Verifiable Digital Credentials – Best Practices for Organizations Requesting and Using Identity Data

Version 1.0

October 2026

BETTER IDENTITY COALITION

Introduction

Governments are increasingly offering their residents and customers the option of obtaining a digital counterpart to the paper and plastic credentials governments issue today – and storing those credentials in a digital wallet. In the United States, state governments have been at the forefront of digital credentials with new mobile driver's licenses (mDL) initiatives, however, a variety of Federal, state, and local agencies are considering launching similar initiatives to support other authoritative government credentials including passports, social security cards, and birth certificates. Together, these digital IDs represent a new class of government-issued verifiable digital credentials (VDCs) that will likely transform the ways that people in the United States prove their identity, both in person and online.

VDCs have the potential to improve security, privacy, usability, and inclusivity for individuals and business if they are designed, deployed, and used responsibly. However, the introduction of VDCs, specifically government issued ones, also brings the possibility that misuse or overuse of these credentials could erode security, privacy, and civil liberties. Among the top concerns is that, by making it easier than ever for individuals to prove who they are online, companies and government agencies will start to ask for ID for use cases where they rarely – if ever – did so before. And in doing so, it would significantly change the balance of power in terms of what is expected of individuals to allow them to engage and transact online.

Since the dawn of the Internet, the ability to be anonymous or pseudonymous online in the vast majority of one's interactions has been a core feature of the Internet. An exception has been in a set of high-value and/or high-risk transactions – largely associated with financial services, health care, and government benefit programs – where there are legal or regulatory requirements to determine the identity of an individual, or in some cases, validate something about them (i.e., that someone is over 21 or a resident of a particular state). There are also a number of transactions where there is no legal or regulatory requirement to collect and validate identity data but where the risk model is such that service providers do not make a product or service available online because there is a business need for that provider to validate identity or attributes – and so that service provider has traditionally asked to see an ID.

As VDCs start to be used in the marketplace, it is important to ensure that their arrival does not lead to a world in which individuals are expected to share their identity every place they go online.

Likewise, there are some concerns that VDCs could be used to augment or replace cookies and other technologies that are currently used to track behavior online. VDC standards have been specifically architected to ensure that individuals can assert their ID – and online service providers can validate identity or attributes – without enabling new forms of tracking. It is important to ensure as VDCs are implemented that they are not used by some actors to enable new ways to track individuals.

In many other countries, governments are setting rules to govern who can ask for proof of ID online, and in what circumstances. In the U.S., however, the Federal government has not focused much attention on this issue, nor have most state governments. This set of Best Practices is intended to address these concerns – by establishing guidelines that digital wallet providers, issuers, and others in the digital identity ecosystem can follow, and use as a tool to restrict inappropriate or overly invasive requests for identity information from online service providers. The goal is that, by proactively setting rules of the road for the use of VDCs, these best practices can mitigate the risks involved with new government digital credentials while ensuring that the benefits of improved security, privacy, usability, and inclusivity are fully realized.

Best Practices Overview

Purpose

These Best Practices aims to set a high bar for security, privacy, usability, and inclusivity associated with the use of VDCs, by:

- Introducing a set of core Best Practices for VDC use.
- Defining core use cases and attribute bundles where it is appropriate for online service providers to ask for validated identity and/or attributes.
- Outlining use cases where a request for validated identity and/or attributes is inappropriate and should be restricted.

Companies and organizations that pledge to adhere to the Best Practices will be empowered to restrict or limit requests for validated identities and/or attributes that are outside the scope of the practices.

In doing so, the Best Practices seek to preclude scenarios that could lead to gross overuse of digital identity and/or activities with regard to VDCs that could erode the ability to be anonymous or pseudonymous for many online interactions or otherwise cause harm.

Note that this initial release of Best Practices is a starting point to try to move the VDC ecosystem forward in a way that improves security, privacy, usability, and inclusivity for everybody. We expect to iterate on the Best Practices as we get feedback and lessons learned from those implementing VDCs, and new issues that were not anticipated emerge.

Scope

The Best Practices are initially aimed at issuers, digital wallet providers (also known as credential manager providers) and online service providers (also known as verifiers) that will ask consumers to share validated identity data from their VDCs. It is also aimed at other organizations such as vendors that play a role in verifying and validating identity for online service providers using government-issued VDCs.

