SpruceID

State-Endorsed Digital Identity

Utah Department of Government Operations

Prepared by: Spruce Systems, Inc. (dba SpruceID)

Table of Contents

I. Executive Summary

SpruceID is honored to submit this response to the Utah Department of Government Operations regarding the State-Endorsed Digital Identity (SEDI) program. Our proposal is grounded in Utah's statutory requirements for privacy, unlinkability, and individual control. SpruceID's Credible platform has already issued tens of thousands of verifiable digital credentials in Utah and powers the California DMV's mobile driver's license program, where more than two million credentials have been issued. These deployments demonstrate the scalability, usability, and privacy protections necessary for a successful SEDI program.

SpruceID's design philosophy emphasizes privacy by design. We propose selective disclosure, unlinkable identifiers, privacy-preserving revocation mechanisms, and hardware-based protections to ensure that SEDI credentials enforce statutory principles technically, not just administratively. Residents will remain in control of their credentials, and no centralized repository of personal data will exist in issuer or wallet infrastructure.

We recommend that Utah define SEDI as a framework of technical and statutory controls, not as a single credential. A "SEDI credential" would apply to many possible credentials, whether it is a digital identification card issued by the DMV, or a digital veteran's ID card issued by the UT VMA, which represent the State's highest-assurance digital identity, meeting all required protections such as unlinkability, minimal disclosure, and individual control outlined in SEDI. At the same time, the framework can be referenced piecewise to guide the design of other state-issued credentials—such as professional licenses, permits, benefit eligibility records, or guardianship credentials—by allowing them to adopt relevant SEDI controls where appropriate. This framework approach ensures consistency across credential types, maximizes flexibility, enables interoperability with existing credential ecosystems, and preserves resident choice, while remaining fully aligned with Utah Code § 63A-16-1201.

We also emphasize adoption and inclusivity as critical success factors. SEDI must be simple to use, accessible across populations with limited digital literacy, and designed with recovery and support mechanisms for worst-case scenarios. Usability is a security requirement: if residents cannot use credentials easily and safely, adoption will falter, and protections will erode. A composite SEDI model lowers barriers to entry by allowing Utahns to opt in to the credentials most relevant to their lives, from driver licenses and professional licenses to permits and benefit eligibility proofs.

We recommend a multi-format issuance strategy that aligns with national and international standards. By relying on open, widely adopted standards, Utah can avoid vendor lock-in, accelerate adoption by verifiers, and maximize cross-jurisdictional acceptance.

Finally, we highlight the need for sustainable governance. Utah should treat SEDI as public infrastructure, funded as a shared good rather than a private service. By certifying multiple wallets and issuers against a published Utah SEDI profile, the State can foster a healthy ecosystem of vendors, spur innovation, and ensure residents retain choice while benefiting from consistent protections.

SpruceID is proud to already partner with Utah in digital identity innovation and stands ready to expand this collaboration. Our approach—rooted in standards, interoperability, privacy, and citizen

empowerment—offers a path to make Utah a recognized leader in secure, privacy-preserving, and practical digital identity.

II. SpruceID Overview & Experience

Spruce Systems Inc. (dba SpruceID) is a U.S.-headquartered company with a stated mission of letting users control their data across all digital interactions. SpruceID provides end-to-end solutions for digital licensing, permitting, and identity. We specialize in delivering lifecycle management systems for government-issued credentials that are secure, privacy-preserving, and interoperable across ecosystems. Our approach is built on verifiable digital credential (VDC) technology, which reduces the cost and complexity of in-person verification while protecting individual privacy in online interactions.

SpruceID's core platform, **Credible**, enables governments to issue, manage, and revoke digital licenses, permits, and identity endorsements that can be held in multiple wallet environments, including custom government applications or consumer wallets such as Apple, Google, and Samsung. Credible supports multiple agencies simultaneously through secure, isolated workspaces and deep system integrations, allowing states to modernize identity infrastructure without sacrificing security or usability.

Our record of delivery demonstrates the scalability and adaptability of this approach. SpruceID powers the California DMV mobile driver's license program, which features a privacy-preserving design that avoids any "phone home" or centralized server retrieval when a credential is presented. For this program, Credible has been deployed inside DMV infrastructure and integrated with DMV back-end systems. SpruceID also developed the public-facing CA DMV Wallet application, which enables Californians to store and present credentials such as driver's licenses and vehicle registrations. This program introduced industry-leading innovations, including dual-format issuance (ISO/IEC 18013-7 mobile driver's license and W3C Verifiable Credentials) and online presentation. To date, more than two million digital driver's licenses have been issued through this program.

In Utah, SpruceID has partnered with the Department of Government Operations to deliver verifiable credentials for permits such as off-highway vehicle education certificates and food handler permits. These pilots integrated Credible directly with Utah systems and enabled issuance of hundreds of thousands of verifiable credentials. This work has given us firsthand experience with Utah's statutory framework for digital identity and its commitment to privacy and unlinkability. We are therefore uniquely positioned to help Utah extend these pilots into a full-fledged SEDI program that balances interoperability with the technological compliance requirements outlined in Utah Code § 63A-16-1202.

SpruceID's team combines expertise in digital identity standards, user experience, and secure software engineering. Our leadership has held senior positions at companies such as Microsoft, AWS, Visa, and Fast Enterprises, and has contributed directly to standards bodies including W3C, ISO, IETF, and OIDF. This breadth of expertise ensures we can deliver solutions that not only meet Utah's requirements but also anticipate national and international interoperability demands.

Our value proposition lies in the combination of standards-based development, interoperability, public-sector delivery experience, technical excellence, and user-centered design. We have repeatedly demonstrated the ability to integrate with legacy systems, design modern citizen-facing applications,

and deliver production-ready solutions that operate securely at scale. Our approach emphasizes agile iteration, close collaboration with state agencies, and adherence to privacy and security principles that align with Utah's requirements.

Finally, SpruceID is committed to security and privacy by design. Our systems employ device attestations, hardware-backed key storage, hardware security modules, and advanced cryptographic techniques. We incorporate privacy-enhancing technologies such as selective disclosure, unlinkable identifiers, and revocation mechanisms that preserve anonymity. This combination of safeguards directly supports Utah's vision of a digital identity system that enforces compliance technologically, rather than relying solely on administrative rules.

SpruceID is proud to already be a partner of the State of Utah in digital credentialing innovation. We look forward to contributing our experience and technology to support GovOps in establishing a robust, trustworthy, and citizen-centric State-Endorsed Digital Identity program.

III. Legal, Regulatory, and Policy Considerations

1. What legal issues or other conflicts and concerns exist with the definitions as outlined in the Definitions section of this document and Utah Code § 63A-16-1201?

Overall, the definitions in Utah Code § 63A-16-1201 are well aligned with national and international best practices in digital identity, particularly the emphasis on the issuer–holder–verifier trust triangle, the avoidance of centralized credential storage, and the requirement that wallets be under the control of the individual. However, SpruceID observes several areas where refinement may be needed to avoid conflicts in implementation and ensure consistency with other state and federal frameworks:

1. **Definition of SEDI.** The current statutory language does not specify if SEDI is intended to be a single credential or a framework encompassing multiple credential types. We recommend clarifying in statute that SEDI is a framework, not a single monolithic credential. The framework applies primarily to foundational identity credentials, defined according to the World Bank as "an identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services." However, functional credentials, such as permits or entitlements, may reuse SEDI controls where appropriate and interoperate with SEDI-compliant wallets and verifiers, but need not be labeled SEDI themselves. This ensures flexibility and reduces the risk of misinterpretation while maintaining privacy and statutory principles.

