State-Endorsed Digital Identity
Request for Information
by the Utah Department of Government Operations

Submitted to: Aimee Ellliott, amelliott@utah.gov

Reply from the Open ID Foundation

Table of Contents

I. Overview

The OIDF welcomes the opportunity to comment on the Utah SEDI RFI. These comments reflect general considerations of the OIDF based on our experience supporting US and global implementers who are considering or have already selected our specifications. We have made best efforts to tailor our comments to your SEDI RFI and context, but we may well be missing context specific to Utah. If desired, we would be happy to discuss our comments and support your due diligence in the weeks and months ahead. You can reach us at director@oidf.org to arrange a meeting. Of course we also warmly welcome Utah direct participation, contribution and feedback to our Work Groups, and Community Groups if our work could or will support your roadmap.

The OpenID Foundation (OIDF) is a non-profit, global open standards body committed to helping people assert their identity wherever they choose. Founded in 2007, we are a community of technical experts leading the creation of open identity standards that are secure, interoperable, and privacy preserving. The Foundation's various families of standards are used today by billions of people across millions of applications. Today, the OpenID Foundation's standards are the connective tissue to enable people to assert their identity and access their data at scale, the scale of the internet, enabling "networks of networks" to interoperate globally. Individuals, companies, governments and non-profits are encouraged to contribute to the Work Groups and participate in the Community Groups, and there is no fee to contribute, access, or utilize the Foundations specifications or open source tests. Membership empowers voting on specifications and discounts on self-certification. Membership fees are just $50 for individuals, and individuals have the same voting rights as the largest corporate and government members. The OIDF has a sustainable operating model where we receive ~40% of our revenue from voluntary memberships (400+ members), ~50% revenue from self-certification which is optional for implementers, and 5-10% revenue from member-directed funds used to accelerate projects that benefit to OIDF community (e.g. formal security analysis, open source test development, and interoperability events). You can learn more about the OpenID Foundation at openid.net.

In the last five years, one of the OIDF's families of specifications, FAPI, has become the standard of choice for Open Banking and Open Data implementations, allowing people to access and share data across entities using a highly secure communications protocol. This spring, the US Financial Data Exchange officially selected FAPI for their "blue" profile which can be used by users to give consent for their data to be shared from their data holder (e.g. bank or FI like JPMC or Paypal) to another entity like a FinTech (e.g. TuboTax used by ~50%+ Americans). Since FAPI was introduced, several other jurisdictions have selected it including UK Open Banking, Brazil Open Finance, Brazil Open Insurance, Australian Data Standards Body for Open Data, ConnectID (Australia), and the Chilean Monetary Authority. Furthermore, Norway's HelseID national e-health system deployed FAPI 2.0 to exchange health data across the national healthcare network, treating health records with bank-level security. Beyond the ability to achieve security, interoperability and scale across ecosystems by default, many public and private sector-led ecosystems choose FAPI because the Foundation adheres to the best practices for standards development and maintenance as defined by the WTO (e.g. consensus, transparency), and our specifications go through extensive, formal mathematical security analysis to ensure the security posture is well understood before they are taken to Final.

Most recently, the OIDF's Digital Credentials Protocols Work Group have seen adoption at global scale of the OpenID for Verifiable Credentials (OpenID4VC) family of protocols that includes OpenID for Verifiable Presentation 1.0,, OpenID for Verifiable Credential Issuance 1.0, the High Assurance Interoperability Profile

(draft, near final), and DCQL for specific sets of data a user will authorize for release. These specifications are compatible with SEDI policy requirements, a key theme on which we will elaborate on in more detail in this document. In the US, private sector implementers of OpenID4VP/VCI include Google Wallet, Samsung Wallet, Amazon, and 1Password who jointly announced their acceptance of the specifications in the Google Blog post April 30th. Several of these entities joined other global implementers in the May 5th public interop of OpenID4VP and the DCP WG interop of OpenID4VCI where the specs were proven out as interoperability before both specs moved to Final this year. These announcements indicate clear US private sector support for the OpenID4VP 1.0 and OpenID4VCI 1.0 specifications. Like FAPI before them, these specifications have also been through several phases of formal security analysis by the University of Stuttgart.

In terms of government adoption of OpenID4VP/ OpenID4VCI, first it is worth noting that any of the 18 US states issuing mDLs that support Google Wallet and Samsung Wallet, will also support the OpenID4VP specification through the architecture selected by these wallets to enable online presentation. We also hope to see other major digital platforms like Apple Wallet follow suit in the near future, further extending the reach of state-issuers and their ability to leverage OpenID4VP and averting redundancy in the build relying parties will need to do. In fact, Apple has been an active contributor to the OpenID4VP, OpenID4VCI, and HAIP specs via the DCP WG for 18+months, and in other standards forums to support the interoperability of the specs that move to Final. The California DMV offers its own CA DMV Wallet to Californian residents, and the CA DMV has deployed OpenID4VCI and OpenID4VP since its launch. The CA DMV enables many relying party use cases for the CA DMV itself (e.g. login and access to disable placards) and for private sector use cases (e.g. proof of age for alcohol purchase). It is also worth noting that the CA DMV issues its credentials using OpenID4VCI, which are accepted by TSA and DHS in line with the mdoc specifications accepted for travel through US TSA security checkpoints. The CA DMV has also sought to support public and private sector adoption of standards with the CA DMV and OIDF cohosted hackathons in October and November of 2024, in which large financial institutions, social businesses, many branches of California and federal government stakeholders took part, and 5 other countries attended as observers (Mexico, Germany, Italy, Japan, Taiwan).

NIST National Cybersecurity Center of Excellence (NCCoE) for digital identities has also selected OpenID4VP to support the “open a bank account” use case, work completed in partnership with US State issuers (e.g. California, Maryland, Georgia), digital platforms (e.g. Google, Microsoft), and US Banks/FIs (e.g. JPMC, Wells Fargo, Navy Federal Credit Union, PNC, Raymond James, Bank One, Cap One). This thorough project conducted over a year of weekly consultation delivered a UX front end for a mock NIST NCCoE bank and a back end capable of consuming mdoc credentials from numerous wallets concurrently. This NIST project affirmed that mdocs/mDLs are compliant with CIP regulatory requirements like CIP. However, beyond baseline compliance, it also surfaced FI requirements that if met could substantially raise the confidence of FIs in the credentials and accelerate their adoption nationwide. The gaps and requirements are recapped in this NIST report Septemebr 2025: https://pages.nist.gov/nccoe-mdl-project-static-website/building_mdl_assurance/building_mdl_assurance.html. As a CRADA participant in the NCCoE, the OIDF is working in partnership with NIST to document the requirements and author a potential metadata schema that US issuing authorities could integrate into the credentials they issue to close the gaps identified by FIs. The report draft is with the eKYC & IDA WG for comment now and will be released on Openid.net in mid-October. The OIDF’s eKYC & IDA WG will likely progress the recommendations in the report in partnership with the NIST NCCoE, and the OIDF Board is considering expanding this report to encompass non-US Financial institution requirements as a next phase of work.

Outside of the US, other governments and private sector entities are also rapidly adopting OpenID4VP/VCI. One reason the OpenID4VC family of specifications appeal to government decisionmakers, is that the specs offer governments domestic sovereignty in selecting and configuring the protocol to their ecosystem

requirements. For example, the protocol offers the flexibility to support different credential types allowing for presentation across platform, across device and across countries. For example, the protocols support data formats such as mobile documents ("mdocs") from ISO/IEC 18013-5, Selective Disclosure JSON Web Tokens (SD-JWTs) from the IETF and VCs from the W3C. The most widely known adopter of OpenID4VC specifications is the European Union Digital Identity Wallet (EUDIW) initiative which encompasses all 27 member states which must issue credentials compliant with OpenID4VP/VCI specifications by the end of 2026 and all EU financial institutions must be prepared to accept the EUDIW by the end of 2027. Furthermore, the Swiss government wallet project includes OpenID4VP/VCI in its architecture, OpenID4VP/VCI are underway for adoption by the Western Balkan countries by the end of 2027 so their residents and businesses can interoperate with Europe. We have also seen support of OpenID4VP by the Japanese Digital Agency Pilot with Japan Railways for student benefits, and OpenID4VP/VCI is expected to be deployed by the Taiwanese government as per a recent presentation to that effect. Other countries have indicated to OIDF that they have selected OpenID4VP/VCI but it is not yet public information, and yet more are evaluating its fit within their policies and roadmaps - similar to the journey Utah is on now.

It is worth highlighting that work on the OpenID4VP/VCI/ HAIP specifications has progressed under formal liaisons, MOUs and membership agreements with peer Standards Development Organizations including the W3C, IETF, FIDO, ISO, the Cloud Signature Consortium and government standards bodies like NIST and ETSI. The OIDF seeks to ensure our specifications are interoperable with peer SDOs specs, especially where they are layered together to support implementers and ecosystems. For example, the ISO working group implementing online usage of mDLs as ISO/IEC 18013-7 has further included OpenID4VP as an implementation option as part of the drafts of Annex B and Annex D, adding new privacy features in addition to improving interoperability for implementers that select these annexes.

State exemplars and what Utah can re-use:

- **California (DMV Wallet / IDs in Wallet):** California's mDL program now supports digital IDs in state and commercial wallets and is expanding online use. While California websites only describe the mDL roadmap at a high level, the remote verification profile they are moving toward is the ISO/IEC 18013-7 flow,i.e., an OpenID4VP-based presentation for online use. Utah can consider mirroring California's approach: adopting ISO/IEC 18013-5/-7 + OpenID4VP, require conformance testing, and publish verifier policy profiles to standardize what is asked and disclosed.

- **European Union Digital Identity Wallet (EUDI Wallet):** The European Union is implementing a EU-wide federated model of national digital identity wallets, built on eIDAS 2.0 and the European Digital Identity Framework. The EUDI architecture aligns closely with the same core standards selected by California DMV, using ISO/IEC 18013-5/-7 for mDL interoperability and integrating OpenID4VP and OpenID for Verifiable Credential Issuance (OpenID4VCI) for presentation and issuance. Both jurisdictions utilize ISO mdocs for driving license use cases. In the US, states are also using mdocs for every-day use cases while Europe is leaning towards the use of SD-JWTs for non-driving license use cases, at least in part so they can help relyin parties adopt the technology more easily. The EU Architecture Reference Framework and wider design demonstrates how multi-jurisdictional interoperability, cross-sector credential acceptance, and robust user consent management can coexist within a standards-based ecosystem. Beyond the architecture of the ARF, Utah may want to consider the EUDI governance model for insights on credential assurance levels, trust lists, and interoperability

frameworks that allow residents to use state credentials seamlessly across both public and private domains.

- **Google Wallet:** Google's digital identity integrations, including mobile driver's licenses and verifiable credentials, leverage ISO/IEC 18013-5 and support OpenID4VP and HAIP for remote presentation. By building on open standards, Google Wallet enables state-issued IDs to function consistently across Android devices and web contexts, preserving privacy while simplifying user experience. If Utah followed a path consistent with California DMV, EU ARF, and Google Wallet (and the others mentioned here) it can benefit from aligning with the same interoperability standards, ensuring SEDI credentials can be recognized by major wallet platforms while maintaining user control and minimizing proprietary dependencies.

- **OpenWallet Foundation (Multipaz):** The OpenWallet Foundation (OWF) is developing open-source wallet frameworks — including Multipaz, a reference implementation that supports OpenID4VP, OpenID4VCI, HAIP, and ISO/IEC 18013-7 profiles. OWF's goal is to prevent fragmentation by enabling governments, enterprises, and vendors to build interoperable wallets that adhere to shared standards and enable access to open source code, and avert the dependencies and fragmentation that can arise with the use of proprietary APIs. Utah can re-use the freely available, open source code components hosted by the OWF to accelerate development, and ensure long-term sustainability through participation in an open, global community. When open source code is used in conjunction with open standards like OpenID4VP/OpenID4VCI and open source test suites, the barrier to entry and the assurance of code and platform security levels up across all implementers while distributing the maintenance costs.