In addition, the Appendix of this document provides additional recommendations to online service providers around their use of VDCs, focusing on both collection of VDC data and use of that data.

It is expected that verifiers who choose to adopt the Best Practices will be organizations specifically called out in the use cases in Section VIII; and in adopting the Best Practices, they will be pledging to use VDCs in accordance with the terms outlined in the use cases. Verifiers can self-select into the use cases that are most appropriate to their business or mission.

Likewise, this initial version of the Best Practices focuses solely on laying out recommended policies to govern use of VDCs. As such, it does not include any provisions to certify that organizations who have pledged to follow the Best Practices are actually doing so, nor does it address issues around technical infrastructure that could be used to enforce the Best Practices, such as a way for wallet providers to grant or revoke access tokens to online service providers seeking to access VDC data stored in those wallets. However, it is possible that future iterations or versions of these Best Practices might address these

issues, or that other organizations will seek to launch certification programs or technical infrastructure to complement and support the Best Practices.

How these Best Practices were Developed

The Better Identity Coalition convened a workshop in Q1 2025 to discuss emerging concerns about potential overuse of VDCs, explore potential ways to address those concerns, and discuss whether there might be stakeholder interest in a potential third party, voluntary Code of Conduct as one way to address them. The event was conducted under the Chatham House Rule and included about 60 attendees who came from a mix of privacy and civil liberties advocates, consumer advocates, digital wallet providers, other vendors in the digital identity market, and major relying parties from financial services, retail, and health care. The event also included government officials.

At the workshop, attendees reached a consensus that:

- Some sort of "rules of the road" are needed as digital counterparts to government-issued identity credentials roll out.
- In the U.S., government is not likely to create these rules any time soon.
- It would probably be helpful for a third party to create a Code of Conduct or set of Best Practices that could fill this gap.

The workshop did not explore:

- What would go into the Code (i.e., what use cases would be permitted or forbidden)
- How it would be enforced
- Who would develop and run it

Following the workshop, the Better Identity Coalition convened a small working group with representatives from wallet providers, privacy and civil liberties groups, issuers, and relying parties. Based on their inputs, Coalition staff drafted a strawman which was released in Q4 2025 for public consideration and feedback.

A few core themes emerged in the feedback to the strawman:

- First, while some stakeholders were more enthusiastic than others, everybody generally thought that some sort of "rules of the road" would be helpful to promoting an ecosystem for VDCs that mitigates the risks involved with new government digital credentials while ensuring that the benefits of improved security, privacy, usability, and inclusivity are fully realized.
- Second, many stakeholders thought the strawman's primary focus on wallet providers was too narrow. Commenters thought that ideally, the strawman should also focus on two other sets of stakeholders:
    - Issuers (i.e., state governments) – with some arguing that issuers of credentials should have a say (if not the say) in how the credentials they issue are used.

  - Verifiers (i.e., relying parties), who are ultimately the entities that will be making the request for credentials.

- Third, some stakeholders suggested that individuals should not be banned from choosing to share identity data from their VDC if they wanted to do so – and were uncomfortable with a policy that might expressly seek to keep an individual from sharing their data – especially since issuers do not generally restrict individuals from deciding to share their physical credential. With this, some noted that there is a difference between precluding an individual from sharing their data and precluding a verifier from requesting it; there was more comfort around the latter concept, particularly because some state governments today restrict some parties from scanning the barcode on a physical credential.

- Fourth, some stakeholders argued that a code of conduct would not be meaningful if there was no way to enforce the code, and suggested that the term "code of conduct" might not be appropriate for a set of rules without a clear enforcement mechanism.

- Finally – to the point above – some issuers noted they were not comfortable with a third-party organization trying to make these decisions, and with this, other organizations such as wallet providers expressed concern that if issuers fought back against this effort, we would lose consensus for action.

As a result of this input, Better Identity Coalition decided to pivot from a formal "Code of Conduct" to a set of "Best Practices" that focuses less on setting formal, binding rules and more on outlining guidance and best practices around appropriate and inappropriate requests for identity data from VDCs.

The primary driver behind this shift was to ensure we published a document that could be supported by a wide variety of stakeholders in the VDC ecosystem.