2. **"Issuer" versus "Endorser."** The RFI defines both terms but treats them as interchangeable. In practice, these roles can be distinct. For example, the Department of Health may issue a food handler permit, while GovOps or the Driver License Division may act as an endorser of identity. Clear guidance is needed to delineate these functions (meaning those who generate credentials versus those who vouch for identity), particularly if the State allows for multi-agency issuance or endorsement of identity credentials. One such clarification could be that the state may issue credentials which endorse an individual's identity, but that there is no singular credential that seeks to define the individual's identity.

3. **Guardianship and Delegation.** The statute recognizes guardianship but does not address examples of the specific scenarios in which a digital solution would need to support it. Today, guardianship processes in Utah are fragmented across probate court, family court, and agency-level determinations, with no clear mechanism for digital verifications. Without clarity, agencies risk legal challenges if they inadvertently allow the wrong person to act on behalf of a dependent. Rather than treating guardianship as an abstract capability, we recommend that Utah identify a non-exhaustive list of key use cases it wants to enable. For example, a parent accessing school records on behalf of a minor, a guardian applying for healthcare or social services on behalf of a dependent senior adult, or a foster parent temporarily authorized to pick a child up. Each of these may require a different level of assurance, auditability, and inter-agency coordination. By articulating these scenarios, the State can better guide the design of SEDI features, ensuring that guardianship is implemented in a way that is operationally practical, rather than just theoretically technically feasible.

4. **Overlap with Federal Frameworks.** Federal requirements (REAL ID, TSA ID verification, immigration rules, etc.) may not accept a SEDI credential unless it is treated as a digital representation of the physical credential, or it may require an agency rule change. Depending on how SEDI is further defined, if the SEDI acts as a new type of digital credential with its own data format, not necessarily a mirror of existing credentials, this tension could lead to Utah residents being confused about where their SEDI works and doesn't work, as happened in other states where digital driver's licenses were released that were non-conformant with the data format accepted by TSA ("mdocs" as defined in ISO/IEC 18013-5). Legal clarification avoids residents being denied services or misled about the scope of acceptance.

5. **Verifiable Data Registry definition.** The way the VDR is defined here could accidentally imply that it stores user data, which could violate Utah's explicit prohibition on centralized storage. If the definition isn't carefully narrowed, agencies or vendors might interpret it as a mandate to build a large centralized identity database, recreating the very risks Utah law is designed to prevent. Clarifying that the VDR only contains issuer metadata, schema definitions, and revocation registries only, and having an agency responsible for its governance and allowed scope protects both privacy and compliance.

2. Should the SEDI exist as an additional method for individuals to prove their identity or should it mirror existing credentials in a digital form?

SpruceID recommends that Utah define the SEDI not as a single credential that a user can obtain, but as a framework of technical controls. These controls can be implemented through a variety of technologies, enabling many types of credentials to qualify as SEDI credentials if they comply with framework requirements, including technical maturity and interoperability. Under SEDI, these controls must apply in full to credentials appropriate for foundational identity use cases, ensuring strong privacy, unlinkability, minimal disclosure, and individual control. The same framework can also be applied piecewise to other credential types, allowing Utah to deploy the right safeguards for the right context. For example, a certain credential may require revocation mechanisms but not the full set of high-assurance controls, while all credential types might consistently adopt "no phone-home" verification as a baseline requirement.

This approach ensures that Utah does not have to choose between "mirror" and "additional method" but can deploy the right kind of SEDI-compliant credential for the right use case. The framework would

allow for Utah to issue digital-only credentials that would not be practical in the physical world. It also allows the State to move iteratively, prototyping, piloting, and refining credential types individually without requiring the entire ecosystem to be redesigned each time. By adopting a framework model, Utah gains the flexibility to meet federal requirements where needed, adapt to unsolved challenges like guardianship, and maintain interoperability with existing verifier ecosystems both inside and outside the state.

3. What challenges or advantages do you anticipate for the State once a viable SEDI program has been established?

A State-Endorsed Digital Identity program will provide Utah with immediate security and service delivery benefits. By enabling cryptographic verification and selective disclosure, the State can move beyond vulnerable methods such as usernames, passwords, and spoofable document scans. This strengthens protections against phishing, identity theft, and deepfake fraud, while also making it easier for residents to access services securely and more convenient for agencies to deliver them without requiring repeated in-person checks.

These improvements also translate into measurable economic value. Stronger identity assurance makes it easier for Utahns to securely and legitimately access the services they're entitled to, and could measurably cut rates of fraud for benefits programs. Streamlined digital service delivery decreases the costs of manual verification and paperwork processing, freeing resources for higher-value activities, and increasing efficiency and satisfaction by shortening the amount of time Utahns spend trying to access government services. In addition, private-sector reliance on government-backed credentials, particularly in finance, healthcare, and regulated industries, amplifies the return on investment by lowering compliance costs for businesses and reinforcing Utah's role as a reputable anchor of digital trust.

The largest barrier to success will not be technical feasibility but adoption. The industry's experience with mobile driver's licenses shows that uptake can be slow without clear incentives for both residents and verifiers. Coordination with federal authorities and private sector businesses will be essential to ensure SEDI is accepted in critical contexts such as TSA checkpoints and other REAL ID-covered access points, or presentation for access to regulated financial services such banking, lending, or stablecoins. If verifiers outside Utah must make custom changes to support SEDI, uptake may stall. Interoperability with established ecosystems is therefore the most important lever Utah can pull to drive real-world use.

To enable rapid and at-scale private-sector adoption, interoperability must be a central design principle. Businesses are unlikely to invest in new verification technology unless it aligns with ecosystems already gaining traction. Today, the mobile driver license (mDL) ecosystem (and its underlying protocols and data formats) represents the most likely path to rapid verifier adoption, as POS vendors, retailers, and financial institutions are already beginning to build toward it. By ensuring SEDI credentials are interoperable with the underlying data models and protocols defined in the mDL standards and ecosystem, while also forbidding features that may violate SEDI principles such as "no phone home," Utah can reduce adoption friction, accelerate private-sector uptake, and extend the utility of SEDI to the everyday transactions that matter most to residents. Equally important, residents must be able to use

SEDI credentials without facing steep learning curves or complex wallet setup; minimizing barriers to entry ensures adoption is not limited to only technically-sophisticated users.

Usability and user experience will be central to success: if the solution is difficult or confusing, adoption will lag and even security could be compromised, yet designing an intuitive experience for diverse populations is not trivial. Utah should expect the initial rollout may have imperfections; therefore, building in the capacity to adapt and iterate quickly based on real-world usage and feedback will be essential. A public education campaign highlighting the privacy-preserving attributes of SEDI will also be important to build trust and counter perceptions that the program represents increased government surveillance.

