure and user-friendly alternative.

There are two types of passkeys: synced passkeys and device-bound passkeys. Synced passkeys are stored in the cloud and can be accessed across multiple devices, offering convenience and easy recovery. Device-bound passkeys, on the other hand, are stored locally on a specific device or security key, which provides enhanced security. For a more in-depth look at passkeys and how to implement them, refer to Passkey Central.

Passkeys exhibit a robust resistance to phishing attacks due to their foundational design principles. Each passkey is intrinsically tied to the specific origin of the service, identified by the Relying Party ID, thereby ensuring that authentication can only occur with the legitimate and intended service provider. This origin-specific challenge-response mechanism is inherently resistant to replication by phishing sites, rendering such attacks ineffective.

[1] https://www.nist.gov/identity-access-management/projects/nist-special-publication-800-63-digital-identity-guidelines

Equally significant is the privacy-preserving architecture of passkeys, which is designed to uphold user confidentiality and prevent tracking. During authentication, no personal or biometric data is transmitted or shared externally. Biometric verification processes, such as fingerprint or facial recognition checks, are conducted locally on the user's device, ensuring that sensitive data remains under the user's control.

Because passkeys generate unique cryptographic keys for each service and cannot be reused across platforms, cross-platform tracking is precluded and the privacy concerns associated with social logins that enable providers to monitor user activity across multiple services are avoided. Unlike traditional authentication methods (such as passwords or two-factor authentication), the use of unique cryptographic keys effectively mitigates the risk of cascading breaches that can result from a single compromised account. By replacing shared secrets with device-bound cryptographic keys, passkeys fundamentally neutralize phishing as a viable attack vector. When passkeys are synchronized across devices via cloud-based mechanisms, they are protected through end-to-end encryption.

This privacy-centric design fosters a sense of security and trust among users and reassures them that their personal information is not being tracked or misused by government entities or service providers. By combining phishing-resistant authentication with privacy-preserving principles, passkeys represent a significant advancement to secure and user-centric digital identity management.

1.3 The intersection of VDCs and passkeys

Both VDCs and passkeys enhance security and reduce friction during digital interactions. VDCs focus on securely representing qualifications and attributes (association with the real user), while passkeys specifically target phishing-resistant authentication (what a user has). When used together, these two technologies complement each other to enhance security within the digital world.

2 Core concepts of digital identities

This section covers the differences between digital identities, authentication, and authorization. It also examines how to enhance the use of verifiable digital credentials.

2.1 Verified identities vs authentication vs authorization

Digital identities play a crucial role in facilitating online transactions. Commonly, VDCs contain identity attributes that can be presented as evidence to verify the identity of the VDC holder. For example, an individual might use their VDC to assert attributes such as name, date of birth, and address in order to verify their identity and open a financial

account with a bank. The bank can use these attributes to comply with regulations such as **Know Your Customer (KYC)** or **Anti-Money Laundering (AML)**.

Identity verification is the process of confirming that a person is who they claim to be, often during onboarding, using trusted documents for proof of identity. Once a verified identity is established, authentication helps verify individuals on return visits. While passwords or two-factor authentication have traditionally been used for authentication, passkeys are not only more secure than traditional authentication methods but also provide users the convenience of quickly using a biometric to unlock a cryptographic key which is then used for authentication. Passkeys, unlike VDCs which may assert information about the user each time they are presented, are privacy preserving and do not provide user attributes during authentication.

VDCs can be used to transmit requested identity attributes to relying parties during authorization requests.[2] This method can decrease the relying party's exposure to risk, as it provides a more holistic view of an end user through their verified set of attributes. The relying party can then make an informed decision regarding that user's access based on their rules for access and the attributes presented.