OIDF best-practice package to adopt "as is":

1. **Standards set:** OpenID4VP 1.0 for online presentation using HAIP + OpenID4VCI 1.0 + HAIP for issuance; pair with ISO/IEC 18013-5/-7 and allow W3C VC and SD-JWT VC formats to ensure portability. These specifications are already final or moving to Work Group final call so they can be voted as final this quarter. Beyond spec development, OIDF specs are actively maintained by the WG to ensure their alignment with ecosystem and implementer requirements over time. Beyond OpenID4VC family of specs, Utah may also want to consider OpenID for Identity Assurance 1.0 for standardised assurance metadata. This family of specifications hosted by the eKYC & IDA WG are the specs that NIST and OIDF intend to extend in order to close the gaps identified by US FIs and NIST as part of the NIST NCCoE mDL/ Digital Identity project.

2. **Interoperability:** Utah can consider aligning with proven, NIST NCCoE hosted interop patterns (e.g., mDL "open a bank account" architecture using OpenID4VP + HAIP + DCQL). If Utah were to select OpenID4VP + HAIP + DCQL and follow the path matured by the NIST NCCoE project, then Utah residents can benefit from a fast track to use of their Utah issued credentials in federally regulated contexts. As mentioned in the introduction, NIST/ OIDF conducted a series of interips this year to prove out the specifications while assessing the requirements and fit of mDL/mdoc technologies with US major financial institutions. Given there are 10,000+ banks in the US, and Utah residents will use a wide range of financial service providers, leveraging existing interoperability patterns can help unlock financial sector use cases for Utah residents and businesses. If Utah were to select an architecture that deviated substantially from the NIST NCCoE approach, it could lead to slower adoption by US FIs who may need to re-evaluate a new architecture.

3. **Open Source tests and Self-Certification.** If Utah were to select OIDF specs, Utah could consider voluntarily or even requiring ecosystem participants leverage open source tests that also align with NIST NCCoE interop patterns (e.g., mDL “open a bank account” architecture using OpenID4VP + HAIP + DCQL).All OIDF open source test suites can be used locally or run from OIDF website, allowing implements to “build to the tests” and achieve conformance to the specs in so doing - all at no cost. For example, open source tests for OpenID4VP and OpenID4VCI used by implementers for the interops in 2025 are freely available at https://openid.net/how-to-certify-your-implementation/. Implementers that wish to self certify, will be able to do so later in 2025 when the tests are published and OIDF will review implementer test results and publish the results online (for modest fees). The OIDF offers open source tests and low cost conformance to support the wider mission and vision of the foundation and ensure implementers are able to realize the security, interoperability, scale and privacy-preserving features inherent to the specs. In 2H 2026 OIDF will expand conformance services to include an accreditation model we expect to resonate with accreditation labs and “managing entities” that are private or public sector led.

4. **Verifier policy & registration:** Utah can consider publishing verifier metadata and policy profiles (what claims, for which purpose, with what legal basis), and certify wallets/verifiers against those profiles to enforce least disclosure and unlinkability—an RFI priority.

5. **Open, inspectable protocols:** Utah’s RFI stresses open, non-surveillance tech and interoperability. Adopting OpenID4VP/18013-7 with Annex D (OpenID4VP + HAIP) meets those criteria and keeps Utah aligned with private sector adopters and other jurisdictions adopting the same specifications. OIDF specifications are open standards, freely available to everyone. To support our liaisons with ISO and ITU, OIDF also has a standing practice of submitting our final specifications for consideration by ISO as “publicly available specifications” and to ITU-T for Q10 recognition. In 2024 OpenID Connect has been approved for ISO PAS and ITU-TQ10 status achieved in 2025. Both OpenID for Identity Assurance and FAPI 1.0 have passed the ISO ballot and have ISO numbers assigned, so when comments from member states are conformed by OIDF, these two specs families will also be published as ISO Publicly Available Specifications. FAPI 2.0 was submitted to ISO for PAS status and it is in ballot now with member states concluding their vote in December 2024. Other OIDF specs like OpenID4VP, OpenID4VCI, HAIP, and Shared Signals will also follow this procedure. When these specs are recognized by ISO, they are made available by ISO for no fee (as opposed to the fee to publish each spec that would apply to specs developed within ISO WGs) and when specs are recognised by ITU-T they are translated into 5 other languages to support global adoption.

6. **Security collaboration.** By working closely together, ecosystems and implementers can support each other, and offer a more robust identity infrastructure more resilient to attack. Most security concerns are actively discussed in Work Group meetings, and are assessed proactively with formal security analysis. Even then, security vulnerabilities could arise that creates risks for existing implementers. For example, OIDF communicated a Responsible Disclosure notice to ecosystems and IETF ahead of public disclosure to the WGs, to ensure ecosystems live using the impacgted OIDF and IETF specifications had a narrow window to proactively remediate any gaps in their deployments before bad actors might hear about the vulnerabilities in public working group meetings or in documents open to the public. In this case, the probability was very narrow that an attack could or would be pursued by a bad actor, however all ecosystems briefed took the disclosure very seriously as the situation merited. Since OIDF does not know which entities select our open standards, OIDF was able to leverage the relationships established with public and private sector ecosystems, including those that had utilized the self-certification service, to engage the subject experts in each organization in a timely

manner…and then coordinate with IETF and OIDF WG Cochairs to ensure the gaps were closed in the specifications in a timely manner as well.

7. **Ecosystem Best Practices.** Many public and private sector ecosystems are joining the new OIDF Ecosystem Support Community Group to refine or develop their roadmaps for open data and digital identity. This forum empowers decision makers to engage directly with each other to develop their architecture and roadmaps pre-launch, and then refine and maintain them post launch. Ecosystem decision makers and implementers (those with responsibility for the critical infrastructure) are a relatively limited pool of subject matter experts. This Community group can act as one of the safe-spaces to mature thinking on architecture, spec configuration and trade-offs in security and privacy decisions as they arise - issues that are critical for decision makers but which fall outside the scope of work groups and public conferences. The challenge facing any ecosystem decision makers does not end with launch, on the contrary, it is an ongoing journey and one that is likely to continually evolve in the months and years ahead.

II. Legal, Regulatory, and Policy Considerations

1. How can the state ensure compliance with relevant privacy laws and regulations (e.g. the Government Data Privacy Act and the Utah Consumer Privacy Act in the context of a SEDI program?

OIDF recommends building privacy into the system by design and not relying only on policy. If Utah selects open interfaces like OpenID for Verifiable Presentations (OpenID4VP) and OpenID for Verifiable Credential Issuance (OpenID4VCI) then the protocols can be leveraged to support selective disclosure (share only what's needed), pairwise identifiers (a different ID per verifier to prevent tracking), and no "phone-home" wallet behavior (without user informed consent or anonymized metrics for limited security functions) . Utah has the ability to combine these technical safeguards with legal controls such as clear purpose limitation, short data-retention periods, Data Protection Impact Assessments, and certification of wallets and verifiers to Utah's privacy rules.

2. eWhat legal considerations are relevant to the liability and responsibility of the state, Digital Wallet Providers, Verifiers, and Holders within the SEDI ecosystem?

The state has the opportunity to define roles clearly in law so that responsibility and liability are balanced across the ecosystem. The state's may wish to take on the responsibility to operate the trust framework, oversee conformance, and revoke endorsements only in limited, clearly defined circumstances—this ensures stability and predictability. In that context there may be obligations at the state level for Digital Wallet Providers to safeguard cryptographic keys, comply with conformance requirements, avoid collecting metadata, and honor user consent; these duties are part of protecting individuals from exploitation and preserving trust in the system. The State may also consider how Verifiers are restricted to requesting only the minimum necessary data and must follow strict limits on retention and use, ensuring proportionality and preventing function creep. Holders retain control of their data and should not be held liable for how verifiers misuse information, which reinforces fairness. Contracts across the ecosystem should include audit rights, breach notification, and indemnification, and may reference international profiles such as OpenID for Identity Assurance (eKYC & IDA) to align with best practices.

The OIDF is aware and acknowledges that some of these requirements are met by the DHS/TSA for TSA related use cases, by AAMVA's the Implementation Guidelines and DTS to support issuer obligations, and that FIDO is considering requirements that digital Wallets might voluntarily adhere to. However, at the moment of providing this RFI, OIDF also acknowledges that there are gaps in liability and privacy in the US context.

Although OIDF is not a governance entity and would not operate an ecosystem, OIDF does currently and will continue to make all best efforts to support ecosystems considering or ecosystems that select our specifications. For example, as mentioned in the introduction, the OIDF is introducing an accreditation service to support accredited labs and managing entities (both state led and private sector led) that wish to ensure that their ecosystems accurately deploy OIDF specifications and open source tests. To that end, OIDF intends to expand the current self-certification service, and pilot this accreditation model over the next 6 months to launch this new capability for ecosystems in 1H 2026. If Utah RFI does lead to the selection of OIDF specifications, we are happy to explore what Utah might require to support your community.

3. Should the state legislate any aspects of the relationship between Digital Wallet Providers and Holders? If so, what should be included in law?

Yes, Utah may want to consider legislative measures. Utah may want to legislate certain aspects of the wallet–holder relationship to protect individual rights and foster trust, as we have observed in other ecosystems. For example:

- Informed and revocable consent is essential so people retain control over when and how their credentials are shared.
- Preventing surveillance and monetization of metadata ensures wallets do not become tools for tracking or profiling users.
- Portability (export/migrate credentials between certified wallets) between certified wallets protects against lock-in and supports competition and user choice.
- Setting minimum security requirements (e.g., hardware-backed keys where available) reduces risks of fraud and identity theft
- Honest and accessible interfaces help people make decisions without being manipulated.
- Clear recovery options are needed, but without escrowed keys, so that control stays with the holder.
- Finally, a simple dispute-resolution process strengthens accountability and ensures users have a fair path to address issues.

The OIDF acknowledges that Utah is both a thought leader in privacy and digital identity so some policies may be natural to be state-led policy decisions. However Utah residents and businesses also operate in a wider US context (in which cross-state use cases and federal regulations apply in some use cases) and Utah operates in a wider global context as well. If Utah were to select policies that served Utah residents in businesses within Utah, but which limited the ability of residents and businesses to interoperate more widely in the US or Global contexts that could limit the adoption of Utah's digital identity capabilities.

4. What aspects of identity should be included and endorsed in a SEDI?

From our experience, a state-endorsed digital identity typically includes only the core attributes necessary to establish a person's legal identity, while leaving room for selective, privacy-preserving use. This means anchoring the SEDI to verified attributes such as legal name, date of birth, residency status, and a unique state identifier. These are foundational for proving identity and meeting regulatory requirements.

We see other attributes treated differently in different jurisdictions. Some jurisdictions include address in the mdoc. In Utah, you might prefer to have other attributes—like address, contact details, or eligibility information—not universally bound into the SEDI itself but instead linked as verifiable credentials issued by relevant agencies. If Utah went the route to separate out some attributes, the separation could reduce risk, support data minimization, and allows individuals to disclose only what is necessary in a given context. That said harmonizing of an approach within a country (e.g. an mdoc currently contains an address) might support national adoption, so careful consideration is merited to ensure the best choices are made for Utah residents and businesses.

More generally, a state-endorsed identity at this “core plus credentials” level provides interoperability with international standards, aligns with principles of proportionality, and reinforces user control. It also ensures that the SEDI functions as a durable trust anchor while avoiding the pitfalls of over-collection or centralized profiling.