Note that at some point if industry and government consensus for the ideas in these Best Practices grows stronger, we may seek to evolve the Best Practices into the formal self-regulatory Code that was first envisioned.

Ownership and Maintenance of Best Practices

The Better Identity Coalition will retain ownership of the Best Practices. As feedback on the quality and effectiveness of the Best Practices emerges, the Better Identity Coalition will consider revising them to address this feedback and improve the Best Practices going forward.

Individuals and organizations that would like to request the addition of new use cases and associated data bundles – or changes to existing ones – can make a formal request by filling out the form at https://www.betteridentity.org/key-initiatives/best-practices. The Coalition will consider the merits of each request and publish updates to the Best Practices and associated use cases every 6 months.

Target Scope and Application

1. This document details a set of voluntary Best Practices, and as such, they are open to any entity that wishes (and considers the Best Practices relevant to its business or operations) to implement and adhere to. Organizations may choose to publicly commit to adherence to the Best Practices, and outline how the Best Practices apply to that entity and its operations.

2. Enforcement (in terms of using the Best Practices to restrict certain requests for identity or validated attributes) is up to the discretion of the entity who has pledged to follow them.

3. At present time, there is no certification of entities that pledge to adhere to the Best Practices– though we or another party may choose to create such a program in future years.

4. At present time, there is no technical infrastructure built to support implementation of the Best Practices (for example, a way to provision access keys to relying parties who want to access digital credentials for a purpose that is allowed under the code) – though we or another party may choose to create such a program in future years.

Terminology and Definitions

Below is a list of commonly used terminology and definitions.

1. Attribute - An attribute - sometimes known as a claim - is a quality or characteristic ascribed to someone or something. An identity attribute is an attribute about the identity of a subscriber (e.g., name, date of birth, address).

2. Credential Manager - An application, hardware device, or service which securely stores, organizes, manages, and enables presentation of VDCs. Digital wallets, state mDL apps, password managers, and passkey managers are examples of credential managers.

3. Digital Wallet - A type of credential manager which typically holds VDCs and other digital representations of physical world objects

4. Identity Proofing - The processes used to collect, validate, and verify information about a subject to establish assurance in the subject's claimed identity.

5. Holder - The individual possessing the wallet and/or VDCs. This individual is typically the subject of the credential (aka, the person to whom the VDC was issued).

6. Issuer - The entity that issues a VDC\- for example, a state motor vehicle department for a driver's license, or the Social Security Administration for the SSN.

7. Validated Attribute - An identity attribute can be said to have been "validated" if an organization has gone through a process or act of confirming that a set of attributes are authentic, accurate and associated with a real-life identity.

8. Verifiable Digital Credential (VDC) - A cryptographically verifiable, tamper-evident assertion of claims about a subject, signed by an Issuer. VDCs are stored in a credential manager.

9. Verifier - The entity that cryptographically validates the authenticity and integrity of a VDC. A verifier is typically, but not always, the relying party - also known as an online service provider.

10. Verifier Service - The underlying platform or infrastructure service which enables a Verifier to validate a VDC. In many cases, a verifier service will be a product offered by a digital identity vendor who helps verifiers integrate with different VDCs. Companies that provide that tool are called Verifier Service Providers.

Principles

1. The emergence of VDCs should not materially impact the ability of individuals to be anonymous or pseudonymous online.

2. VDC's have been designed specifically to preserve and enhance privacy, with the ability for a verifier to ask an individual to share only a limited subset of their identity information and do so in a way that does not allow any party to track how or where an individual uses their VDC. Issuers, digital wallet providers, verifiers, verifier service providers, and others in the digital identity ecosystem should design and use VDCs only in ways that embrace these features, with a focus on solutions that minimize the amount of data an individual is asked to present in online transactions.

3. There are a number of use cases where online service providers have a legal or regulatory requirement to collect and validate data on an individual's identity – either a full credential, or sometimes a subset of attributes associated with that credential – and use of a VDC for these purposes should be explicitly permitted, provided that the request is for a subset of identity data directly relevant to the requirement.

    - For example, a bank is legally required to obtain the name, date of birth, address, and taxpayer identification number (TIN) from customers opening new accounts.