2.2 Enhancing verifiable digital credentials use

VDCs are designed to enable individuals to make verifiable claims about identity attributes or entitlements without serving as direct authentication mechanisms. Unlike authentication methods that authenticate users to specific services, VDCs focus on sharing attested claims (for example, date of birth, and address) through a decentralized *triangle of trust* that involves issuers, holders, and verifiers. VDCs are designed with privacy in mind, as standards such as **SD-JWT** and **ISO mdoc** require that when users share specific claims from a credential (for example, age from a driver's license), the integrity of the original document must be proven cryptographically. Users retain ownership of VDCs, enabling them to present credentials across platforms without relying on centralized authorities. This flexibility makes VDCs ideal for scenarios that require proof of identity.

Passkeys provide a phishing-resistant authentication method that binds authenticators to specific domains. Passkeys do not pass Personally Identifiable Information (PII) or

[2] Authorization is the process of granting the correct level of access to a user after their identity is authenticated. As a specific function within Identity and Access Management (IAM) systems, authorization helps system managers control who has access to system resources and set client privileges. Access controls are used to assign a set of predetermined access rights to a user identity and use of attribute exchanges to help determine authorization requests is gaining traction in the cybersecurity industry.

similar information at the time of authentication, thus preserving the privacy of the user. However, VDCs can pass along unnecessary PII, when requested by a relying party and agreed upon by the Holder. For instance, a malicious actor could impersonate a bank's identity verification portal, capture a user's PII from their VDC, and exploit the user's PII. While cryptographic signatures ensure credential integrity, they do not address contextual misuse, highlighting a gap in current standards. Therefore, it is better to utilize VDCs for user credentials and attributes.

Despite these risks, VDCs are increasingly adopted for high-assurance processes:

- Universities can use VDCs to streamline enrollment by verifying academic records and extracurricular participation.
- Banks can employ VDCs for eKYC (electronic Know Your Customer), combining document verification (for example, passports), biometric liveness checks, and AML and Politically Exposed Person (PEP) screening to onboard customers remotely.
- VDCs mitigate fraud in transactions requiring stringent identity assurance, such as cross-border financial transfers or healthcare licensing. For example, selfie verification and document-centric checks ensure the physical presence of users during high-value agreements.
- In cross-border education, VDCs enable instant verification of international student credentials, reducing administrative delays and fraud risks.

However, these applications often require supplementary safeguards (for example, multi-factor authentication, liveness detection) to compensate for the PII phishing susceptibility of VDCs.

VDCs offer transformative potential for decentralized identity management, particularly for enrollment and high-assurance transactions. By integrating VDCs with phishing-resistant authentication mechanisms and advancing interoperability standards, government entities and organizations can harness their benefits while mitigating risks. As the ecosystem evolves, collaboration among government entities, standards bodies, and industry stakeholders will be essential to balance innovation with security.

3 Key considerations

VDCs and passkeys are built according to widely accepted standards, which promotes interoperability and offers seamless integration across various platforms and services. This standardization is crucial for widespread adoption and the creation of a truly interconnected digital identity ecosystem.

3.1 Privacy consideration

Privacy preservation is a key feature that must be present for both VDCs and passkeys. Combining VDC's and passkeys benefit both the end users and relying parties. In this ecosystem, users maintain control over their credentials and can selectively share attributes as needed, for example when enrolling as a user with a relying party. Relying parties can be confident that the person behind the VDC is, more likely than not, who they say they are.

Moving forward however, the identity industry as a whole should address growing concerns about data privacy and control in the digital age. While VDCs are privacy-preserving mechanisms that hold and share verified credentials, relying parties should only request the minimum attributes required from the end user to enroll them in the application. Depending on the application type and legal and regulatory requirements, the attributes could be as little as email address and name or may also include verified home address and national identity number.

3.2 eIDAS 2.0 regulation

The European Digital Identity Regulation 2.0 (**eIDAS 2.0)** regulation describes where passkeys can be implicitly or explicitly used within the EUDI Wallet. The PID for an EUDI Wallet should be used with a high eIDAS LoA for initial authentication to a relying party. A FIDO passkey can be enrolled to the user's EUDI Wallet to meet this requirement. The passkey can then be used for repeated authentication with pseudonyms to the relying party. In this way, passkeys can co-exist or complement the VDC in the EUDI Wallet ecosystem.