As mentioned in the NIST NCCoE comments, and closing gaps to meet US Financial institution requirements for adoption, there may also be select meta-data related to the assurance process that states such as Utah may wish to share in select use cases as well. For example, FIs are interested in the level of assurance established during the proofing and issuance process of an mdoc/mDL, in line with the best practices defined in NIST SP 800-63-4, as well as evidence to ensure no change has occurred from the time of issuance to the time of presentation (e.g. ensuring a Pin was not used to unlock a wallet then used to open a bank account).

The state of Utah may want to give itself some flexibility to evolve the data that is in the “Core+plus” attributes, allowing for evolution as more and more use cases (especially regulated use cases) are enabled over time.

5. <u>What should the criteria be for an individual to receive a SEDI?</u>

Below are some observations from OIDF when working with other jurisdictions:

- The criteria for receiving a SEDI should consider balance inclusivity with assurance. At a minimum, issuance should consider being anchored to foundational, high-assurance, government-issued identity evidence such as a birth certificate, driver license, or other state-recognized credential. To ensure consistency and trustworthiness, the process should consider following well-known proofing guidelines such as NIST SP 800-63-4, applying IAL2+ levels of assurance where appropriate.
- At the same time, the framework must provide alternative, verifiable pathways for residents who lack traditional documents—such as through vetted agencies or trusted introducers (references in NIST SP 800-63-4)—so that vulnerable populations are not excluded. Eligibility should consider being tied to residency or lawful presence in the state, with narrowly defined grounds for non-issuance or revocation. By combining standards-based assurance with inclusive pathways, Utah can establish a SEDI that is both secure and equitable.

6. <u>Are there any additional situations where a SEDI should be able to be revoked?</u>

Below are some observations from OIDF when working with other jurisdictions:

- Revocations are typically rare, narrowly defined, and transparent. Beyond cases of fraud or proven misuse, a SEDI should only be revoked when the underlying legal identity has fundamentally changed or been invalidated—for example, if a source document such as a birth certificate or immigration record is found to be fraudulent, or when a court order requires a change.
- Routine life events—like name changes, address updates, or changes in guardianship—should not require revocation but typically would trigger updates to the SEDI. Revocation typically never be used as a punitive measure unrelated to the validity of the identity itself, as this undermines trust and risks disenfranchising individuals.
- To preserve privacy, revocation mechanisms should consider using privacy-preserving status lists (batched or aggregated) so that checking revocation does not allow verifiers to track where or how

often someone uses their credential. By limiting revocation to evidence-based circumstances (like when a wallet instance is known to have been compromised) and implementing privacy-protective status checks, the state can maintain both system integrity and individual rights.

7. What should be the funding model for the SEDI program?

No comment.

8. How can the state reliably determine guardianship for the initial and ongoing endorsement of a SEDI?

Below are some observations from OIDF when working with other jurisdictions, and observations from work within the eKYC & IDA WG which has developed work on delegated authority, including guardianship cases (parent/child, elderly person/ caregiver, foster child/foster parent and foster child/foster agency or school).

These delegated authority use cases are complex and in our observation, are not yet widely supported yet by ecosystem experts (government, private sector, development agencies etc) or investment to mature the requirements and mechanisms to resolve them.

A few observations:

- Guardianship could be recognized in the SEDI system through verifiable, legally grounded evidence that can be updated over time.
- At issuance, the state can rely on existing court orders, statutory appointments, or other authoritative records that establish guardianship for minors or individuals under care. These could be represented as verifiable credentials, so that the relationship can be cryptographically bound to the holder's identity without requiring central storage of sensitive information.
- For ongoing endorsement, the system must allow changes as guardianship shifts—whether due to age of majority, court modifications, or termination of legal authority. This means supporting selective delegation and time-limited credentials, enabling guardianship rights to expire or be revoked automatically.
- To ensure privacy and interoperability, Utah may wish to use standards-based approaches (e.g., W3C Verifiable Credentials, OpenID for Verifiable Presentations) that allow guardianship proofs to be portable and auditable without exposing unnecessary details. Combined with regular eligibility checks against authoritative state records, this provides a reliable and privacy-preserving foundation for guardianship within the SEDI ecosystem.

The OIDF is both working on specs to support delegated authority and the OIDF Board approved investment into a whitepaper on Age Assurance to help identify requirements and close the gaps between emerging policies and protocols. The first draft of this paper is expected to be issued December 2024, for a final version in Q1 2024. Oversight for the paper is provided by the eKYC & IDA WG and a subgroup of Board members. Utah feedback into this paper would be most welcome to help accelerate the requirements gathering process, and mechanisms to enable gap closure in standards. .

9. To what extent should the state require technical standards to be open and freely available and implementable to the public and implementors?

The OpenID Foundation is itself predicated on the development and scaling of freely available and open technical standards.

In that respect, OIDF would also advise Utah to prefer open, freely available, and implementable technical standards. Open standards ensure transparency, interoperability, and public trust by allowing independent review, testing, and verification. They reduce vendor lock-in, foster innovation, and make it possible for a competitive ecosystem of wallet providers, verifiers, and issuers to interoperate without costly proprietary integrations.

Requiring standards that are both openly published and royalty-free ensures that any qualified implementor can build to them, lowering barriers to entry and expanding adoption. This approach also aligns with international frameworks such as W3C Verifiable Credentials and OpenID specifications for issuance and presentation, which are developed in open forums and supported by multiple stakeholders worldwide.

By committing to open standards, the state strengthens security through broad peer review, protects individuals against monopolistic practices, and creates a foundation for long-term sustainability and cross-jurisdictional interoperability.

That said, no specification and no architecture no matter how mature or thoughtful is ever completely static. To that effect, Utah will want to consider what requirements merit being in the legislation, vs in operating policies vs those required for conformance. We observe ecosystems incorporate open standards into all of these policy layers, however, what success looks like for Utah will depend on how you can not only set up your ecosystem for launch but then also maintain it effectively overtime to support adoption, privacy, security, and interoperability outcomes as technologies evolve.

10. To what extent should the State rely on open protocols and open source software so the public can inspect the state's technology?

The state should carefully consider open interfaces and open source software, particularly for the components that affect trust, security, and interoperability. Open interfaces and standards developed in multistakeholder forums (e.g., W3C, IETF, OpenID Foundation) ensure transparency, peer review, and alignment with international best practices. They also allow Utah's SEDI ecosystem to interoperate across jurisdictions and with private-sector systems, avoiding lock-in to proprietary solutions.

Open source implementations further strengthen trust by making the code base inspectable, testable, and verifiable by independent experts and the public. This transparency helps identify vulnerabilities earlier, fosters innovation, and reassures citizens that their identity infrastructure is not a "black box." Implementers such as the CA DMV Wallet, OWF Multipaz, OIDF (for open source tests) MOSIP, and the Center for Digital Public Infrastructure are a few of the entities that have developed open source code around digital wallets for the purpose of transparency and to support adoption. However, many private entities also use the open standards but their code is not "open source" (e.g. Idemia or Apple typically do not typically use open source code for their digital wallet deployments).

Whether open standards only are chosen or open source code as well, all implementers should utilize formal conformance testing, certification, and secure operational practices to ensure quality and resilience. By combining open standards and robust certification processes (and in some cases open source code as well), Utah can deliver a system that is transparent, accountable, and trustworthy while still meeting high standards of security and reliability.

11. Should the state require certification of Digital Wallets that can hold a SEDI?

In our observations, Yes, certification of Digital Wallets is essential to ensure trust, security, and interoperability. Because wallets are the primary interface between individuals, issuers, and verifiers, they must be independently validated against agreed-upon standards. If the wallet has weak security or does not work as expected it is likely there will be significant confidence issues in the minds of end-users. Certification should ideally require wallets to pass tests such as OpenID Foundation (OIDF) conformance tests to prove interoperability, demonstrate conformance with Utah-specific privacy controls (no metadata collection, robust and honest consent user experiences), and meet security baselines such as key protection and tamper-resistance.

Periodic re-certification is usually required or mandated to address software updates, emerging vulnerabilities, and evolving standards. To support transparency and accountability, the state may also maintain a public registry of certified wallets and verifiers, enabling citizens and relying parties to confirm conformance easily. For example, Visa and MasterCard balance technology innovation by establishing “scheme rules” with which banks must conform and update their systems to comply with annually. This balances the need for ongoing innovation with the stabilities needed to support US and global payments interoperability.

By grounding certification in open international standards while adding state-specific privacy and security requirements, Utah can ensure that every wallet in the SEDI ecosystem is both interoperable and aligned with the state’s policy values.

OIDF typically recommends all participants in an ecosystems establish conformance before launch on production systems, and then re-certify annually to ensure a solid baseline of conformance in the (inevitable event) that systems are updated which can introduce security, interoperability, and customer experience issues. We also observe and recommend real-time testing for conformance so that any issues can be captured in real-time (or near real time), even though these tests might not be run by an accreditation lab or the OIDF itself. This learning regarding real time testing is a learning from OIDF’s work with many open banking and open data deployments. Such learnings area likely to apply and be extensible to the 37 countries that have selected OpenID4VP and have launched or plan to launch over the next 2 years. However, there is one known major variation from Open banking and open data. Many RPs in digital identity ecosystems will be much smaller scale than a bank or health care provider (as seen in open banking/open data). For digital identity, conformance is also important down to the smallest relying party, therefore consideration must be given to the models required to enable and scale conformance “out to the edge” with the smallest businesses. For example, some “mom and pop” online shops may seek to establish conformance directly, while others may seek to establish their conformance via a vendor relationship like Shopify, Apple, or MasterCard who facilitates the technical conformance of businesses using their services).

12. What does the state need to do to ensure that a SEDI can be accepted in other jurisdictions outside the state?

In our observations, to ensure that a Utah SEDI can be accepted in other jurisdictions, the state must align with open, widely adopted standards and governance frameworks and seek conformance to them to ensure interoperability, security, privacy and operational scale capabilities are in place.

Where the standards vary in substantive ways, technical interoperability could still be achieved by either implementing translation proxies. However this is cumbersome and relies on all parties to deploy the proxies, which will become a function of the cost/benefit of enabling the proxies in each counter party jurisdiction.

The easier path to interoperability is to select, implementing and conform to internationally recognized interfaces such as W3C Verifiable Credentials, ISO/IEC mDL standards, OpenID for Verifiable Credential Issuance/Presentation (OpenID4VCI/OpenID4VP) and FIDO. Conformance with these standards allows other states, federal agencies, and private-sector systems to verify Utah-issued credentials without bespoke integrations and the security and privacy issues that often arise with bespoke solutions. In short – it just works, as we observed with the interop events hosted by NIST and OIDF this summer: May 5th public interop of OpenID4VP and the DCP WG interop of OpenID4VCI. Implementers from Japan, Germany, the US, Australia/NZ and others jointly proved out the specs under the observation of NIST, the EU, and the Japanese Government.

Legal and policy interoperability is just as critical. Utah may wish to seriously consider participate in federal and interstate trust frameworks and align assurance levels with well-established guidance such as NIST SP 800-63 (IAL2+). This creates a common language of trust that other jurisdictions can recognize. Reciprocal agreements or memoranda of understanding with peer states and federal partners can further formalize cross-acceptance.

Finally, the state should maintain transparent certification and governance processes, including a public registry of certified wallets and verifiers. This enables other jurisdictions to independently validate conformance with Utah's trust framework and reinforces confidence in the SEDI.

By combining open technical standards, assurance-aligned policy, and mutual recognition mechanisms, Utah can ensure its SEDI is portable, trusted, and widely usable beyond state borders.