4. **What existing statutes, rules, or policies may need to be amended or updated to facilitate the creation and operation of a SEDI program consistent with Utah Code § 63A-16-1202? Please provide specific examples and proposed changes.**

First, statutes governing core identity documents should be updated to recognize SEDIs as a legally valid equivalent method of proving identity. Utah Code § 53-3-235 establishes the Electronic License Certificate Program and authorizes the Driver License Division to issue an electronic license certificate. However, as currently written, § 53-3-235 operates in parallel to § 63A-16-1202 rather than being integrated into them. To ensure clarity and consistency, § 53-3-235 should be amended so that an electronic license certificate is treated simply as a license when used to evidence driving privileges, but when it is used for identification purposes, it must be governed by the requirements in § 63A-16-1202. This alignment would bring the Electronic License Certificate Program under the broader statutory guardrails of SEDI, ensuring that when digital driver's licenses are used as IDs, they meet the privacy, unlinkability, and minimal disclosure standards mandated by law.

This reframing places the SEDI statute (§ 63A-16-1202) as the overarching authority for identity use cases, avoiding duplication and ensuring consistency across all identity credentials. It also strengthens Utah's leadership by positioning the SEDI framework as the governing standard for digital identity, while preserving the Driver License Division's role in managing licenses as credentials for driving privileges. This division of responsibility allows for checks and balances that can strengthen a republic, and agencies are able to better focus on their specialized tasks under their clear mandates.

Second, harmonization is needed between SEDI revocation limits and existing suspension authorities. Current provisions in Utah Code § 53-3-220 and § 53-3-231 give the Driver License Division broad authority to suspend or revoke licenses under various circumstances. By contrast, § 63A-16-1202 deliberately constrains revocation of SEDI endorsements to narrow, well-defined cases. To avoid conflict and preserve the statutory intent of SEDI, the appropriate approach is to narrow the scope of §§ 53-3-220 and 53-3-231 so that suspension of driving privileges does not automatically affect a SEDI endorsement. In this model, a license may be suspended for driving purposes, but its status as a valid SEDI credential for identification would remain intact unless the specific, narrowly defined SEDI revocation grounds apply.

Third, additional legislation should be enacted to establish a formal certification program for wallets, issuers, and potentially verifiers participating in the SEDI ecosystem. This program should be authorized under Title 63A-16 and harmonized with the Utah Consumer Privacy Act (§ 13-61) to ensure

statutory alignment. The legislation should specify that the designated regulating entity may conduct audits and certify providers directly, or delegate certification responsibilities to qualified external organizations, provided such delegation is formally approved by the appropriate higher authority.

This certification program would mandate compliance with privacy-preserving technical standards, restrict verifiers from requesting or storing more information than is legally required, and require wallets to obtain clear user consent before transmitting credential data. Wallets would also need to provide plain-language explanations of how data is used in each transaction. By creating a statutory basis for certification and oversight, Utah can ensure that unlinkability and data minimization are not just principles, but enforceable requirements with technological and governance safeguards.

We recommend that the State enact a pilot program allowing provisional, limited, and expiring operating approvals of issuers, wallets, and verifiers, preceding the establishment and full operation of its formal certification programs, for the purpose of encouraging market solutions to operate in real world environments and generate learnings. The appropriate oversight agency would be able to adapt the resulting learnings towards creating the formal certification programs. Today's best practice in the software industry has been to take an iterative "agile" approach towards implementation, and we believe this would be the best approach to creating certification programs for software as well, to fully engage industry early and often in a limited operating capacity, instead of attempting to fully specify rules a priori, which may become irrelevant if not created with perfect knowledge.

Finally, guardianship provisions should be updated to enable digital verification of lawful authority. Current guardianship is handled through disparate processes under the Utah Uniform Guardianship and Conservatorship Act (Utah Code § 75-5). Amending Title 75 to recognize digitally verifiable guardianship credentials would allow Utah to meet its statutory mandate to support guardianship and delegation in the SEDI ecosystem.

5. Are there any potential legal or regulatory barriers at the state or federal level that should be considered?

Several legal and regulatory barriers may affect the implementation of a SEDI in Utah. At the state level, existing statutes were drafted for physical credentials and may not clearly authorize digital equivalents in all contexts. For example, certain eligibility or benefits programs may require in-person identity verification by rule or statute. Without explicit recognition of SEDI as a legally valid proof of identity, agencies may be constrained in adopting digital credentials for remote service delivery. Similarly, fragmented guardianship processes under Title 75 could create uncertainty about who may lawfully act on behalf of minors or incapacitated individuals without further statutory clarification.

At the federal level, financial compliance laws represent one of the most significant barriers. The Bank Secrecy Act and implementing regulations under FinCEN require financial institutions to follow strict customer identification (CIP) and customer due diligence (CDD) procedures. Currently, these frameworks are built around physical identity documents. For SEDI to reach its full potential, federal rules and guidance will need to be updated to explicitly recognize digital credentials as satisfying CIP and CDD obligations. This alignment is essential not only for financial institutions but also for the U.S. Department of Treasury's ongoing work to provide clarity around digital identity, as recognized in its recent Request For Comment (RFC) entitled "Innovative Methods To Detect Illicit Activity Involving Digital Assets." Utah should anticipate these requirements and design SEDI to be compatible with

KYC/AML standards from the outset, while advocating for federal modernization that enables digital identity to reduce fraud and compliance burdens.

Interoperability with the REAL ID Act and Transportation Security Administration (TSA) rules is another critical consideration. For SEDI credentials to be accepted for air travel or at federal checkpoints, the credentials must meet the data and security requirements of REAL ID-compliant state driver licenses and align with ISO/IEC 18013-5/-7 standards. Until federal agencies formally recognize digital credentials beyond pilot programs, Utah will need to ensure that SEDIs can present a compliant subset of attributes in TSA contexts while still preserving privacy in other transactions. Federal privacy and data protection requirements, such as the Children's Online Privacy Protection Act (COPPA) and sector-specific health and financial regulations, also impose constraints on how identity data associated with SEDIs may be processed or disclosed.

Utah should also account for private-sector reliance and liability. Businesses such as bars, firearm dealers, and other regulated entities are often required by law to check IDs. Statutory clarification should ensure that when a business accepts a properly presented SEDI credential, it satisfies its legal obligations and shields the business from liability for relying on a state-certified credential. This protection will lower barriers to adoption in the private sector while promoting consistency across regulated industries.

Cross-jurisdictional acceptance is another area where legal barriers may arise. Other states may not recognize SEDI credentials unless they are explicitly harmonized with national standards or through robust coalition building, and private-sector verifiers may hesitate without clear guidance from federal agencies (especially if they are federally regulated such as the banking sector), or trusted platforms/brands such as the dominant wallet providers. Utah will need to mitigate these risks by adopting open and interoperable standards, aligning SEDI issuance with authoritative records that already satisfy federal requirements, and pursuing intergovernmental agreements to ensure recognition. By proactively addressing these barriers, Utah can map SEDI credentials directly to reducing compliance costs and increasing efficacy,creating a pathway for broad adoption across both government and private services.

6. What state regulations or statutes need to be modified or repealed?

Several statutes will require modification to ensure that identity functions are governed by the SEDI framework rather than by legacy provisions in the Driver License Division or other credentialing authorities. Today, Utah law implicitly treats driver licenses as both driving permits and primary identity credentials. To align with the statutory principles in § 63A-16-1202, identity powers should instead be vested in SEDI, with the DMV and other agencies retaining authority over the underlying functional credential (e.g., authorization to drive).

Specifically, provisions such as Utah Code § 53-3-220, § 53-3-231, and § 53-3-235 grant the Driver License Division broad powers to issue, suspend, and revoke electronic license certificates. These should be amended to clarify that such powers apply only to the functional driving privilege. When a driver license is used for identification, it must operate under § 63A-16 and the SEDI framework. This ensures that revocation, privacy, unlinkability, and minimal disclosure requirements are governed by SEDI protections, not by licensing authorities.