Section **5f.3**[3] of the eIDAS 2.0 regulation reads that while very large online platforms must accept and facilitate the use of EUDI Wallets for authentication, they must do so "in respect of the minimum data necessary for the specific online service for which authentication is requested". Therefore, eIDAS 2.0 allows online platforms to support pseudonymous PID authentication, rather than require those platforms to also accept VDCs that are issued by and tied to a government-issued credential.

Consequently, passkey providers will need to issue and restore passkeys. The passkey provider services can be operated by different entities in the EUDI Wallet ecosystem: by the cloud-based EUDI Wallet backend, by the PID provider, or by the Qualified Trust Services Provider (QTSP) that issues the (Qualified) Electronic Attestation of Attributes ((Q)EAAs).

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183

Cloud-based EUDI wallets and passkey providers have an interesting synergy. PIDs and (Q)EAAs are hosted at a cloud-based EUDI Wallet backend that is accessed from the user's devices using FIDO passkeys. If the user's device is lost or replaced, the user would only need to restore the FIDO passkey, which will then give the user access to the PIDs and (Q)EAAs. This allows for rapid recovery of an EUDI Wallet since the user can first download the FIDO passkey to a device and then use the FIDO passkey to get instant access to the cloud-based EUDI Wallet.

3.3 Use cases for an integrated approach for VDCs and passkeys

Passkeys and digital identity wallets are not competing technologies, but rather complementary solutions that together create a robust, portable identity ecosystem. Passkeys serve as a secure gateway to digital identity wallets, providing strong defense against unauthorized access, and wallets serve to provide valuable data during high-risk transactions. This combination enhances security and streamlines the user experience by unifying verified identity (EUDI Wallet) with easy authentication (passkey).

Perhaps most importantly, this combination allows for the creation of reusable identities. Users can prove their identity once and then reuse the same VDC across multiple services, significantly reducing friction for digital interactions while maintaining high security standards. The potential applications for this integrated approach to digital identity and authentication are vast and span multiple sectors:

- Online verification: In e-commerce, (for example, state-backed liquor stores) age verification for purchasing restricted products can be streamlined using verified credentials stored in a digital wallet and accessed securely with a passkey.
- Government services: Secure access to tax filing systems and other government benefits can be facilitated through this combined approach, enhancing security while improving user experience.
- Healthcare: Verifying prescribing doctor's credentials across multiple hospitals becomes more efficient and the secure transfer of patient records between healthcare providers can be streamlined.
- Education: Higher education systems can more effectively prevent account takeovers and students can create reusable identities that carry their records throughout their academic careers and beyond.
- Financial services: Know Your Customer (KYC) processes can be significantly streamlined and enhanced security for high-risk transactions can be implemented more effectively.

In most use cases, relying parties should use VDCs to enroll their constituents at the beginning of their interactions and accept passkeys for further interactions with the constituent. If a constituent is conducting a high-risk transaction, then the relying party should ask for additional attributes from the VDC at the time of authentication. Additionally, a VDC should be used for passkey recovery, while a passkey should be used to access the VDC.

4 Recommendation

Government entities and organizations who adopt passkeys as the primary form of authentication for constituents can leverage their enhanced security and ease of use. To ensure trust and usability, passkeys should be backed by verified digital credentials (VDCs), especially in scenarios where a verified identity is required for passkey issuance or account recovery. VDCs provide a robust mechanism to securely recover passkeys while maintaining a high level of assurance.

To implement this effectively, a tiered approach based on Identity Assurance Level (IAL) requirements and the risk tolerance of the data being protected within the service is recommended. For services with moderate IAL requirements, relying parties (RPs) should:

- Read a government-issued ID to verify the user's identity.
- Create a passkey tied to the verified identity.
- Use the passkey for re-authentication in all subsequent interactions.