III. Programmatic, Procedural, and Implementation Considerations

1. What specific policies and procedures should be established to govern the issuance, use, management, and revocation of state-endorsed digital identities?

Based on OIDF observations of other jurisdictions, we would recommend a clear “trust framework” that defines:

- **Issuance policies** aligned to NIST SP 800-63 (document checks, liveness, fraud screening) and binding to a user-controlled wallet;
- **Use policies** requiring selective disclosure, pairwise identifiers, and no unauthorized phone-home wallet behavior (so verifiers cannot track people);
- **Lifecycle management policies** for recovery, suspension, and key rollover
- **Revocation limited to** fraud, key compromise, death, or a court order, with privacy-preserving status checks (e.g., batched status lists) so revocation lookups don’t leak where someone used their credential.

This approach implements Utah’s statutory priorities for privacy, unlinkability, and limited revocation in technical, enforceable ways.

2. What are various models for implementing a state-endorsed digital identity program? Please describe the pros and cons of each model, considering factors such as budget, security, user adoption, and scalability.

The points related to security,adoption and scalability are addressed elsewhere earlier in the RFI.

OIDF is not best placed to common on budgets.

However, we would point out that OIDF specs are proven to enable interoperability and security by default, as all implementers in an ecosystems (wallets, relying parties, issuers) can build their deployments to the positive and negative open source tests eliminating nearly all human errors from mis-interpretation of the specs. This enables implementers to focus on testing interoperability and a much narrow set of issues that might arise to debug. This is the lived experience of the OIDF with many open-banking/open data deployments of FAPI which enables interoperability and security by default… and similarly with the 9 interop events conducted in 2025 culminating in the OpenID4VP 1.0 and OpenID for VCI 1.0 this summer. Virtually all bugs detected in pairwise testing were minor human errors that were easily identified and remediated.

3. What is your experience in developing similar projects? Please provide examples.

The **OpenID Foundation itself is not a vendor** and does not sell products; our mission is to make these community-driven standards available to all, and ensure implementers that select OIDF specifications realize the benefits inherent within the specs like the security, interoperability, privacy-preserving capabilities, and operational scale.

The OpenID Foundation develops and stewards widely deployed identity standards used globally, including OpenID for Verifiable Presentations (OpenID4VP) and OpenID for Verifiable Credential Issuance (OpenID4VCI). OIDF also convenes conformance test suites and interop events that include public-sector and commercial participants, providing the “test-once, deploy-many” assurance Utah seeks.

All OIDF specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. If Utah selected OIDF specifications and identified gaps in specifications or gaps in tests, that implementation experience and requirements are warmly welcomed into the OIDF relevant Working Groups and our certification team as appropriate. One of the strengths of the OpenID Foundation is the agility with which we can bring in expert feedback, evolve our specifications and test suites bases on consensus decision making, and then partner with implementers to evolve together.

4. How can the SEDI program stay updated with the latest technology trends and advancements?

In our experience, the the SEDI program should be designed as a living system, able to incorporate new standards and practices without requiring wholesale replacement. It is useful to focus more on the interfaces than the software. Utah can achieve this by adopting open, modular, and extensible interfaces (e.g., W3C Verifiable Credentials, OpenID for Verifiable Credential Issuance/Presentation, ISO/IEC mDL) so that updates can be layered in as the standards evolve.

The state may wish to seriously consider also participate actively in multistakeholder governance bodies (W3C, IETF, ISO, OIDF, and related state/federal forums), ensuring Utah’s requirements are heard and that it benefits from global best practices. Regularly scheduled reviews of the SEDI technical baseline—aligned with NIST guidance and industry security updates—can help ensure the program stays resilient against emerging threats such as quantum computing or new forms of fraud.

Finally, Utah may want to require periodic re-certification of wallets and verifiers against updated conformance tests, and maintain a publicly available standards roadmap so implementers and citizens understand how the program will adapt. This combination of open standards, active participation in standards bodies, and structured update processes ensures the SEDI remains modern, secure, and interoperable over time.

5. How can the State leverage existing infrastructure or initiatives in developing a SEDI program while still meeting all requirements in Utah Code § 63A-16-1201 et seq.?

Based on our experience, Utah could accelerate deployment of a SEDI by building on existing infrastructure and initiatives, provided they are integrated in a way that preserves the state’s policy values of privacy, security, and individual control. The state already maintains high-assurance identity records through systems

like the Driver License Division, health departments, and vital records; these can serve as authoritative sources for identity proofing and credential issuance, avoiding duplication and reducing costs.

For example, Utah couldleverage its single sign-on portal and existing digital service infrastructure as an integration point for SEDI, provided the program enforces unlinkability and selective disclosure so that user interactions are not aggregated or tracked across services. Where mobile driver license pilots and verifiable credential projects are already underway, lessons learned about usability, adoption, and standards conformance should directly inform the SEDI's design.

At the same time, the state can consider anchoring SEDI in open interfaces (e.g., W3C VCs, OpenID4VCI/OpenID4VP) and certification frameworks so that local infrastructure remains interoperable with national and international ecosystems. By layering SEDI on top of what already exists, while strictly enforcing Utah Code § 63A-16-1201 et seq. requirements—such as non-surveillance, revocable consent, and individual control—Utah can reduce implementation risk, speed time to value, and ensure the system is future-proof and trustworthy.

6. Are there any technological or other constraints limiting the types of credentials the State can issue digitally versus physically?

Yes, there are legal constraints that affect which credentials can be digitized and how.

Some credentials are anchored in statutory or federal requirements that assume a physical form (e.g., REAL ID-compliant driver licenses as regulated by the RealID Act and Waiver program run by DHS/TSA, and certain immigration or federal benefit documents). For these, the state may be limited in issuing digital equivalents (sometimes call "derived credentials") until federal standards evolve. As one example, the State department is not issuing mdocs of passports, instead the TSA has decided to accept Apple and Google "derived" credentials established by scanning the user's passport, completing selfie check comparison with the passport on the chip, and other checks, but the underlying digital credential is not issued by or managed by the State Department-the entity that issued the physical passport document. So there is evidence in the US market of derived credentials being acceptable for regulated use cases, however, there are some risks associated with that model (eg lifecycle management and revocation if the underlying credential is revoked; the DHS/TSA may be able to catch that change of status, while other relying parties might not).

Digital credentials must meet high security and privacy thresholds which are not insurmountable but important to note. They require tamper-resistance, selective disclosure, and revocation mechanisms—features that are not always straightforward to implement for every credential type. Credentials tied to sensitive health, financial, or legal data may also require additional privacy safeguards or restricted distribution channels.

There are also adoption and equity constraints to address: not all residents have access to smartphones or secure devices capable of holding cryptographic keys. This means some credentials may need to remain physical, or hybrid models may be required.

By carefully evaluating each credential against its legal mandate, risk profile, and technology readiness, and by anchoring implementations in open standards like W3C VCs, ISO/IEC mDL, and OpenID4VCI/OpenID4VP, Utah can determine which types are best suited for digital issuance while ensuring compliance with state law (§ 63A-16-1201 et seq.) and federal obligations.

7. Based on your experience or research, is it better to issue state endorsed credentials centrally or regionally?

OIDF has observed both models, e.g. EU central approach for all of Europe, and US approach where each state is deciding if or when to issue a digital identity credential or not. Amongst the 37 jurisdictions that have selected OpenID4VP to date, and of the 60 jurisdictions that intend to issued digital identity credentials globally…most of these are centrally organized digital identity programs at a national or regional level. It is more the exception to see state level issuance of digital identity credentials (as currently observed in US, Canada, and Australia). Therefore, the vast majority of digital identity credentials issued to date and expected to be issued over the next few years are likely to be from outside the US not from inside the US.

Entities like the OpenID Foundation, the Better Identity Coalition, and FIDO have encouraged US federal decision makers to consider a US national strategy (e.g. FedID Conference 2024), to improve the national security posture of the US a whole. The current US national approach is fragmented, with NIST providing best practices for the USG resiliency and helping to unpack FI adoption with the NIST NCCoE project, DHS/TSA mostly focused on the TSA security and federal building access and some deep dives into use cases like Disaster & Emergency Support, the NSA addressing the USG/ defence/intelligence security posture, and AAMVA facilitating consensus amongst state issuers on their own requirements (e.g. Implementation Guidelines and DTS). That leaves material gaps on relying party governance, some of which the digital platforms are supporting by default. In contrast, other jurisdictions take a more “top down” regional or national strategy approach. To get a sense of the range of digital trust frameworks in the global contest, the Utah government may want to review the DNA of Trust Frameworks report published by SIDI Hub that analyzes and compares the following trust frameworks from around the globe:

- UK Digital Identity and Attributes Trust Framework (DIATF)
- EU eIDAS2
- US NIST Version 4 draft
- Canada DIACC Pan Canadian Trust Framework
- Bank ID Sweden
- Thailand ETDA Trist Framework
- Singapore Singpass
- Modular Open-Source Identity Platform (MOSIP).

The free report is available here https://sidi-hub.community/publication/the-dna-of-digital-id/.

8. What are best practices for ensuring accessibility and inclusivity for all State residents, including those with limited digital literacy or access to technology?

OIDF observers that many jurisdictions consider accessibility and inclusivity amongst the core design principles of the SEDI program, not afterthoughts. Best practices include:

- **Multiple access channels:** Ensure that residents can use SEDI both digitally and through complementary physical or assisted options. This includes supporting printed QR codes (e.g. pilots in CA DMV, and used commonly by MOSIP implementers), secure smartcards, or assisted service centers for those without smartphones.

- **Inclusive device support:** Wallets would ideally run on a wide range of devices, with lightweight options that work on low-cost hardware and in low-connectivity environments. Offline-capable credentials (e.g., ISO/IEC mDL) reduce reliance on constant internet access.

- **Accessible user experience:** Require wallets and verifier apps to conform to WCAG accessibility standards for visual, auditory, motor, and cognitive accessibility, and provide multilingual interfaces with plain-language explanations of rights and consent.

- **Support for digital literacy gaps:** Provide outreach, training, and in-person enrollment assistance, so individuals with limited digital skills can still access and manage their identities safely.

- **Guardianship and delegated access** would ideally be supported for minors, elders, or those unable to manage their own credentials, as mentioned above. These are complex use cases that require additional focus by implementers and standards bodies (and OIDF has commenced some of this work).

- **Non-discrimination and equity:** Policies should ensure that inability to access or use a digital identity cannot be the sole reason for exclusion from essential services; physical alternatives must remain available.

- **Privacy-preserving design:** Especially for vulnerable populations, systems must minimize data collection and avoid metadata tracking, which can disproportionately harm those with fewer alternatives.

By embedding accessibility and inclusivity requirements into certification, procurement, and governance processes, Utah can ensure that the SEDI program serves all residents equitably, regardless of ability, income, or technical literacy.

9. How can the State foster collaboration and interoperability with private sector entities and other governmental entities in the context of digital identity?

OIDF would expect that collaboration and interoperability are essential to the success of a SEDI program. Utah can foster both by anchoring its system in open, widely adopted standards such as W3C Verifiable Credentials, ISO/IEC mDL, and OpenID for Verifiable Credential Issuance/Presentation (OpenID4VCI/OpenID4VP). These standards are already implemented across industries and jurisdictions, reducing integration barriers for both public and private sector partners.

Fostering collaboration requires transparency and open communication: maintaining public registries of certified wallets and verifiers, publishing roadmaps, and creating advisory councils with representatives from industry, civil society, and other government entities. This ensures the ecosystem evolves inclusively, maintains trust, and scales effectively across sectors.

We expect that Utah is very capable of convening experts within the Utah boundaries. However, we encourage you to look outside of Utah for safe spaces where experts are already convening to derisk your program's

ability to interoperate outside of Utah. For example, the OIDF offers one of those safe spaces to feedback requirements, test out ideas and maintain your roadmap over time.