Similarly, any other statutes that currently embed identity functions in agency-specific credentialing programs should be harmonized by bringing the identity role under SEDI. For example, statutes related to professional licensing or vital records can continue to govern those programs' functional purposes, but when those credentials are used as proof of identity, they must comply with the SEDI framework.

By consolidating identity authority under SEDI, Utah avoids duplicative or conflicting rules, ensures that all digital identity transactions are governed by the same privacy and security requirements, and positions SEDI as the single authoritative framework for identity use in the state.

7. What legal frameworks or best practices from other jurisdictions with digital identity programs could inform the State's approach?

The most relevant precedent for Utah's future issuance of SEDI credentials is the federal mobile driver's license (mDL) final rule issued by TSA, which specifies many requirements around the issuance of an mDL, which cover important base measures including public key infrastructure, operational security of the organization, and privacy measures. It further does not mandate "phone home" behavior, and the actual credential format and presentation method are a small aspect of the overall content. The rule is the clearest example to date of how a U.S. regulator has set out requirements for issuers, wallets, and verifiers in digital identity in a way that has created production operational environments at scale. It establishes concrete safeguards for privacy, device security, and acceptance in regulated contexts such as airport checkpoints.

Utah can use this rule as a baseline reference point for SEDI, adopting the provisions that align with Utah's statutory principles while omitting (or even forbidding) those deemed inconsistent with unlinkability, minimal disclosure, and user choice described by SEDI. By generalizing from the mDL rule rather than being bound by it, Utah can ground SEDI in the most developed U.S. rulemaking while retaining flexibility to design an approach that works across multiple credential types, and explicitly disallow unlawful functionality such as "phone home" capabilities.

Europe provides valuable policy and privacy research through its eIDAS 2.0 program, but it also demonstrates the risks of leading with granular regulation instead of market alignment. Years of investment into open-source wallets and libraries have yielded limited adoption, and repeated delays have prevented traction at scale. Utah should draw from Europe's research on privacy-preserving design and governance models, but avoid its pitfalls by leading with statutory principles and then surveying the market for solutions that can conform to them. Unlike the EU, Utah should work with dominant wallets such as Apple, Google, and Samsung, alongside independent wallet vendors, to ensure broad adoption and adherence to the SEDI principles, without requiring every user to migrate to a state-specific wallet.

From an interoperability perspective, the ISO/IEC 18013 working group provides a strong example, with regular events convening both governments and technology vendors to demonstrate cross-vendor exchange of credentials. SpruceID hosted the first interoperability event for ISO/IEC 18013-7, which included successful participation from NIST, Okta, Samsung, Google, Panasonic, and other global organizations. Utah could replicate this approach for SEDI, convening staged demonstrations and publishing results to build confidence and accelerate adoption. Additionally, the OpenID Foundation (OIDF) regularly hosts interoperability events which include usage of ISO/IEC 18013-7, but also public

and open standards such as usage of IETF SD-JWTs, W3C Digital Credentials API, and OpenID for Verifiable Presentations (OID4VP). SpruceID has participated in many OIDF-hosted interoperability events, towards technical maturity of its solutions. Joint demonstrations across many vendors has accelerated a technology's path to technical maturity, and we believe that SEDI credentials would benefit from a similar approach.

Similarly, programs like NIST's National Cybersecurity Center of Excellence (NCCoE) underscore the importance of engaging relying parties early and continuously. NCCoE has already aggregated input from banks, healthcare providers, retailers, and technology vendors to validate workflows for digital identity. Utah should follow this model by establishing structured forums where SEDI requirements are co-designed with verifiers, ensuring adoption is smooth and operationally feasible.

Within the U.S., lessons can be drawn from other state pilots. High-population states have shown how early interoperability testing with TSA (through the TSIF program) validates credentials against federal requirements before statewide launch. Other states have also shown the importance of aligning statutory definitions of "bona fide identity" to explicitly authorize digital credentials in contexts such as alcohol sales, firearm purchases, and other regulated transactions. Utah should update its own statutes, including the Alcohol Beverage Control Act and related administrative rules, to ensure that SEDI credentials are recognized as valid proof of identity wherever state law requires ID presentation. This recognition should be coupled with liability protections for private-sector verifiers: if a bar, retailer, or federally licensed firearm dealer accepts a properly presented SEDI, it should be deemed compliant with its legal obligations.

Internationally, India's DigiLocker illustrates both the promise and the risks of digital identity platforms. DigiLocker has reached over 550 million users with more than 9.4 billion documents issued. Legally, India has elevated the status of documents shared via DigiLocker to be on par with physical originals under IT Rules 2016, with benefits including increased access to banking, faster delivery of public services, and reductions in document fraud. However, its highly centralized architecture creates metadata exposure risks and concentrates trust in a single government-operated repository. Such a model would not be appropriate for Utah or many states within the United States. Instead, SEDI can achieve the same public benefits through a decentralized framework, where multiple issuers, wallets, and verifiers interoperate under statutory guardrails. By decentralizing trust, Utah can ensure that residents enjoy access, security, and fraud reduction benefits without replicating the risks of centralization, which were for example exploited in the Office of Personnel Management data breach in 2015, leaking 22.1m records on Americans, including sensitive documents for government security clearances and background checks.

Combined, these lessons point to a practical path for Utah: draw on the TSA mDL final rule as a baseline; leverage EU research without replicating its regulatory overreach; build on ISO and OIDF interoperability successes through Utah-led demonstrations; align statutory definitions to recognize SEDI in regulated transactions; and prioritize decentralized architectures that preserve privacy, unlinkability, and individual control.

8. 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?

Compliance with Utah's privacy statutes should be embedded directly into the design and governance of SEDI, ensuring that protections are enforced through both technology and policy. One approach is to use personal data licenses, where every credential presentation carries machine-readable terms that specify how the data may be used, for how long it may be retained, and whether it may be shared. Wallets can enforce these licenses automatically, creating automated privacy compliance that is consistent with statutory requirements and reducing reliance on after-the-fact enforcement.

Utah could also establish the principle of reasonable disclosure, defining contextual norms for when certain attributes may be shared. For example, in a bar setting, presenting "over 21" is a reasonable disclosure, but if the bar requests an email address, that exceeds the scope of the transaction and must be flagged or presented differently. An insurance company might ask for someone's basic history, but additionally requesting genetic indicators of future disease may be considered unlawful or predatory. Embedding these rules into wallet UX and verifier obligations ensures that disclosures remain consistent with Utah's privacy laws while still supporting legitimate use cases.

It is a very difficult but important task to determine the proper governance around agreeing upon "reasonable disclosure" across many different industry use cases. We believe that one entity would not be able to make good judgements across all industry verticals, and so industry engagement is critical for this to be successful. Further, it remains unclear if a government agency is the best entity to coordinate these efforts, versus non-profits, cooperatives, or even private companies specializing in digital reputation management. This is a hard and open problem in decentralized identity, but necessary to create the benefits while managing the risks of increased user control.

It is our strong preference that this should operate in a decentralized manner, with wallets mediating requests and issuers not serving as intermediaries for every transaction. We believe that enforcement of these reasonable disclosure frameworks should be composable across many different sources and list maintainers, and ultimately configured at the wallet level. We should "push decision-making towards the edges" as much as possible, while ensuring reasonable defaults which provide an acceptable trade-off between user choice and safety.