4. There are a number of use cases where there is no legal or regulatory requirement to collect and validate data on an individual's identity, but where:

    - The risk model is such that service providers do not make a product or service available online because there is a security or business need for that provider to validate an individual's identity or an attribute tied to that identity, and

    - Most consumers would want the ability to access that product and service in a fully online environment and would welcome the ability to do so rather than have to present their ID in person.

    Use of a VDC for these purposes should be permitted, provided that:

    - The request is only for a subset of identity data directly relevant to the requirement or transaction.

    - Use of a VDC allows a consumer to do something online that they would otherwise not be able to do without presenting their ID in person or validating a subset of their identity data through another solution online.

- For example, an individual may wish to have a fully digital check-in experience at a hotel – including getting a digital key provisioned to their smartphone – but may be required by the hotel to first present their ID at the front desk before receiving a room key as part of the hotel's security protocols, which provide a level of physical safety assurance to hotel staff and guests. We detail more of these use cases in Section VIII.

5. In the above categories of use cases, the fact that an online service provider has a legal, regulatory, or business requirement to collect identity data for one use case should not serve as license to collect identity data for every use case. And user consent for an online service provider to collect identity data for one use case should not be interpreted as having granted consent for every use case.

    - For example, while a bank has a legal and regulatory requirement to collect identity data for an individual seeking to open an account – and should be permitted to leverage VDCs to do so – that bank should not request VDC data from an individual visiting its website to browse products or services. Nor should a hotel request identity data from an individual who is simply visiting its website to browse its rooms or facilities.

    - Verifiers should avoid uses cases that try to "induce disclosure" – which is defined by the National Institute of Standards and Technology (NIST) as a situation where "individuals feel compelled to provide information disproportionate to the purpose or outcome of the transaction."[1] Per NIST, "Induced disclosure can include leveraging access or rights to an essential (or perceived essential) service. It can lead to problems such as discrimination, loss of trust, or loss of autonomy."

6. There are potential use cases where online service providers have no legal or regulatory requirement to collect and validate data on an individual's identity, and where collecting identity information would not enable a service provider to make a product or service available online that would not otherwise be available. Use of a VDC for these purposes should be restricted.

    - For example, an online service provider should not collect identity information from a VDC to be used solely for marketing purposes, or as a tool to track consumer behavior online.

Use Cases and Associated Rules

In line with the six principles outlined above, the Best Practices defines three categories of use cases:

1. Use cases where online service providers have a legal or regulatory requirement to collect and validate data on an individual's identity – either a full credential, or sometimes a subset of attributes associated with that credential – and use of a VDC for these purposes should be explicitly permitted, provided that the request is for a subset of identity data directly relevant to the requirement.

[1] See https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md

2. Use cases where there is no legal or regulatory requirement to collect and validate data on an individual's identity, but in line with principle 4:

    a. Organizations have historically required some proof of identity in person, or

    b. Use of a VDC would allow a consumer to do something online that they would otherwise not be able to do today without presenting their ID in person or validating a subset of their identity data through another solution online.

3. Use cases that should be restricted, given that there is no legal or regulatory requirement to collect and validate identity data, nor is there any significant risk-based justification or business case to collect VDC data.

In line with the Best Practice's principles, here are the rules that apply to the following use cases in each of these categories:

Use cases tied to a legal or regulatory requirement

Financial Services		
Use Case	Data Permitted to be Collected	Notes
New account opening (CIP/KYC)	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	The five use cases here were all taken from the use cases defined by NIST in their NCCoE mDL Project. SSN and TIN are not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)
Setting up online access after an application is approved	Same as above	
Instant approval (when CIP/KYC is fast tracked)	Same as above	
Preventing unauthorized high-risk transactions	Same as above	
Account recovery (if a password or other authenticator is lost)	Name DOB Address SSN or TIN Issuer of ID (i.e., what agency)	

Health Care		
Use Case	*Data Permitted to be Collected*	*Notes*
Register for new patient portal	Name DOB	SSN and TIN are not available through a state mDL, but might be

	Address SSN or TIN Issuer of ID (i.e., what agency) Sex	available through other VDCs yet to be created (i.e., a digital SSN card) In some health use cases, sex is a required attribute
Telehealth ID verification	Name DOB Address SSN or TIN Issuer of ID (i.e., what agency)	
E-Prescribe of controlled substances for health providers	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	
Pick-up of prescriptions that are controlled substances	Name DOB Address Issuer of ID (i.e., what agency)	
Account recovery (if a password or other authenticator is lost)	Name DOB Address SSN or TIN Issuer of ID (i.e., what agency)	