The state may also want to establish a trust framework and certification program that applies equally to government agencies, commercial verifiers, and wallet providers. By publishing clear conformance requirements—covering privacy, consent, metadata protections, and security baselines—Utah creates a level playing field and ensures any participant can interoperate if they meet the rules.

10. What strategies can be employed to promote the adoption and use of the SEDI program by individuals and organizations?

Promoting adoption requires building both trust and utility. The most effective strategies typically combine user confidence, clear value propositions, and strong ecosystem incentives:

- **Trust through transparency:** Adoption grows when individuals and organizations understand that the system is privacy-preserving, non-surveilling, and user-controlled. Public education campaigns might highlight protections like revocable consent, selective disclosure, and perhaps also address or even limit metadata monetization that could distort the desired ecosystem outcomes.

- **Utility through real use cases:** People and organizations are more likely to adopt SEDI when it solves practical problems, and that those practice use cases drive organic behavior change and technology adoption. Early focus may be on high-frequency, high-value use cases (e.g., age verification, healthcare access, financial onboarding, and government service login). Demonstrating convenience and security in daily contexts drives network effects and adoption.

- **Incentives for verifiers and issuers:** Offer streamlined certification, liability clarity, and reduced conformance costs for organizations that accept SEDI. For agencies, embedding SEDI in digital service delivery can reduce fraud and administrative overhead.

- **Inclusive access and support:** Many jurisdictions consider wallets and digital identity credentials a “public good” such that wallets and credentials are made to be freely available, certified to a common high bar, and available on most everyday smartphone common devices. As noted above, most jurisdictions also seek to offer alternative methods for those without smartphones and allow for assisted enrollment and recovery channels build for residents with additional needs e.g. lower digital literacy.

- **Interoperability with existing standards:** Demonstrating compatibility with W3C, ISO, and OIDF interfaces reassures organizations that SEDI investments will also work across jurisdictions and sectors, preventing lock-in.

- **Visible state leadership:** Public commitments, clear governance, and participation in national and international trust frameworks signal stability and sustainability to both individuals and businesses

By combining trust, convenience, incentives, inclusivity, and interoperability, Utah can encourage widespread adoption of SEDI as both a citizen service and a cross-sector digital identity utility.

11. How can the State ensure efficient operations and delivery of services by governmental entities while supporting both physical and digital identities?

From our observations, efficiency comes from operating digital and physical credentials as complementary, not competing, channels. The state may consider adopt a dual-track approach: continue supporting physical credentials for residents who need them, while using SEDI to streamline digital service delivery and reduce costs over time.

Key strategies include:

- **Shared trust framework:** Establish a unified certification and conformance framework so that whether a credential is digital or physical, agencies and verifiers rely on the same assurance rules, liability structures, and minimum security/privacy requirements.

- **Integration with existing systems:** Link SEDI into the state's single sign-on portal, agency databases, and existing identity verification processes, reducing duplication while enabling stronger fraud prevention.

- **Progressive digitization:** Prioritize digital issuance for new use cases (e.g., online benefits, remote verification) while maintaining physical fallback channels. Over time, digital adoption will reduce reliance on physical issuance, lowering administrative burdens.

- **Operational efficiency through automation:** Use open interfaces (e.g., OpenID4VCI, OpenID4VP, W3C VCs) to automate verification processes that currently require manual review or in-person validation, accelerating service delivery.

- **Inclusive fallback options:** Ensure service delivery does not exclude those unable to use SEDI by keeping physical credentials valid and accepted, and by providing assisted enrollment or guardian delegation.

- **Lifecycle management:** Streamline updates (e.g., name or address changes) by allowing digital credentials to be refreshed automatically or near-real-time, reducing agency workload compared to physical reissuance.

By harmonizing standards, integrating digital and physical processes, and phasing in automation while preserving inclusivity, Utah can achieve both efficiency and equity in service delivery.

12. What wallet certifications should be recognized by the state?

Utah may want to consider wallet certifications that guarantee interoperability, privacy, and security across the SEDI ecosystem. Certification ensures wallets comply with both international best practices and state-specific requirements, giving residents and verifiers confidence in their use.

Best practice is to require:

- **OpenID Foundation (OIDF) conformance tests** for interfaces like OpenID4VCI and OpenID4VP, proving interoperability with issuers and verifiers.

- **W3C Verifiable Credentials and Decentralized Identifier conformance**, ensuring wallets can support selective disclosure, revocation status checks, and cross-jurisdiction portability.

- **ISO/IEC mDL standards** certification where applicable, especially for credentials aligned with driver licenses or travel use cases.

- **Utah-specific privacy and usability controls**, including bans on metadata collection, robust consent UX, and accessibility conformance (e.g., WCAG).

- **Security baselines**, such as hardware-backed key protection, tamper resistance, secure update mechanisms, and vulnerability disclosure processes.

- **Periodic re-certification**, so wallets remain compliant as standards evolve and new threats emerge.

- A **public registry of certified wallets and verifiers**, maintained by the state, to give individuals and organizations an easy way to verify conformance.

By recognizing both global standards (OIDF, W3C, ISO) and adding Utah-specific requirements, the state ensures wallets remain interoperable across borders while reflecting Utah's commitments to privacy, user control, and trust. Utah may also want to keep an eye on any services that FIDO and OIDF offer to ecosystems, since many public and private sector entities are seeking support for low/cost high quality and consistent support that is scalable to their local context (e.g. supporting domestic sovereignty, and local policy requirements while enable interoperability and security by default.)

13. Should the SEDI program include a wallet issued by the State?

In our observation, an issuing authority having their own wallet option and making it available as a choice to the residents, helps not only with user-wallet choice and user-platform choice (or not), but it also supports the evolution of the marketplace to ensure balance and outcomes that support both competition and protect resident, business, and government interests.

A state-issued wallet ensures that every resident has free access to a trusted, certified wallet that embodies the state's privacy, consent, and accessibility requirements. This is especially important for residents who might otherwise be underserved by the market, and can also ensure there is a safe space to develop use

cases that would not otherwise be prioritized by private sector entities (E.g. disabled parking placards in California, or the CA DMV /OIDF Hackathon demonstration by Entidad, of how mDL can be used by farm workers to access benefits they are lawfully entitled to receive, as featured in the local ABC News coverage)

At the same time, the ecosystem would ideally remain open to multiple certified wallets from private providers. Competition fosters innovation, usability, and resilience, while certification ensures all wallets—state or private—meet the same privacy-preserving, security, and interoperability standards.

If Utah issues a wallet, it may want to consider:

- Pass OIDF freely available, open source conformance tests for interoperability, especially for wallet-related functionality (OpenID4VP, OpenID4VCI, HAIP, DCQL using mdocs or SD-JWTs are already available and usable today).
- Demonstrate Utah-specific privacy controls (no metadata collection, strong consent UX).
- Meet security baselines (hardware-backed key protection, tamper resistance).
- Be open source or otherwise transparently auditable, to build public trust.

By offering a state wallet as a reference implementation—while also certifying private wallets—Utah has the ability to consider guarantees for universal access, protect residents' rights, and encourage a healthy, innovative ecosystem.

14. What methods should exist to change an existing SEDI for life events such as legal name changes, modification of birth certificate for sex changes, or addition/removal of guardians?

The SEDI program should consider supporting seamless, privacy-preserving updates for life events without requiring unnecessary revocation and reissuance. Updates can be handled through authoritative state records, ensuring accuracy while minimizing disruption for the individual.

Best practices include:

- **Binding to authoritative sources:** When a legal change is recorded (e.g., name change, amended birth certificate, guardianship modification), the issuing authority would ideally update the underlying record and trigger issuance of a refreshed credential.
- **Incremental updates vs. revocation:** Ordinary life events (name, sex marker, guardianship) could ideally be managed as updates, not full revocations, so that individuals retain continuity of their SEDI identity. Revocation would ideally be reserved for fraud or invalid identity evidence.
- **Privacy-preserving mechanisms:** Use status lists or versioning that allow verifiers to check the validity of the latest credential without learning where or how often it is used. Batched or aggregated status lists prevent surveillance.

- **User-centered processes:** Provide clear notifications, transparent timelines, and appeal paths for individuals affected by changes. Guardianship updates should allow for delegated credentials with time limits or automatic expiry when the underlying authority ends.

- **Standards-based approaches:** Ensure updates are interoperable by relying on interfaces like OpenID for Verifiable Credential Issuance, which provide explicit mechanisms for updating verifiable digital credentials which have already been issued. This allows changes to propagate securely and consistently across ecosystems, even across multiple wallets and issuers.

15. What factors should the state consider to increase adoption of the SEDI program? What should the state avoid that could decrease or hinder adoption?

Adoption depends on trust, usability, and clear value. To increase adoption, Utah should:

- **Demonstrate value in everyday use cases:** Prioritize high-frequency, high-utility scenarios such as age verification, healthcare access, and streamlined government services. People will adopt what makes life easier and safer.

- **Guarantee privacy and user control:** Enforce strong protections—no metadata collection, revocable consent, selective disclosure—so residents know SEDI empowers them rather than tracks them.

- **Ensure universal access:** Provide a free, state-certified wallet and maintain physical credential alternatives. Support accessibility (WCAG conformance), multilingual UX, and assisted enrollment for those with limited digital literacy.

- **Promote trust through transparency:** Open standards, open interfaces, and certification processes (including public registries of wallets and verifiers) build confidence among both individuals and organizations.

- **Enable interoperability:** Align with national and international standards (W3C, ISO, OIDF, NIST SP 800-63) so credentials are widely usable across sectors and jurisdictions.

Consider avoiding: vendor lock-in, centralized tracking, and bespoke interfaces that diverge from other states—those factors risk raising costs for banks, airlines, and retailers and slow acceptance if the approach is not nationally if not globally standardized. This aligns with Utah's aim to reduce conflict with existing law and other jurisdictions while establishing SEDI.

IV. Standards and Technology

1. What technical standards, technologies, and frameworks should be considered for the SEDI program? How do these ensure security, privacy, interoperability, and portability of digital identities? Proposals should cover all aspects of the program, including the issuing, holding and verifying of credentials. Please provide examples of relevant national or international standards.

Utah may wish to keep the SEDI program technology-neutral and center procurement on the statutory principles already outlined in the RFI and Utah Code—individual control, unlinkability, minimal disclosure, and privacy enforced by technology—so multiple mature approaches can compete on merit. That means ISO/IEC mobile documents (e.g., ISO 18013-5/-7 mDL/mdoc), W3C Verifiable Credentials (VCs), traditional X.509 PKI, and event-log systems like KERI/ACDC, recognizing each has distinct strengths and trade-offs across issuance, holding, and verification. Requirements framed around those principles will maximize interoperability across jurisdictions and sectors, prevent vendor or interface lock-in, and leave room for innovation while remaining anchored to Utah's policy goals for decentralization, security, and privacy.

A interface-first, format-agnostic approach ensures that Utah can support both ISO/IEC mobile documents (ISO 18013-5/-7 and ISO 23220) and W3C Verifiable Credentials (VC Data Model 2.0, VC-JWT, VC-Data-Integrity) without locking into a single ecosystem. The OpenID for Verifiable Credential Issuance (OpenID4VCI 1.0, Final) standard provides this flexibility: a DMV could issue a driver's license simultaneously as an ISO mdoc for TSA checkpoints and as a W3C VC for university or employer logins, both delivered over the same secure OAuth-style issuance interface. Because OpenID4VCI does not require "phone-home" checks at the time of presentation, it preserves unlinkability and avoids issuer telemetry that could compromise privacy.