To further protect residents, Utah could consider imposing an insurance requirement on verifiers or entities that retain personally identifiable information (PII). This creates a financial incentive to minimize data collection and retention, while ensuring that residents are protected if breaches occur. Utah could also consider strongly restricting the appropriate request criteria SEDI credentials, which would transmit PII and result in full identification. Finally it would also be possible for wallet providers to align on a privacy-preserving fraud signal mechanism, where relying parties overcollecting data are detected via anonymized aggregated reporting so that investigations and enforcement can take suitable action.

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

Clear allocation of liability and responsibility is essential for the trust and sustainability of the SEDI program. The State's role is to establish statutory guardrails, oversee governance, and authorize a

certification framework that ensures all ecosystem participants meet consistent standards. This includes creating a certification program for both digital wallet providers and credential issuers, verifying that they comply with Utah's statutory principles for privacy, unlinkability, minimal disclosure, and security. Certification could be managed by the State directly or delegated to accredited third parties, but it must be anchored in statute to carry legal force.

Digital wallet providers bear responsibility for ensuring acceptable security mechanisms, proper user consent, presenting clear and plain-language disclosures which meet accessibility requirements, and ensuring features like personal data licenses and privacy-protective technical standards are honored in practice. Certified wallets must also support recovery mechanisms for key loss or compromise, ensuring that holders are not permanently locked out of identity credentials due to technical failures. Digital wallet providers should coordinate with issuers, designing solutions which anticipate that wallets and keys will be lost, stolen, and compromised.

Issuers are responsible for creating a strong operational environment that ensures the accuracy of the attributes they release, and for maintaining correct and untampered authoritative source records. They are also responsible for ensuring that SEDI credentials are issued to the correct holders, and to any acceptable wallets, free of unreasonable delay, burden, or fees. They must provide accessibility to holders, such as providing workable paths for holders who lose their credentials, wallets, and/or keys. Their certification ensures that SEDI credentials are issued only under audited processes that meet required levels of identity proofing and revocation safeguards.

Verifiers should have a statutory obligation to identify themselves appropriately to holders for any information request, such as through presentation of a cryptographically verifiable organizational ID. This ensures that holders can have the ability to verify the identity of the requestor of their data prior to sharing it, whether it is a business entity, government agency, or individual. The degree of required verifier identification will depend on the context, which would have similar industry coordination and governance criteria required as those described for "reasonable disclosure" in (III.8). Verifiers must also limit collection to reasonable disclosure norms, retain only what is necessary, and carry insurance if they choose to store PII, aligning financial incentives with privacy preservation.

Finally, holders are responsible for maintaining control of their own wallets and approving data disclosures. However, liability should remain limited: if holders act in good faith and use a certified wallet, the risk of misuse or over-collection should fall on verifiers and not on residents themselves. Penalties are appropriate as well; holders who use credentials to knowingly commit fraud should face consequences.

10. 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 should legislate certain aspects of the relationship between Digital Wallet Providers and Holders to ensure that statutory principles under Utah Code § 63A-16-1202 are enforced consistently across the ecosystem. Digital wallets are the primary interface through which citizens will exercise control over their SEDI credentials, and legislation is the clearest way to guarantee that privacy, unlinkability, and individual control are preserved regardless of which vendor provides the wallet.

At a minimum, legislation or appropriate agency rulemaking should specify that wallet providers must:

- Store credentials under the control of the Holder, using hardware-backed keys where available, and prohibit the provider from accessing or transmitting credential contents without the Holder's consent.
- Support selective disclosure and unlinkability as much as possible, so Holders are not forced to reveal more information than necessary or risk correlation across verifiers.
- Prohibit "phone-home" to the state or 3rd parties, and tracking functionality that does not attain proper user consent, ensuring that wallet use cannot be monitored by unapproved third parties or the State.
- However, with proper user consent, it should be possible for the user to utilize a hosted "cloud wallet" that could receive requests over the internet at any time, or actively delegate authority for specific actions to the user's AI agent.
- The State may consider imposing requirements on fiduciary duties that the wallet provider must maintain for its users to remain certified.
- Provide clear user interfaces for lifecycle events such as credential revocation, expiry, and recovery, consistent with statutory requirements.
- Comply with Utah's consumer protection and privacy laws, including the Utah Consumer Privacy Act, with explicit remedies for misuse or breach.
- Ensure accessibility and inclusivity, including compliance with WCAG and Section 508 standards, support for screen readers, high-contrast modes, multiple languages, and simplified flows for residents with limited digital literacy.

In addition, the State should require certification of wallets against a published SEDI protection profile and create clear liability rules. Legislation should establish that wallet providers are responsible for implementing technical safeguards, that Holders maintain control over disclosure decisions, and that verifiers may only request attributes that are legally permitted. By legislating these aspects, Utah will ensure that citizens can trust any certified wallet to uphold their rights, while fostering a competitive ecosystem of providers who innovate on usability and design within a consistent regulatory baseline.

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

Under a SEDI framework model, a SEDI credential meets all of the statutory and technical controls required by § 63A-16. SEDI credentials are reserved for foundational identity use cases, where a resident's core attributes (such as full legal name, date of birth, and proof of Utah residency or lawful presence) must be verified and endorsed with strong privacy, unlinkability, minimal disclosure, and device binding. Because SEDI credentials must implement the full suite of technical protections, they offer Utahns and verifiers the greatest level of trust, integrity, and legal certainty.

At the same time, not every credential needs to rise to the level of a SEDI. Other state-issued credentials (such as professional licenses or permits) can mix and match elements of the SEDI

framework depending on what is appropriate for the use case. For example, a certain credential may need revocation mechanisms but not the full identity-proofing requirements of a foundational credential, while all state-issued credentials should consistently adopt “no phone-home” as a baseline requirement. This flexibility ensures that Utah can apply the right safeguards in the right situations, without overburdening lower-assurance credentials. This gives agencies the ability to create the best solutions for their specific mandates, and a common criteria for the Office of Privacy and other supervisory agencies to conduct efficient evaluations.

The framework should also enable derived or privacy-preserving assertions across both SEDI and non-SEDI credentials. Examples include proofs such as “over 21,” “Utah resident,” or “holds a valid professional license.” These contextualized disclosures allow residents to share only what is needed for a given transaction, consistent with statutory requirements for minimal disclosure and individual control.

Sensitive or persistent identifiers, such as driver license numbers, state-issued unique identifiers, or user-managed (self-sovereign) unique identifiers, should be used sparingly and only when necessary. Their inclusion must be paired with safeguards to prevent linkability across transactions and to ensure the benefits clearly outweigh the risks. Similarly, when sensitive attributes such as Social Security numbers, biometric templates, or detailed address histories are incorporated into SEDI credentials, the issuer should have specific written guidelines on their proper handling to ensure that the principles of data minimization are upheld.

When the State contemplates mandating acceptance of SEDI credentials, we recommend that it also clarify to verifiers which attributes are required for a given category of use cases. Different SEDI-compliant credentials may vary in the attributes they contain, such as choosing to include or omit biometrics. SEDI credentials should include an explicit indicator of their proofing and assurance level (e.g. IAL2 vs. IAL3 under NIST SP 800-63A, or the Fair/Strong/Superior classifications for identity evidence and verification strength defined in that standard). Some use cases might require biometrics or a higher-level of proofing, while others may only require core identity attributes; verifiers should request only the minimal attributes necessary, ensuring Utahns retain flexibility in how they prove their identity.