Government entities and organizations who adopt passkeys as the primary form of authentication for constituents can leverage their enhanced security and ease of use. To ensure trust and usability, passkeys should be backed by verified digital credentials (VDCs), especially in scenarios where a verified identity is required for passkey issuance or account recovery. VDCs provide a robust mechanism to securely recover passkeys while maintaining a high level of assurance.

To implement this effectively, a tiered approach based on Identity Assurance Level (IAL) requirements and the risk tolerance of the data being protected within the service is recommended. For services with moderate IAL requirements, relying parties (RPs) should:

- Read a government-issued ID to verify the user's identity.
- Create a passkey tied to the verified identity.
- Use the passkey for re-authentication in all subsequent interactions.

For services with higher IAL requirements, collaboration between government entities and organizations like the FIDO Alliance is essential. Together they can develop solutions to ensure that passkeys meet stringent assurance levels while maintaining user privacy and convenience.

Additionally, there is a pressing need for standards and mutual recognition arrangements for IAL across jurisdictions. Government entities should work to establish clear guidance that states which IAL levels are required for specific services for legal compliance and consumer protection. These standards should aim to be valid across as many countries as possible to facilitate interoperability and trust for cross-border digital interactions.

By adopting passkeys as the foundation of authentication and aligning them with verified credentials and standardized IAL frameworks, government entities can enhance security, improve user experience, and foster global cooperation in digital identity management.

5 Appendix

5.1 Verifiable digital credentials for government deployments

The digital identity landscape is undergoing significant transformations worldwide. This appendix explores how government entities around the world are implementing VDCs.

5.2 APAC VDC efforts

Asia-Pacific countries are embracing the idea of a VDC. Countries such as Japan, South Korea, and Australia are working together to ensure interoperability amongst their VDCs. Australia's **Digital ID Act 2024** created accreditation requirements for digital IDs and enhanced the trust framework between different providers.

In Asia, government-issued digital credentials are advancing rapidly but unevenly; a reflection of diverse economic, technological, and regulatory landscapes. Recent deployments highlight both the progress and the critical role of standards bodies (such as **ISO/IEC** and **W3C**) in shaping secure, interoperable systems. In Asia, countries such as India, Singapore, and South Korea are leading with robust digital ID systems, while Australia is harmonizing mDLs with international standards for secure, interoperable credentials.

Singapore's **SingPass** is a benchmark for seamless public and private service access. South Korea leverages digital IDs for e-governance, incorporating **FIDO** and **ISO/IEC 29115** standards. Japan's Digital Agency[4] drives *Individual Number* (*My Number*) card enhancements through initiatives such as the **Asia Pacific Digital Identity Consortium**[5] launched in December 2024.

The government of Japan started issuing digital National IDs (individual number card/My Number card on smartphones) in mdoc format (standardized under **ISO/IEC 18013-5**) for iPhone users on June 24, 2025, and is planning to issue it for Android users in 2026. For the digital National ID, identity information such as name, birthdate, address, gender, and individual number (called *My Number* in Japan) are included. The aim is for digital National IDs to be used in various identity proofing use cases for both in-person and remote use cases.

In Southeast Asia, Thailand's 2022-24 Digital ID Framework targets 10 million digital IDs and National Digital ID platforms. When discussing biometrics across Mobile ID, D.DOPA, the creators of this framework referenced **NIST 800-63** and **ISO/IEC 19794** standards. Malaysia's MyDigital ID, which adheres to **ISO/IEC 27001**, and Sarawak's

[4] https://www.digital.go.jp/en
[5] https://www.apdiconsortium.org/

planned **Sarawakpass**, aims to emulate **SingPass** for cashless transactions and service access. The Philippines' **PhilSys** has enrolled 68 million, focusing on digital issuance to bypass physical card delays. In March 2025, Taiwan's Digital Ministry introduced a prototype **Taiwan Digital Identity Wallet** (TW DIW), a non-mandatory mobile app for storing IDs and licenses, using biometric authentication and selective disclosure. A sandbox trial began in March, with broader testing planned for December, but it is not a full digital ID replacement and excludes medical data sharing.