For presentations, OpenID for Verifiable Presentations (OpenID4VP 1.0, Final) works with the Decentralized Identity Foundation's DCQL (formerly Presentation Exchange) to let verifiers specify what attributes they need—such as "over 21" or "resident of Utah"—without revealing the entire credential. This enforces the statutory principle of minimal disclosure. Self-Issued OpenID Provider v2 (SIOPv2) complements this by letting the wallet act as an OpenID Provider, so the holder can both authenticate and present credentials in one step, whether on the web or on mobile, ensuring control stays with the individual.

To convey regulated trust signals, OpenID Connect for Identity Assurance (IDA 1.0, Final) provides a standardized JSON structure for carrying information about identity proofing strength, liveness, and evidence. Combined with OIDF's High-Assurance Interoperability Profile (HAIP) and Data Claim Query Language (DCQL), Utah can support private-sector reliance use cases like banking or healthcare. For example, during remote account opening, a wallet could present (a) the credential, (b) cryptographic holder binding, and (c) IDA assurance claims via OpenID4VP, meeting NIST SP 800-63-3 assurance requirements without issuer callbacks that might enable tracking.

On the security side, the Financial-grade API (FAPI) 2.0 Security Profile, developed within the OpenID Foundation and aligned with IETF OAuth 2.1, DPoP, JARM, and HTTP Message Signatures (RFC 9421), ensures high-assurance protections for issuance and presentation endpoints. This allows Utah to reuse hardened, regulator-accepted interfaces across agencies and private-sector verifiers. To support cross-state portability, OpenID Federation 1.0 enables automated trust establishment through published federation authorities, ensuring that Utah-issued credentials can be accepted in other states or by national agencies without bespoke integrations.

Privacy-preserving status lists, aligned with W3C Status List 2021 and adopted in SD-JWT-VC implementations, allow revocation at scale without linking individual credential checks. For example, when a license is suspended, the issuer simply flips a bit in a published status list. Verifiers check this list through relays or caches, avoiding per-presentation callbacks that could compromise unlinkability.

Together, these standards could cover the full SEDI lifecycle:

- **Issuing**: OpenID4VCI (with ISO and W3C formats), secured by FAPI 2.0.
- **Holding**: SIOPv2 wallets with pairwise identifiers, local key storage, and selective disclosure by default.
- **Verifying**: OpenID4VP with DCQL, IDA assurance claims, and privacy-preserving status lists.

By anchoring to international standards bodies—OpenID Foundation (OpenID4VCI, OpenID4VP, SIOPv2, IDA, Federation, FAPI2), W3C (VCs, DID, Status List), ISO/IEC (18013-5/-7, 23220, 29115), and IETF (OAuth, JOSE, SD-JWT, HTTP Message Signatures)—Utah ensures that SEDI credentials remain portable across sectors and jurisdictions while protecting privacy and user control. To operationalize this, Utah could publish a SEDI Profile that binds these standards into a vendor-neutral certification program, requiring wallets and verifiers to implement selective disclosure, unlinkable revocation, and holder-controlled presentation by default.

2. <u>What criteria should be used to determine if the State would ideally support a given digital identity standard/technology?</u>

The State would ideally adopt a principled, future-proof approach when deciding which digital identity standards or technologies to support. Two factors are paramount. First, adoption: technologies with broad and growing adoption across both public and private sectors are more likely to deliver real value for Utah residents and relying parties. This includes standards already in production use for common scenarios such as airport screening (ISO 18013-5/7 mobile driver's licenses), web authentication and login (OpenID Connect), and verifiable credentials for online services (W3C VC Data Model, OpenID4VCI/VP). Adoption ensures interoperability, vendor competition, and reduces the risk of Utah becoming locked into a proprietary or niche solution.

Second, consensus-based, international governance: in line with WTO best practices, the State would ideally only support standards developed through open, consensus-driven processes led by recognized international bodies such as ISO/IEC, W3C, IETF, and the OpenID Foundation (OIDF). Standards that lack transparent, multi-stakeholder governance are at risk of stagnation, obsolescence, or capture by a single vendor.

Beyond these two primary considerations, additional criteria can strengthen Utah's evaluation. Ecosystem size and maturity matters: a healthy ecosystem of independent vendors, wallets, verifiers, and tool providers ensures competition and sustained innovation. For example, OpenID Connect and the OIDF's newer profiles (OpenID4VCI, OpenID4VP, SIOPv2, FAPI 2.0, and Identity Assurance 1.0) have multiple interoperable implementations and active cross-jurisdiction pilots, supported by OIDF's public certification and conformance testing programs. Real-world use case alignment is also crucial: the standards would ideally support transactions that matter most to Utah residents, from proof-of-age at retail to professional licensing, healthcare access, or higher-education login. Standards would ideally also demonstrate scalability, with evidence from

large-scale deployments (such as OpenID Connect's global use in authentication or ISO mDL pilots at TSA). Finally, Utah would ideally evaluate how a standard addresses security and recovery in worst-case scenarios, such as stolen keys, lost devices, or credential compromise. Standards that include privacy-preserving revocation mechanisms (e.g., W3C status lists, SD-JWT-VC, or OIDF-aligned approaches without issuer "phone-home") and support user-controlled recovery pathways would ideally be prioritized.

In summary, Utah would ideally support digital identity standards that (1) are widely adopted with strong market momentum, and (2) are developed through consensus-based, internationally recognized standards bodies. Combined with ecosystem maturity, real-world alignment, scalability, and robust recovery options, these criteria ensure that SEDI will rest on stable, interoperable, and future-proof foundations.

3. Does your solution allow for portability of digital credentials between jurisdictions, such as from one state to another?

Yes. Portability is built into OpenID Foundation standards. Using OpenID4VCI, Utah can issue the same credential in multiple formats—such as an ISO mdoc for TSA screening and a W3C Verifiable Credential for online services or an SD-JWT for presentations during travel to Europe —ensuring cross-jurisdiction and cross-sector use with consistent assurance signaling. OpenID Federation 1.0 provides the framework for scaling trust between states, agencies, and private relying parties, while the High-Assurance Interop Profile (HAIP) supports alignment on assurance across different ecosystems. These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver secure, interoperable, and portable credentials.

These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver portable credentials.

4. How can the state reduce abuse, prevent selling credentials, and know if a citizen's SEDI is being used without their permission?

The State can protect residents from credential abuse by combining policy measures, certification programs, and built-in technical protections. One option is to establish a voluntary verifier certification program, where organizations that wish to request or accept SEDI credentials can demonstrate compliance with Utah's privacy and security requirements. Certified verifiers could be listed in a public directory, giving residents confidence that their credentials are only being requested by trusted entities, without the State needing to maintain a restrictive "allow list." This creates a clear incentive for verifiers to meet higher standards while keeping the ecosystem open and competitive.

For some use cases where there is higher risk (e.g. payments, romance scams driving bulk payments), then additional steps including some form of RP registration might be pragmatic to protect users and businesses from fraud by further strengthening the ties between user identity and entity identity on both sides of a transaction. This topic merits monitoring as fraud and scams are already accelerating with AI deep fakes,

causing material concerns to financial institutions, legislators at state/federal levels, and to consumers and businesses. The US House of Representatives formed a bipartisan Caucus on Fraud and Scams in September 2025, with a focus on legislation designed to protect US citizens and business from bad actors, especially foreign adversaries. See the recent Aspen Institute report on a National Strategy to prevent Fraud and Scams in which digital identity credentials/VCs and shared signals are mentioned as supporting capabilities for a wider US strategy.

For higher-risk transactions, credentials may also be be bound to the citizen's device, making them unusable if sold or transferred. Wallets can enforce this through device keys and require a local authentication step—such as biometrics, PIN, or knowledge-based prompts—before a credential is released. Modern digital identity standards also provide challenge-response interfaces and nonces that ensure each presentation is unique and cannot be replayed. Cryptographic signatures further protect authenticity, offering stronger guarantees than physical credentials ever could.

To help identify systemic risks, Utah could require wallets to collect anonymized and aggregated statistics on verifier requests, flagging patterns like excessive data requests without exposing personal histories. Risk-based obligations for relying parties, such as requiring insurance coverage for those who store or process SEDI data, would add financial incentives for responsible behavior. In addition, optional transparency mechanisms—such as registries of credential issuances or signed event logs—could help detect fraudulent activity while maintaining privacy, if carefully designed.

OIDF standards offer interface-level protections that directly reduce the risks of unauthorized use or resale of credentials:

- **Cryptographic holder binding**: With OpenID4VCI issuance, credentials are tied to a cryptographic key on the resident's device. This makes it infeasible to sell or share a credential, since only the bound device can generate valid proofs.

- **Verifier policy and attestation**: Through OpenID Federation 1.0, verifiers publish metadata about their policies and assurance practices. Combined with OpenID Connect for Identity Assurance (IDA), Utah can enforce that only certified verifiers can request certain attributes, and residents can see policy signals before sharing.

- **Replay protection and selective disclosure**: OpenID4VP ensures that every credential presentation includes a unique nonce and challenge-response, blocking replay attacks. With SD-JWT-VC or ISO mdoc selective disclosure, residents can share only the attributes required by the verifier.

- **Shared Signals & Events**: The OIDF Shared Signals and Events Framework enables anomaly and compromise reporting between parties. Utah could adopt this as a policy layer, where wallets or verifiers notify each other if abuse or compromise is suspected, without leaking individual user activity.

- **Portability with integrity**: Because OID interfaces are portable by design, Utah can support multiple credential formats (e.g., W3C VC and ISO mdoc) with consistent assurance signaling. This ensures that portability does not weaken protections—credentials remain device-bound and cryptographically verifiable across jurisdictions.

Together, these technical safeguards create an ecosystem where credentials cannot be reused, resold, or silently misused, while verifiers and wallets operate transparently under Utah's trust framework.

These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver a robust system.

5. Does your solution support unlinkability so that the use of the SEDI with a verifier by an individual cannot be tracked by any other entity? If so, how much will it have to be managed via policy?

Yes. OIDF standards such as OpenID4VP with SD-JWT-VC or ISO mdoc enable unlinkability by design, ensuring that each presentation is cryptographically unique and does not require callbacks to the issuer, so verifiers cannot track an individual across different interactions. Most of this protection is delivered technically, with policy mainly needed to guide verifier behavior and transparency.

These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver secure, interoperable, portable, and unlinkable credentials.

6. How does your solution support revocation while maintaining unlinkability capabilities?

Yes. OIDF standards support revocation while preserving unlinkability by using privacy-preserving status lists and pairwise identifiers. In practice, revocation is handled through batched status list bitmaps published by the issuer; verifiers simply check a bit rather than querying an individual record. This means a suspended license can be flagged without any "phone-home" to the issuer, so no entity can track presentations across verifiers. Technical protections make unlinkability the default, while policy can complement by restricting over-collection and requiring audit of verifier behavior.

These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver secure, interoperable, portable, and unlinkable credentials.

7. Does your solution allow for a legal guardian to obtain or use a SEDI on an individual's behalf?

Yes. OIDF standards support guardianship and selective delegation as privacy-preserving, first-class flows. A legal guardian relationship can be modeled as a Guardianship Verifiable Credential issued by the competent authority, which links the guardian and subject with defined scope and time limits. Utah's trust framework could require that such delegation be time-boxed or limited to specific purposes, ensuring it cannot be misused or extended beyond its intended context. When needed, the guardian's wallet can present both the Guardianship VC and the subject's relevant SEDI attributes together in a single OpenID4VP interaction. Pairwise identifiers

and verifier policies ensure that only the minimum necessary information is revealed, consistent with Utah's principles of user rights and data minimization. For example, a parent authorizing school services would present the guardianship credential plus the child's proof of enrollment, while the verifier learns only what is required to grant access.