In our recommended approach, SEDI credentials must have all of the SEDI controls, whereas other credential types may selectively apply SEDI controls as appropriate.This allows Utah to maintain a consistent governance framework, while enabling innovation across a broad ecosystem of credentials.

If SEDI is instead treated as a single credential, then the attributes endorsed within it should be limited to the minimal set of core attributes needed to legally establish identity. A state-issued unique identifier could be included as necessary, but should employ careful safeguards to mitigate the privacy risks of persistent identifiers. As with the framework approach, the credential should enable privacy-preserving derived assertions as much as possible to minimize disclosure in everyday transactions.

In all cases, the State should avoid embedding unnecessary or highly sensitive attributes by default, which would create risks without providing clear benefits. If these attributes are embedded due to requirements or by user request, then we recommend that there are clear written guidelines and policies which would prevent the overcollection of user data, and prevent the normalization of requests for strong identity. This helps to avoid a dystopian “checkpoint society,” in which a state endorsement is required for any action.

12. What should the criteria be for an individual to receive a SEDI?

An individual's eligibility to receive a SEDI-compliant credential should be defined in future legislation that duly expresses the will of the people of Utah; whether it is made available to residents or also to non-residents, whether there are age restrictions, whether it must be obtained in person or if remote provisioning is possible, whether out-of-state sites can also provision an in-person credential to an individual, whether certain criminal histories affect one's eligibility, etc. The framework should also allow for different types of SEDI foundational identity credentials to be available for different groups of people, with each type containing only the attributes necessary for its intended use cases. For example, some SEDI credentials may include biometrics for higher-assurance contexts, while others may omit them to support groups (e.g. minors) for whom lighter, minimal-attribute credentials are more appropriate. We believe that the public square is the best forum to decide these criteria in a free and democratic society, and the most productive framing would be criteria as they enable the most important cases for Utahns, and unlock innovation.

After an individual is demographically eligible for a SEDI credential, the technical perspective of identity proofing requirements may be applied. SEDI credentials represent the highest bar and eligibility for issuance should be limited to cases where strong identity proofing can be achieved. At a minimum, issuance of a SEDI credential should require NIST 800-63A-4 IAL2 with strong biometric matching, or IAL3 proofing, with in-person enrollment used for IAL3-level credentials. The credential itself should reflect the assurance level under which it was issued, so that relying parties can distinguish between different grades of SEDI when determining suitability for a given use case. For example, a SEDI credential issued at IAL3 could be accepted for secure physical building access similar to a DoD CAC card, while an IAL2 with strong biometric matching SEDI credential could be sufficient for access to benefits or other service eligibility checks. There may be alternatives to use of the NIST 800-63A-4 levels that can help make tradeoffs to help increase accessibility without sacrificing security in specific scenarios, but we believe that NIST 800-64A-4 would be a strong starting point in the right direction, and it would be possible to describe exceptional scenarios where other approaches are appropriate, such as in the case of a minor without stable biometrics.

We would not recommend issuance of SEDI credentials below IAL2 with strong biometric matching, except in narrowly defined circumstances where the credential is explicitly limited in scope or duration, such as lightweight credentials designed to support access to shelter or services for homeless residents who may not have the documentation required for higher-assurance proofing. Even in these cases, such credentials should be clearly distinguished from full SEDI credentials, both in how they are represented and in the contexts where they may be accepted, even if they implement many (or all) of the SEDI controls. SEDI credentials should also meet any NIST 800-63B-4 AAL requirements necessary for digital evidence or cryptographic verifiable attribute bundles to be considered high quality evidence for future identity proofing.

Other state-issued credentials that may not necessarily rise to the level of SEDI (such as professional licenses, recreational permits, or library cards) may continue to use eligibility criteria defined by their issuing authorities, and can selectively apply SEDI technical controls as appropriate for their use case. For example, a professional license may use SEDI's revocation and no-phone-home rules, but not require the full identity-proofing standard of a foundational credential.

Revocation and duplication of SEDI credentials should remain tightly constrained by Utah Code § 63A-16-1202, ensuring that endorsements are only withdrawn in narrow cases such as fraud, verified ineligibility, or security compromise.

By anchoring SEDI credential issuance to rigorous identity proofing (NIST 800-63A-4 IAL2 with strong biometric matching or IAL3) and explicitly reflecting that level within the credential itself, Utah can ensure that SEDI serves as the State's highest-assurance digital identity, usable across both government and regulated private-sector contexts, while still allowing lighter-weight credentials to operate under the same statutory and technical framework where appropriate.

13. Are there any additional situations where a SEDI should be able to be revoked?

Utah Code § 63A-16-1202 already limits the revocation of a SEDI endorsement to narrow circumstances in order to preserve trust and predictability for residents. In most cases, revocation should not be tied directly to the suspension or revocation of underlying credentials such as a driver license, since those events reflect the individual's eligibility to exercise certain privileges rather than their core identity. Instead, a suspended license should simply render the relevant entitlement inactive, while the SEDI remains valid as a representation of the individual's identity.

That said, Utah may wish to consider additional narrowly tailored grounds for revocation beyond those already specified. These could include confirmed cases of identity fraud (e.g., discovery that the SEDI was issued under false pretenses), verified compromise of the cryptographic keys securing the credential, or a court order determining that the endorsement must be withdrawn. In each case, the grounds should be clearly defined in statute, revocation processes should be auditable, and status mechanisms should allow verifiers to distinguish between revoked and non-current credentials. This approach ensures that revocation remains an exceptional event, applied only when necessary to preserve the integrity of the system while safeguarding individual rights.

For credentials that operate as SEDI credentials but also contain other entitlements, such as demonstrating driving privileges in the case of a mobile driver's license, we recommend that the entitlement portion of the credential is managed under the appropriate agency (e.g., the DMV in the case of a driver's license), while the credential's continued operation as a SEDI credential remains subject to Utah Code § 63A-16-1202.

For example,

- **Suspension of privilege (e.g., DUI, unpaid child support, expired professional license):** SEDI remains valid, but the entitlement appears inactive.
- **Loss of eligibility (e.g., non-residency, permanent disqualification from license):** SEDI remains valid, but the specific entitlement is marked revoked.
- **Identity fraud discovered (credential obtained under false pretenses):** SEDI is revoked in full. A SEDI holder could request revocation if they suspect fraudulent usage.
- **Compromise of cryptographic keys (e.g., stolen device keys, compromised private keys):** SEDI is revoked and re-issued with new keys.
- **Court order (judicial directive to revoke digital identity):** SEDI is revoked if required by the order.

- **Death of holder:** SEDI is handled properly upon official notice.

Utah could also adopt a “user-maximalism” approach, where holders retain the ability to present even an expired or revoked credential if they choose. In such cases, verifiers would be able to check the credential’s revocation status, fraud signals, or key compromise indicators under the statutory provisions. This model ensures that decision-making is pushed to the edges, allowing verifiers to apply context-specific judgment, while preserving the State’s authority to determine the legitimacy of SEDI credentials. It also gives residents more control and transparency, since they can see how verifiers treat their credentials in practice.

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

There are several potential funding models for the SEDI program, including consumer convenience fees, verifier subscription models, transaction-based cost sharing, or reliance on vendor-provided services. Each of these can play a role in offsetting operational costs, or generating profit centers. However, because digital identity is a foundational capability that underpins participation in government and daily life, the most sustainable approach is to treat SEDI as public infrastructure.