Government Services and Benefits		
Use Case	*Data Permitted to be Collected*	*Notes*
New account opening – applying for benefits	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN and TIN are not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)
New account opening – proving identity to set up an account at an e-government portal	Name DOB Address SSN or TIN ID number	

	ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	
Account recovery (if a password or other authenticator is lost)	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	

Employment		
Use Case	*Data Permitted to be Collected*	*Notes*
New hire: Proving identity for I-9 compliance purposes	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN and TIN are not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)
New hire: Background check associated with a new hire	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	
Account recovery (if a password or other authenticator is lost).	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	

Age-restricted products and services		
Use Case	*Data Permitted to be Collected*	*Notes*
Age verification	DOB - or preferably, “Over a certain age” ID Expiration Date Photo (if needed for comparison)	Attribute requirements may vary across laws and regulations dealing with different age-related use cases; they also may vary state to state

Vehicle Rental		
Use Case	*Data Permitted to be Collected*	*Notes*
Validation of ID and Driver’s License at Pickup	Name DOB Address ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	

Use cases tied to a business or risk requirement

Hotels/Hospitality		
Use Case	*Data Permitted to be Collected*	*Notes*
Mobile Check-in without needing to visit the front desk	Name DOB Address Issuer of ID (i.e., what agency)	

Education		
Use Case	*Data Permitted to be Collected*	*Notes*
Remote student enrollment	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN and TIN are not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)

Building Visitor Access		
Use Case	*Data Permitted to be Collected*	*Notes*
Mobile Check-in without needing to visit the front desk	Name	

Ticketing (in Entertainment)		
Use Case	*Data Permitted to be Collected*	*Notes*
ID Verification for secure ticket transfers	Name DOB Address ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	

Background Checks		
Use Case	*Data Permitted to be Collected*	*Notes*
ID Validation for background check associated with position of trust	Name DOB Address SSN or TIN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN and TIN are not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)

Account Recovery for Non-Regulated Use Cases		
Use Case	*Data Permitted to be Collected*	*Notes*
Account recovery (if a password or other authenticator is lost).	Name DOB Address	While VDCs should not be collected to set up accounts in the majority of non-regulated use cases, validated attributes from VDCs may be used by verifiers to match with data on file from customers as a “strong signal” to support account recovery for non-regulated use cases. For examples, many retailers will have a customer’s home address and may also have their data of birth; cryptographic validation of those attributes from a VDC can help to support account recovery.

Use cases that are restricted

- Identity and/or age verification to deliver targeted advertising.
- Identity verification used similar to a cookie to track online behavior.

On this last point – one step wallets should take to preclude use of a VDC to track online behavior is to issue a new mobile security object (MSO) (as defined in ISO 18013-5) for each use case, or over a specific period of time. This step can help to address the risk that a VDC could be used to corroborate user behavior across different sites.

Appendix: Additional best practices for verifiers/relying parties

Verifiers making use of government-issued VDCs should use both the IDs and the data contained in them responsibly. Below are some additional best practices that verifiers should embrace by in their use of government VDCs.

- Data minimization: Verifiers shall collect only the minimum data necessary for a transaction.
- Purpose specification and transparency: Verifiers shall clearly explain to users what information is being requested, why it is needed, how it is being used, and how long it will be retained.
- Purpose limitation: Data collected for a transaction shall not be used for any other purpose outside of stated transaction, i.e., information from making a physician's appointment should not be sold to pharmaceutical companies.
- No sharing or selling: Verifiers shall not sell or share data from VDCs with any other organization, except as required by law.
- No tracking: Verifiers shall not use VDCs to track individual behavior on their site or service, or across other sites or services.
- Right to Delete/Correct Data: Individuals should have the ability to delete or correct their data.
- Right to an Alternative Path: Individuals shall not be forced to use a VDC to create an account and alternatives shall be made available, including in person or other options.
- No use of government-issued VDCs as an authenticator: While government-issued VDCs will play a critical role in many identity applications, they are poorly suited for use as an authenticator. Verifiers should use passkeys or other authentication technologies, rather than link authentication to government-issued key material.