These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver secure, interoperable, portable, and privacy-preserving credentials.

8. What types of technology solutions (e.g., decentralized identity, biometrics, digital wallets)should be evaluated for the SEDI program, and what are their respective strengths and weaknesses in the context of the State's policy objectives?

Yes. The State will likely wish to evaluate a range of technology solutions under a wallet-centric, standards-based model, measuring each against Utah's policy objectives of privacy, unlinkability, minimal disclosure, and citizen control. OIDF standards such as OpenID4VCI/VP and SIOPv2 keep issuance and presentation wallet-mediated, avoid "phone-home" verification, and allow Utah to remain format-agnostic across ISO mDL/mdoc and W3C Verifiable Credentials. Biometrics can serve as local device binding choices, but in our observation, should never be shared beyond the wallet. By prioritizing interface conformance over a particular ledger, DID, or KERI stack, Utah remains future-proof, allowing multiple credential formats and ecosystems to interoperate under one framework.

Utah will benefit most from a multi-format issuance approach—for example, ISO mDLs for airport acceptance and W3C VCs for online services—delivered over OpenID4VCI/VP, enforced through certified digital wallets with device-bound keys and optional biometrics for local binding. Emerging approaches such as KERI can be evaluated for specialized use cases, but interface-first, consensus-based standards would ideally remain the foundation so that Utah avoids vendor lock-in and keeps the SEDI ecosystem future-proof.

9. How can the SEDI program incorporate privacy-enhancing technologies (PETs) to protect user data?

The SEDI program can embed privacy-enhancing technologies (PETs) directly into its technical architecture so that protections are enforced by default rather than left to policy alone. By using modern standards from the OpenID Foundation, W3C, ISO, and IETF, Utah can ensure unlinkability, minimal disclosure, and citizen control are built into every issuance and presentation, while retaining flexibility to adopt stronger PETs such as zero-knowledge proofs as the ecosystem matures.

Make privacy the default at the interface layer. Use selective disclosure formats (e.g., SD-JWT-VC) so wallets release only the attributes a verifier asks for (e.g., "over-21," not full DOB). Pair this with on-device proving over OpenID4VP 1.0 so each presentation is a fresh, challenge-bound proof with no issuer "phone-home," preventing cross-context tracking. These PETs align directly with Utah's requirements for unlinkability, minimal disclosure, decentralization, and technical—not just policy—enforcement.

Bind credentials to the holder—without leaking where they're used. Issue over OpenID4VCI 1.0 to a device-controlled key (cryptographic holder binding). Present with pairwise/ephemeral identifiers so different

verifiers see different subject identifiers, limiting correlation. This preserves user control, reduces data proliferation and helps deliver privacy goals, while keeping the State out of the presentation path.

Use privacy-preserving revocation. Publish batched status lists that let verifiers check a bit (not an individual record) to learn if a credential is suspended—refreshed from caches/relays and validated offline during presentation—so revocation doesn't re-introduce linkage. (Example: DLD flips a bit; verifiers update on schedule; no callback at presentation.)

Convey only what's necessary, with auditable policy. Express verifier data needs via DCQL requirements carried in OpenID4VP; carry assurance and evidence in OpenID Identity Assurance Schema Definition 1.0, enabling consistent, minimal, and well-scoped data release. Use OpenID Federation 1.0 metadata to publish verifier policy/attestations and scale cross-jurisdiction trust without bespoke integrations.

Add signals only when needed. If Utah opts to monitor anomalies or suspected compromise, adopt Shared Signals & Events patterns between participating parties—structured, policy-bounded security signals that **do not** expose individual presentation histories.

Future-proof without refactoring rails. Because OpenID4VCI/VP are format-agnostic, Utah can start with SD-JWT-VC and ISO mdoc today and later add ZK-friendly credential formats as they mature—without changing the OID rails or sacrificing PETs. It will also be possible to change to Quantum Resistant Cryptographic algorithms with the pluggable nature of algorithms in the OpenID standard interfaces.

10. What mechanisms should be in place for identity verification and authentication within the SEDI ecosystem?

UtahID as the entry point. Within the SEDI ecosystem, UtahID can serve as the state-managed single sign-on (SSO) platform which uses OpenID Connect, giving residents a consistent way to access services through a "digital front door" that is technologically compatible with the systems within Utah's many agencies. Today, this portal may utilize various identity verification providers from the private sector that use proprietary databases to conduct identity proofing, but in the future, acceptance of a SEDI credential could allow users to have unified access across state agency services while cutting down fraud, ensuring the privacy characteristics of SEDI during identity verification, and reducing the reliance on proprietary databases for identification.

It also means that agencies can rely on the same verification portal, creating more efficiency and accountability to ensure that the state's handling of user-consented data sharing follows SEDI principles and other regulations which apply to state entities. Further, additional protocols atop of OpenID Connect could be used to add data privacy guarantees, by ensuring minimal data retention using eKYC and Identity Assurance flags instead of transmitting unnecessary PII, using pseudonymous identifiers across agencies (or to the private sector) when appropriate to mitigate correlation risk across user sessions and eliminate "phone home" behavior through identifier blinding, and adopting new extensions that can represent the result of checking guardianship from a SEDI-compatible credential such as the OpenID Connect Authority claims extension, which could allow existing agency services to rely on those claims about guardianship without major changes to their infrastructure.

Identity verification (proofing). The strength of identity proofing would ideally be captured using OpenID Identity Assurance Schema Definition 1.0, which conveys how and to what level an identity was verified. UtahID can multiplex across multiple IDV providers so agencies can choose proofing methods that match their

requirements—using lighter checks for informational access and higher-assurance methods (aligned with standards like IAL2) for sensitive services such as benefits administration.

Credential binding (holder control). Credentials could be issued to a cryptographic key on the resident's device via **OpenID4VCI 1.0**, ensuring only the rightful holder can use them. Wallets can require a local step such as a PIN or biometric check, but biometrics remain strictly on-device.

Authentication at verifiers. When a resident presents a SEDI, authentication can be performed through a couple different OIDF specifications (such as OpenID Connect or SIOP v2, with appropriate guardrails, and potentially other options as well), so there are several options for how Utah can combine credential presentation and login in a single step. For higher-risk services, verifiers can apply the FAPI 2.0 Security Profile to provide strong security protections. UtahID may wish to also support risk-based escalation—for example, stepping up from password to MFA or requiring re-proofing if fraud signals or behavioral analytics indicate higher risk.

Cross-jurisdiction trust. OpenID Federation 1.0 allows issuers, wallets, and verifiers to publish metadata and policies so that credentials issued in Utah can be recognized by other states, federal agencies, and private-sector relying parties without custom integrations.

Revocation and replay protection. Revocation can be handled using privacy-preserving status lists, where a verifier checks a shared list rather than contacting the issuer, preserving unlinkability. Each OpenID4VP transaction also includes a unique challenge, preventing replay of earlier credential presentations.

Program flexibility with consistent resident experience. While UtahID provides a unified backbone, each agency would be able to configure its identity verification and authentication workflows to reflect its regulatory environment and fraud risk profile. Residents, meanwhile, should always experience minimal disclosure, data protection, and transparency by default, building trust across the ecosystem.

11. How should data governance and data minimization principles be integrated into the design and operation of the SEDI program?

Build governance into the interfaces, not just policy. The SEDI program has the potential enforce data minimization technically so residents are never asked to disclose more than necessary. With OpenID4VP 1.0 and DCQL, verifiers must define in advance what information they need (`presentation_definition`), and wallets only release that subset—ideally in the form of predicates (e.g., "over 21") rather than full attributes (e.g., date of birth). This ensures that the State's statutory principles of minimal disclosure, unlinkability, and citizen control are consistently applied across all transactions.

Consent and policy encoded in federation. Governance rules and conformance statements could be published through OpenID Federation 1.0 metadata so that verifiers are registered with clear declarations of what they are allowed to request, how long they may retain data, and what trust framework applies. This creates transparency for residents and simplifies conformance monitoring. Utah can require that consent, retention limits, and purpose restrictions are embedded in verifier registration, rather than left to one-off policy documents.

Log only what is necessary. To preserve unlinkability, the system should avoid central logging of individual credential presentations. Instead, wallets and verifiers can log minimal, anonymized events (e.g., proof type or

assurance level used), which help detect systemic issues or policy violations without creating a tracking risk. Where monitoring is needed, privacy-preserving approaches such as aggregated statistics or Shared Signals & Events can flag anomalies without exposing resident activity.

Program flexibility under a unified framework. UtahID can serve as the governance backbone, applying consistent disclosure controls across agencies while allowing program-specific configurations. For example, low-assurance services may only need a basic credential proof, while high-assurance services can require stronger IDA evidence or higher assurance levels. In all cases, data minimization and governance must be encoded at the interface level, so conformance is automatic and independent of vendor choice.

Future-proof and standards-aligned. By building data governance into the technical design using OpenID4VCI/VP, OID4IDA Schema, DCQL, and Federation, Utah ensures that privacy requirements are enforceable across both ISO mDL/mdoc and W3C Verifiable Credentials, and remains open to adopting future privacy-enhancing credential formats (e.g., zero-knowledge proof–friendly models) without changing the overall rails.

12. What considerations should be given to the long-term sustainability and evolution of the SEDI program, including technology updates and adaptation to emerging threats and standards?

The SEDI program should be designed to adapt over time, both to new technologies and to emerging security threats. This means anchoring to open, consensus-based standards such as OpenID4VCI and OpenID4VP (for credential issuance and presentation), OpenID Identity Assurance Schema Definition 1.0, High-Assurance (formerly Financial-grade) OpenID Connect and API Security profiles, and OpenID Federation 1.0. These are maintained by the OpenID Foundation and updated regularly through open working groups, giving Utah a path to stay aligned with the global ecosystem. By requiring that vendors pass formal conformance testing and certification before deployment, Utah can ensure consistency across solutions and reduce the risk of lock-in to one provider’s implementation.

A sustainable program also needs cryptographic agility—the ability to adopt new algorithms as older ones are retired or broken. Utah should plan for post-quantum cryptography (PQC) as standards mature, and participate in OIDF and IETF communities where work on JOSE, DC-API, and related crypto updates is ongoing. Periodic updates to a Utah-specific SEDI Profile can help formalize these changes, while staged rollouts and pilot programs give agencies time to adapt before statewide deployment.

Finally, sustainability depends on governance as much as technology. Utah would ideally commit to participating in OIDF working groups and international standards forums, ensuring it has visibility into the evolution of identity standards and influence over future directions. This proactive engagement will allow the SEDI program to remain secure, interoperable, and adaptable—ready for both today’s needs and tomorrow’s innovations.

13. How can the proposed standards or technology Standard be used for other credential types beyond SEDI?

The same interface rails that support a SEDI can also be used for a wide range of other digital credentials, from professional licenses and permits to benefits eligibility and education records. With OpenID for Verifiable

Credential Issuance (OpenID4VCI 1.0), Utah State bodies and private sector entities can issue credentials in multiple formats—ISO mDL/mdoc (ISO 18013/23220) for in-person acceptance and W3C Verifiable Credentials for online services—without changing the underlying system. This format-agnostic approach means the same infrastructure can serve very different use cases, while preserving Utah's neutrality and avoiding centralized credential stores.

For example, the DMV could issue both an mdoc and a W3C VC over OpenID4VCI for a digital driver license. At TSA, the traveler presents the mdoc; at a university login portal, the same person presents the VC over OpenID4VP. The same pattern works for professional licenses, hunting/fishing permits, or proof of benefits—delivered through wallet-centric issuance and presentation with selective disclosure and device binding.