A public infrastructure model ensures the program remains universally accessible, avoids creating inequities through usage fees, and provides the stability necessary for long-term adoption. Initial funding can come from legislative appropriations, supplemented by federal grants where available, with ongoing costs integrated into existing credentialing and licensing budgets. Other mechanisms, such as optional convenience fees for expedited services or modest contributions from high-volume verifiers, can supplement but should not replace a baseline of public funding.

By positioning SEDI as public infrastructure with broad political and fiscal support, Utah can ensure that the program remains durable, trusted, and responsive to residents’ needs over the long term.

In one alternative and more decentralized model, it would be possible to rely upon certified private sector issuers of SEDI credentials, that are duly contracted for proxy issuance for agencies which have authority to issue SEDI credentials. These private sector issuers could charge a fee for issuing a SEDI credential. It would be possible to introduce a voucher model so that relying parties ultimately pay for an individual’s SEDI credential issuance, which may come under cost for other verification methods depending on the SEDI credential issuance process.

Finally, we believe that models which charge the user for usage of a SEDI credential are detrimental for adoption if there are not immediate use cases that are of large benefit to end users. We recommend avoiding these schemes, or exercising extreme caution and strong justifications must be made for this direction to produce a viable credential ecosystem.

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

Utah has an opportunity to set a high bar for privacy-preserving and citizen-centric guardianship in the SEDI program. Guardianship in digital identity is a complex and, as yet, unsolved problem. A guardianship solution should accept decisions from the entities legally empowered to make them,

represent those decisions in credentials rather than recreating them, and keep endorsements current as circumstances change.

The first step is to enumerate today's pathways to establishing guardianship and to identify which entities are authorized to issue evidence. This mapping enables cohesive implementation and prevents confusion about who can issue what. In parallel, the program should catalog current use cases and requirements by clarifying which agencies authorize which actions and what evidence each verifier needs. Where authorities differ, Utah can allow agencies to issue guardianship credentials that reflect their scope while still unifying common steps to reduce friction. Unification should not displace the entities and courts with the most context and legal mandate. As a future enhancement, the state can gather candidate use cases that digital proof of guardianship could unlock once security and fraud concerns are addressed.

From this map of authorities and use cases, Utah should define a clear guardianship credential taxonomy. There are multiple ways to define guardianship depending on legal and operational context, such as parental authority, foster care, medical consent, or financial guardianship. We recommend making these definitions explicit, ideally in a simple visual framework, so distinctions are clear and responsibilities are traceable. This will naturally lead to multiple guardianship credential types, tailored to definitions, use cases, and issuing agencies. For example, one agency may issue a credential for parental or custodial rights, while another may issue a credential for healthcare decision-making authority.

Digital delivery introduces several challenges that the program should address up front. Endorsements need to change cleanly at the age of majority or when a court modifies an order, including a clear transfer of control to the individual. Reissuance and backstops should be specified for lost devices or keys and calibrated to the chosen technical models. Rollout should be iterative so pilots can surface operational realities and feed refinements. The design should remain flexible enough to accommodate emerging topics, including AI agent-based interactions, without locking in assumptions that are likely to shift.

A practical flow follows from the taxonomy. The state issues a unified, SEDI-compliant guardianship VDC to each guardian, device bound as appropriate and with proof of key possession, containing only minimal data about the ward such as full name and date of birth. Alternatively, the state could offer a lower-assurance base guardianship VDC which requires presentation alongside a SEDI-compliant identity credential Verifiers can request additional evidence, such as a paper or digital birth certificate, when needed. Specific authorities are expressed through additional guardianship VDCs at suitable assurance levels, including verification flows that require more than one presentation when multi-party consent is required. For limited and precise authority, the system supports scoped delegation credentials with explicit expirations. Either the state issues a limited delegation credential at the guardian's request, or the guardian issues a self-sovereign delegation credential that follows a published schema and references the guardian's own guardianship credential. Credentials should reference related evidence as needed. Depending on the use case, hashes, links, or identifiers can connect credentials to each other. Examples include KERI ACDCs that link to other ACDCs, a VDC that carries the hash of a related credential, or a stable identifier for the ward used across presentations.

A few assumptions and concerns should be validated as part of implementation planning. Agencies and courts differ in process and data availability, so clarity about which entities can issue what is required before buildout. Timely updates are critical for transitions such as the age of majority or modified

orders, so the state should confirm how these changes will be surfaced to the credential layer. Device binding raises assurance but also accessibility and recovery considerations that should be right-sized by use case. Self-issued delegations improve flexibility but add operational complexity and need clear policy guidance so verifiers know when they are acceptable. Verifier practices on collection and retention should be limited to what is necessary and supported by program guidance to meet privacy goals.

Finally, we emphasize a strong preference for pushing decision-making towards the edges. We believe that the overall system for guardianship should maximize the ability for appropriate and contextualized exercise of human judgement by responsible individuals. A teacher should have the ability to override if her visceral experience disagrees with the strongly issued guardianship credential, such as if they've never seen an adult before who wishes to claim the child, and the child seems scared; this should escalate to a due process with oversight for more robust consideration without unreasonable delay. A law enforcement officer who sees dozens of children being shuffled across state lines by organized adults ought to be able to exercise probable cause, even if there is a full valid set of guardianship credentials. No doubt, the elderly are likely victims of future fraudulent issuance of guardianship credentials, with fraudsters tricking them into designating guardians who then drain retirement funds entirely. All of these systems, even protected with cryptography, security measures, and fraud detection, will still be faulty. They should be designed to prioritize humans and their wellbeing, even with failures and fraud present.

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

Utah should require or at least express strong preference that the technical standards used in the SEDI program be open, freely available, and implementable by the public and private sector without proprietary licensing restrictions. Open standards are critical to ensuring transparency, interoperability, and long-term sustainability. They allow agencies, citizens, and vendors to independently verify that the technology operates as intended, building public trust in a system where privacy and unlinkability must be enforced by protocol rather than policy alone.

Freely available standards also support interoperability across jurisdictions and with federal programs, and they also allow for smaller vendors to more easily meet the requirements. This is much more likely to result in a competitive market environment, which was evident in the case of the internet's adoption of open protocols such as HTTP and TCP/IP and a variety of web development firms or technology startups entering the market. If SEDI credentials can rely upon open protocols, holders are far more likely to be able to use their credentials beyond state borders, verifiers can more readily adopt the technology without prohibitive costs or licensing fees, and the State avoids lock-in to a single vendor or proprietary solution due to a competitive market of solution providers.

At the same time, Utah should recognize that openness alone does not guarantee privacy or compliance. Standards should be evaluated not only for accessibility but also for alignment with the statutory principles in Utah Code § 63A-16-1202, including individual control, technological compliance, and data minimization. The State's role should be to publish a clear "SEDI profile" that specifies which open standards are suitable and how they must be configured to enforce privacy-preserving features.

To maintain relevance and adaptability, Utah should also establish a governance process for updating the SEDI profile. This process should include structured input from public agencies, private vendors, civil society, and technical experts, and ensure that updates are guided by both statutory principles, technology maturity, and real-world market adoption.

This approach ensures that Utah benefits from the innovation and global adoption that open standards enable while maintaining control over the protections that are uniquely important to Utah residents.