Australia and New Zealand are harmonizing mobile driver's licenses with **ISO/IEC 18013-5**. In Australia and New Zealand, harmonization efforts for mDLs center on adopting **ISO/IEC 18013-5**, which ensures secure, interoperable digital credentials verifiable domestically and internationally. In Australia, Austroads' **Digital Trust Service** (DTS) leads the charge with a pre-production version tested successfully for national scalability. New South Wales, with 4.5 million users since 2019, is transitioning its **Service NSW** app, which offers app-based mDLs, to full compliance, ensuring legal equivalence to physical cards. South Australia's **mySAGOV** app incorporates the standard's verification features. The DTS, targeting a 2025-26 rollout, enables cross-jurisdictional and global verification, was demonstrated at the 2024 Identity and Verifiable Credentials Summit for uses like U.S. airport access and includes New Zealand in its interoperability framework. New Zealand is aligning its NZTA app-based digital licenses with **ISO/IEC 18013-5**, building on mutual recognition agreements with Australia.

5.3 EU VDC efforts

In Europe, the **European Digital Identity Regulation 2.0** (eIDAS 2.0) regulations, which came into force in May of 2024, mark a pivotal shift in how digital identities are managed across the European Union. This updated framework introduces the European Digital Identity Wallet (EUDI Wallet), which aims to provide EU citizens with a secure, interoperable digital identity solution for accessing public and private services across member states.

The EUDI Wallet is a cornerstone of the eIDAS 2.0 regulation[6] and will be offered free of charge to all EU citizens. The purpose of the EUDI Wallets is to enable EU citizens to prove their identity when accessing both online and offline resources or to present specific personal attributes without revealing their full identity. The EUDI Wallets will be

[6] The "Regulation (EU) 2024/1183 as regards establishing the European Digital Identity Framework" (eIDAS 2.0) was adopted by the EU parliament in April 2024. The eIDAS 2.0 regulation will be extended with Commission Implementing Regulations (CIRs), also known as "implementing acts", which will elaborate certain legal aspects of the eIDAS 2.0 regulation. The eIDAS 2.0 CIRs continue to be specified.

able to be used for use cases such as the mobile driving license, payments, access to public services, and opening a bank account.

The EUDI Wallet architecture is outlined in the European Digital Identity Wallet Architecture and Reference Framework (the ARF), which specifies the formats and protocols to be used by the EUDI Wallets. Each EUDI Wallet will be bootstrapped with a Personal Identity Document (PID), which will be enrolled at the high eIDAS Level of Assurance (LoA). In addition to the PID, users will have the option to add additional (Q)EAAs, which can prove the user's identity and claims to relying parties.

The ARF has specified that the following formats are suitable for the PID and (Q)EAAs:

- **ISO/IEC 18013-5** mobile driving license (mDL)
- W3C Verifiable Credentials Data Model v1.1
- IETF SD-JWT-based Verifiable Credentials (SD-JWT VC)

Furthermore, International Civil Aviation Organization (ICAO) Digital Travel Credentials (DTC) can also be used as a (Q)EAA with the EUDI Wallet.

5.4 US VDC Efforts

In the United States, the mobile driver's license (mDL) movement is gaining momentum, and several states have already implemented or are piloting mDL programs. Unlike the centralized approach of **eIDAS 2.0**, the U.S. initiatives are being developed more organically, driven by individual federal agencies and state efforts, alongside industry collaborations. These developments reflect a growing recognition of the need for robust, user-centric digital identity solutions in an increasingly digital world, although they approach this goal through different regulatory and technological paths.

As US states provide their constituents with ID cards and driver's licenses, the responsibility of creating mID and mDLs lies with each of the states. As such, the development and implementation of mDLs in the US has been a gradual and varied process across different states.[7] While only about a third of US states currently offer mDLs, many states are pushing forward, as they recognize the potential benefits of mDLs in improving remote transactions, reducing identity fraud, and enhancing digital identity verification for both government services and private sector services.