OpenID Identity Assurance Schema Definition 1.0 allows Utah to carry assurance signals and trust framework tags across all credential types, while SIOPv2 enables holders to combine login and credential presentation in one flow. To protect privacy, Utah can keep the core identity credential separate and link other credentials to it by policy, minimizing repeated disclosure of sensitive personal information.

In short, the OIDF standards are reusable across all credential formats and types: OpenID4VCI for issuance, OpenID4VP/SIOPv2 for presentation, IDA for assurance, and Federation for cross-jurisdiction trust. This makes the SEDI program not just a driver license initiative, but a platform that can support the full spectrum of state-issued digital credentials over time.

These specifications are developed through an open, consensus-based community process that includes governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to make these community-driven standards available so any provider Utah selects can deliver secure, interoperable, portable, and privacy-preserving credentials.

14. How would the state issue other credentials that tie to the SEDI?

The State can issue additional credentials—such as professional licenses, permits, or benefits—using the same issuance and presentation rails as the SEDI. With OpenID4VCI, each credential is issued to the resident's wallet and bound to a device key, ensuring holder control. These credentials can be in multiple formats (e.g., ISO mdoc for in-person acceptance and SD-JWT-VCfor online services) without requiring separate systems.

Where linkage is required, Utah can keep the core SEDI identity credential distinct and associate other credentials with it through policy and trust framework rules. This minimizes repeated disclosure of identity data, while still allowing verifiers to confirm that, for example, a professional license or benefit claim belongs to the same individual. Presentation occurs over OpenID4VP/SIOPv2, with OpenID Identity Assurance Schema Definition 1.0 providing standardized assurance and evidence claims.

By following this approach, Utah leverages a single, wallet-centric ecosystem that can issue, hold, and verify many different credential types—all anchored to the same OpenID Foundation community standards—while maintaining privacy, unlinkability, and interoperability across jurisdictions.

15. What verification tools does your solution provide for a SEDI credential?

The OpenID Foundation does not provide products, but we maintain standards and verification tools that any vendor can adopt. For SEDI, this includes OpenID4VP libraries and conformance testing suites, which ensure that wallets and verifiers process Verifiable Presentation (VP) tokens correctly and honor DCQL requirements for data minimization. Utah could also require that all verifiers demonstrate conformance as a condition of certification.

In practice, a state ecosystem can combine multiple verification options: a state-hosted OpenID Federation trust service so verifiers know which issuers are recognized; a free, web-based verifier tool for smaller organizations or pilot projects; and mobile verifier applications with offline status-list caching, so credential validity can be checked even without an active network connection. These patterns are already supported within the OIDF interfaces and can be adapted to Utah's needs.

16. Does your solution support various credential expiration length and non-expiring credentials?

Yes. OIDF standards allow issuers to set credential lifetimes at issuance and support both short-lived and non-expiring credentials. Expiration can be encoded directly in the credential claims, while actual usage is protected through short-lived presentations over OpenID4VP, ensuring verifiers only see fresh, challenge-bound proofs. For high-assurance use cases, the High-Assurance Interoperability Profile (HAIP) provides guidance on expiration policies, renewal practices, and assurance signaling.

Renewals, suspensions, or revocations can be handled through status-list mechanisms and key rollover policies, defined in a Utah-specific SEDI Profile, without requiring issuer callbacks that could undermine unlinkability. This gives the State flexibility—for example, issuing short-lived credentials for sensitive benefits programs, while allowing non-expiring credentials (such as proof of graduation) where appropriate.

These specifications are created through an open, consensus-based community process involving governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to provide these community-developed standards so that any provider Utah selects can issue and manage credentials with expiration policies that align to program needs while preserving privacy and interoperability.

17. How does your solution ensure an appropriate level of security, privacy, simplicity, and transparency?

Security. Use of OpenID for Verifiable Credentials (OpenID4VC) specifications along with the forthcoming High Assurance Interoperability Profile (HAIP) for SEDI credentials allows for flexibility in the types of data formats and credential representations (whether they are mdocs, SD-JWT, or KERI/ACDC), but creates requirements around the security model that better support use cases such as financial-grade identity and secure access to benefits through an online portal. We believe this approach can satisfy the requirements for SEDI while also allowing for flexibility in approaches that are largely aligned with the broader industry.

Privacy. By default, pairwise or ephemeral identifiers prevent correlation across verifiers, while selective disclosure formats such as SD-JWT-VC or ISO mdoc allow a resident to share only what is necessary (e.g.,

“over 21” instead of full date of birth). Revocation lists are batched to preserve unlinkability, and wallets enforce local authentication without exporting biometrics.

Simplicity. The ecosystem is designed around wallet-centric interactions where verifiers request only what they need through presentation_definition, and residents respond with a clear, minimal disclosure flow. Verifier tools can be lightweight—such as a simple web-based verifier for small businesses—while wallets can be **certified for conformance** to ensure a consistent resident experience.

Transparency. OpenID Federation 1.0 provides a framework for publishing verifier and issuer policies in metadata, so residents and regulators can see what data is requested, how it is handled, and under what trust framework. Utah can publish a state-managed trust list and conformance program to make conformance visible. Looking forward, Utah can stay aligned with international standards bodies through the OpenID Foundation, tracking updates in post-quantum cryptography (PQC) and other emerging security requirements.

Together, these measures deliver security, privacy, simplicity, and transparency by default, ensuring that Utah residents remain in control while keeping the SEDI ecosystem sustainable and trustworthy.

These specifications are created through an open, consensus-based community process involving governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to provide these community-developed standards so that any provider Utah selects can issue and manage credentials with expiration policies that align to program needs while preserving privacy and interoperability.

18. What is your solution’s approach to post-quantum encryption?

The OpenID Foundation’s standards are designed with algorithm agility, meaning Utah can adopt new cryptographic algorithms—including post-quantum cryptography (PQC)—without changing the underlying interfaces. OpenID4VCI/VP and IDA use JOSE/COSE containers, which are flexible enough to support hybrid and PQC algorithms once standardized. This allows a smooth transition path: first hybrid PQC + classical crypto, then PQC-only, without needing to replace the SEDI technical implementation .

By anchoring to open, consensus-based standards and participating in OIDF working groups, Utah ensures the SEDI program will remain cryptographically resilient and ready for PQC adoption as standards mature.

These specifications are created through an open, consensus-based community process involving governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to provide these community-developed standards so that any provider Utah selects can issue and manage credentials with expiration policies that align to program needs while preserving privacy and interoperability.

19. How is your solution protected against “harvest now, decrypt later” attacks?

To mitigate the risk of adversaries storing encrypted data today to break it later, the SEDI design uses forward-secret channels (e.g., TLS 1.3) and short-lived tokens, so intercepted data becomes useless once a session

ends. Credentials are issued and presented with minimal retained data, and Utah can require PQC-ready credential containers so that even if storage occurs, there is little sensitive information to decrypt later.

This approach ensures that Utah residents' data remains protected not only against today's threats but also against future cryptographic breakthroughs.

These specifications are created through an open, consensus-based community process involving governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to provide these community-developed standards so that any provider Utah selects can issue and manage credentials with expiration policies that align to program needs while preserving privacy and interoperability.

20. What reporting and statistical analysis tools does your solution provide?

The OpenID Foundation does not provide products, but our standards support a privacy-preserving approach to reporting and analytics. Instead of per-presentation telemetry, which could undermine unlinkability, Utah can collect aggregate and anonymized ecosystem metrics. For example, wallets and verifiers can report the number of successful transactions, credential types requested, or assurance levels used—without exposing individual user histories.

Conformance testing and certification programs maintained by OIDF also provide standardized performance and conformance results, which Utah can use to evaluate vendor readiness and ecosystem health. In practice, this means Utah gets the oversight it needs—through aggregated statistics, certification outcomes, and verifier policy metadata—while keeping individual credential use private and unlinkable.

These specifications are developed through an open, consensus-driven community process involving governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our role is to provide these standards and conformance tools so any provider Utah selects can deliver transparent, privacy-preserving reporting within the SEDI ecosystem.

21. Does your solution require that it retain digital user credential information?

No. The OIDF is not providing a solution rather it provides standard definitions of key interfaces between components of an identity ecosystem. OIDF has standards that are designed so that credentials remain in the resident's wallet, not in centralized state or verifier databases. Verifiers are expected to retain only the minimal decision artifacts they need—such as a "yes/no" result ("age ≥18: true") tied to a transaction ID—not the raw credential itself (unless there are regulatory requirements for record keeping of that nature).

A Utah-specific SEDI Profile can make this explicit, forbidding centralized credential stores and requiring verifiers to handle only the limited evidence necessary for conformance or audit. This protects privacy, prevents correlation across services, and ensures residents keep control of their digital identity information.

These specifications are created through an open, consensus-based community process with input from governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our mission is to provide the standards that allow any provider Utah selects to deliver wallet-held, privacy-preserving credentials with no unnecessary data retention.

22. Does your solution avoid centralized storage of credential information in issuer or endorser infrastructure?

Yes. While the OIDFdoes not specify that centralized storage of credential information is or is not needed there are OIDF standards that are intended to keep credentials in the resident's wallet, not in centralized issuer or endorser infrastructure. With OpenID4VCI, credentials can be issued directly to the holder's device and cryptographically bound to their key, so there is no need for a central database of user credentials (aside from the authoritative source data maintained by the issuer). This design aligns directly with Utah's statutory principle of avoiding centralized storage, reducing both privacy risks and the impact of potential breaches.

Issuers and endorsers may maintain their own trust metadata (e.g., signing keys, revocation status lists), but these are public, non-personal artifacts rather than copies of resident credentials. A Utah-specific SEDI Profile can make this mandatory, ensuring wallets retain credentials while verifiers use only privacy-preserving status checks and decision artifacts.

These standards are developed through an open, consensus-driven community process with participation from governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our role is to provide these community-developed standards so that any provider Utah selects can deliver decentralized, wallet-held, privacy-preserving credentials.

23. How can individuals specify limits on how their data can be used when presenting credentials to verifiers?

Limits on data use are enforced both by policy and by technology. When a verifier is onboarded, its policies and data-use restrictions can be published in OpenID Federation metadata and reinforced through contractual obligations. A Utah-specific SEDI Profile can require that verifiers request only what is strictly necessary, and that these requests are clearly communicated to residents enabling them to choose to proceed or not.

On the user side, the wallet enforces selective disclosure, showing the resident exactly what attributes are being requested and allowing them to release only those—such as proving "over 21" without sharing a date of birth. Wallet prompts make data use transparent at the moment of presentation, and refusals or limits can be applied consistently across verifiers.

In this way, individuals control their data in practice, while Utah ensures conformance through verifier registration and certification.

These standards are developed through an open, consensus-based community process including governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our role is to make these community-driven standards available so that whichever provider Utah selects can deliver policy-bounded, wallet-enforced, privacy-preserving credentials.

24. How does your proposed solution allow the presentation of a credential without requiring the holder to surrender their device to another person?

Yes. OIDF standards are designed so the holder never has to hand over their phone or device. Presentations can be initiated through a QR code scan, deep link, app-to-app handoff, or DC-API call so the resident keeps control of their device at all times. For ISO mobile documents, the mdoc device engagement model supports tap or scan interactions where the verifier reads only a cryptographic proof—not the phone itself.

For example, with OpenID4VP, a verifier displays a QR code; the holder's wallet scans it, generates a selective-disclosure proof, and transmits it securely. The verifier receives only the proof that delivers the requested information (e.g., "over 21"), never the raw credential and never the device.

These specifications are developed through an open, consensus-driven community process involving governments, vendors, and experts worldwide. The OpenID Foundation itself is not a vendor and does not sell products; our role is to provide the community-developed standards that ensure Utah residents can present credentials safely, simply, and without ever surrendering their devices.