The Transportation Security Administration (TSA) is evaluating the potential impact of VDCs (such as mobile driver's licenses) on aviation security and operations. The TSA

[7] As of March 2025, the states that offer mDLs include Alaska, Arkansas, Arizona, California, Colorado, Delaware, Georgia, Hawaii, Iowa, Louisiana, Maryland, Mississippi, New York, Ohio, Puerto Rico, Virginia, Utah, and West Virginia.

has integrated digital identity capabilities, including the acceptance of state-issued mobile driver's licenses, at TSA checkpoints using the Credential Authentication Technology 2 (CAT-2) system to provide for a secure and seamless method of verifying an individual's identity. Currently, the TSA is accepting mobile driver's licenses and mobile IDs from 15 participating states. In October 2024, the TSA published a final rule in the Federal Register that would allow passengers to continue using mobile driver's licenses (mDL) for identity verification at TSA airport security checkpoints now REAL ID enforcement began on May 7, 2025.

In addition to publishing the **Digital Identity Guideline SP 800-63**, the NIST National Cybersecurity Center of Excellence (NCCoE) launched an mDL adoption acceleration project to bring together stakeholders from across the mDL ecosystem to work to build out a reference implementation to promote standards and best practices for mDL deployments and to address mDL adoption challenges. The first NCCoE use case will focus on helping consumers create financial accounts and helping financial institutions meet Customer Identification Program/Know Your Customer (CIP/KYC) requirements using mDLs.

For the US Federal government's digital interactions with users, agencies are embracing the idea of a reusable identity stored in a digital identity wallet. Generally speaking, these VDCs are cloud-based and would be used to verify a user's identity prior to interacting with a federal agency for actions such as enrolling in public benefits or filing taxes. These VDCs are also tied to an authenticator that the constituent would use to sign in to the agency's application. Within the federal space, a VDC tied to an authenticator is called a credential service provider (CSP).

5.5 UK VDC Efforts

The UK Government released the **Digital Identity and Attributes Trust Framework (DIATF) gamma version (0.4)**[8], in November 2024, which outlines the standards and roles for digital identity services which relate to digital wallets. The UK plans to introduce digital driving licences in 2025, that will be available through a new GOV.UK digital wallet app on smartphones.

[8] https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04

6 Contributors

- Jerome Becquart, Axiad
- John Bradley, Yubico
- Tim Cappalli, Okta
- Sebastian Elfors, IDnow
- Hideaki Furukawa, Nomura Research Institute, Ltd.
- William Fisher, NIST
- Henna Kapur, Visa
- Sue Kooman, American Express
- Matthew Miller, Cisco
- Jeff Nigriny, CertiPath, Inc.
- Joe Scalone, Yubico
- Alastair Treharne, Ingenium Biometric Laboratories

7 Document history

Change	Description	Date
Initial publication	White paper first published.	September 2025

8 References

The Asia-Pacific Digital Identity (APDI) consortium. APDI consortium. https://www.apdiconsortium.org/

Digital Agency. Home. Digital Agency. https://www.digital.go.jp/en

The FIDO Alliance. Home. Passkey Central. https://www.passkeycentral.org/home

NIST. Digital Identities - Mobile Driver's License (mDL). NIST National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/projects/digital-identities-mdl

NIST. (2025, July). NIST SP 800-63-4 Digital Identity Guidelines. NIST. https://www.nist.gov/identity-access-management/projects/nist-special-publication-800-63-digital-identity-guidelines

Office for Digital Identities and Attributes and Department for Science, Innovation and Technology. (2025, June 26). UK digital identity and attributes trust framework (0.4). Gov UK. https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04

The European Parliament and the Council of The European Union. (2024, April 11). Regulation (Eu) 2024/1183 of the European Parliament and of the Council. EUR-Lex.europa.eu. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183

Transportation Security Administration. (2024, October 7). TSA announces final rule that enables the continued acceptance of mobile driver's licenses at airport security checkpoints and federal buildings. TSA. https://www.tsa.gov/news/press/releases/2024/10/24/tsa-announces-final-rule-enables-continued-acceptance-mobile-drivers