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

Utah should rely on open protocols to the greatest extent feasible in the SEDI program. Adoption will be far faster if the State aligns with protocols already in use because verifiers and private-sector partners (in Utah, in the United States, and globally) are already beginning to adopt those standards. Adoption is ultimately driven by how many verifiers are able and willing to accept a credential, and using open standards that already have traction will help de-risk the program by ensuring compatibility with the broadest set of verifiers.

Open protocols also ensure that the methods of issuance, holding, and verification can be independently reviewed, tested, and implemented by both public and private actors. This reduces the risk of vendor lock-in, enhances interoperability, and strengthens transparency by demonstrating that features such as unlinkability and minimal disclosure are built directly into the technology.

The role of open source software should be carefully balanced. Open source can increase accountability and public confidence, allowing security researchers, civil society organizations, and other governments to inspect implementations for compliance with Utah Code § 63A-16-1202. It can also increase the ability of small firms to enter the market that provide differentiated solutions for specific use cases, while also meeting SEDI credential requirements.

However, not all open source projects are developed or maintained at the same level of maturity. If the State were to release or ordain immature open source implementations as "official," it could create new risks through rushed or under-resourced deployments that could contain security flaws or bugs.

To mitigate this risk, Utah should require that any open source software used in the SEDI ecosystem demonstrate active community support, regular updates, and independent security audits. The State should maintain even higher standards for software it releases officially, such that it does not "pick technology winners" and create adverse incentives in competitive markets meant to deliver the best solutions at the lowest costs. Where projects do not meet these maturity thresholds for open source software, the State should consider certification requirements or mandate third-party audits to ensure confidence. This balance allows the State to demonstrate transparency while still protecting sensitive operational components. Even when open source software is audited, it does not obviate the requirement for end-to-end systems which incorporate them as components to go through their own audit, as security models are extremely sensitive and dependent upon contextualized use.

Finally, Utah should focus on open standards and projects with well-established, actively supported ecosystems that are able to reach long-term sustainability. Technical standards with broad governance

and multiple implementers encourage innovation, ensure interoperability across jurisdictions, and reduce the risk of Utah relying on under-supported technologies. By combining reliance on open protocols, balanced use of open source, and rigorous independent audits, Utah can build a program that maximizes adoption, transparency, and security in equal measure.

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

Yes, the State should require certification of Digital Wallets that are capable of holding a SEDI. Certification provides assurance that wallet providers comply with Utah Code § 63A-16-1202 and that key requirements—such as privacy preservation, unlinkability, minimal disclosure, and security of key material—are enforced by design. Without certification, there is a risk that wallets may vary widely in their treatment of sensitive identity data, leading to inconsistent protections for citizens and possible noncompliance with statutory requirements.

Certification also creates a mechanism for interoperability and trust across the ecosystem. By publishing a clear “SEDI Wallet Protection Profile” and certifying wallets against it, Utah can ensure that wallets from different vendors operate consistently while still allowing for competition and innovation. This is the model used in other regulated environments such as payment card systems and FIDO-certified authenticators. Certification would test not only conformance to technical standards but also compliance with Utah-specific policy requirements, including support for guardianship, revocation, and transparency features.

There must be a continuous degree of evaluation, as software updates could change the nature and therefore SEDI conformance of digital wallets. Digital wallet providers should not go through undue burden or require business-hostile IP terms, but it may be reasonable for the State to inspect binary artifacts or even codepaths on an ongoing basis to ensure that they are free from major design flaws or harmful features. The balance across frequency of review and depth of review must be found, which is another reason why we recommend a pilot program in earlier sections.

Finally, certification helps build public confidence. Citizens will know that any wallet bearing a certification mark has been independently tested and approved to uphold privacy and prevent surveillance, while verifiers will know they can safely interact with those wallets. At the same time, Utah should keep certification processes lightweight and transparent to avoid excluding smaller vendors, ensuring that certification supports security and privacy without stifling innovation. Also, wallet certification programs should consider requirements around sustaining the national defense, with special procedures and guidelines followed for evaluating wallet products implemented in whole or in part by foreign adversaries, non-democratic regimes, or entities without clear liability structures. This balance will allow Utah to foster a healthy ecosystem of wallet providers while maintaining the high level of trust required for SEDI adoption.

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

To ensure that SEDI credentials can be accepted in other jurisdictions, Utah should ensure that the SEDI framework is compatible with data formats and protocols that have received large investments and are broadly acceptable, to the extent they are compatible with SEDI principles. Credential formats

such as W3C Verifiable Credentials, mdocs found in the ISO/IEC 18013-5/7 specifications for mobile driver's licenses, the forthcoming ISO/IEC 23220 which describe mdocs standalone, or SD-JWTs from IETF have received significant investments and growing adoption in the United States and abroad. Emerging protocols and credential primitives such as KERI/ACDCs, Bitstring Status List, CRSet, and Longfellow are entering production use cases globally, and should be carefully monitored and incorporated where appropriate to ensure SEDI credentials benefit from new technologies.

By ensuring that SEDI credentials are compatible with these particular formats without compromising on SEDI principles, Utah maximizes the likelihood that other states, federal agencies, and private-sector entities will be able to validate and trust Utah-issued credentials without requiring custom integrations. A best practice emerging in the field is multi-format issuance, where credentials are simultaneously provisioned in both ISO mDL (ISO/IEC 18013-5/-7), IETF SD-JWT, W3C VC, and/or other formats. This ensures acceptance in federal and regulated contexts that require ISO compliance, such as TSA checkpoints, while still supporting broader digital use cases like online eligibility verification and cross-border interoperability.

It is important to note that adoption in other jurisdictions is not automatic simply because a credential is standards-compliant. Verifiers in other states and federal agencies will only integrate technologies that align with the ecosystems they are already adopting. If Utah did not support major protocols, the program could face significant delays in recognition and limited utility outside the state. By taking a framework approach to SEDI that can create protections in a way compatible with dominant standards today, Utah reduces its adoption risk and accelerates acceptance across both government and private-sector contexts, towards providing usable, efficient, and cost-effective solutions for its residents while maintaining SEDI principles.

IV. 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?

Utah should establish clear policies and procedures to ensure that issuance, use, management, and revocation of SEDIs are governed by principles of security, privacy, and citizen control. A central requirement is that control of the public key infrastructure underlying SEDI, especially control of the root key(s), remains with the State, not wholly controlled by a vendor. This model provides accountability and prevents any outside entity from holding unilateral revocation power.

Policies should also address how issuers and verifiers handle data collection and disclosure. The State should provide guidance to relying parties to ensure that they only request information that is necessary and appropriate for a transaction. Wallets should enforce a reasonable disclosure framework that gives users meaningful choices and warnings when a verifier requests excessive data, similar to how a web browser prompts users before allowing risky actions. This approach places control with the individual and reduces the risk of overcollection of sensitive information.

From a lifecycle perspective, the State should take a pro-individual stance. Wallets, whether state-provided or third-party, should allow holders to present expired credentials or signatures, leaving it

to verifiers to determine whether the information remains acceptable in a given context. At the same time, Utah should establish a targeted revocation mechanism for cases of fraudulently issued credentials, which will inevitably occur at scale, for example if a DMV employee is compromised. Such revocation must be effective and recognized by all verifiers, but designed in a way that does not create unnecessary surveillance or tracking of individual use. This balance ensures the program can protect against fraud while remaining aligned with statutory commitments to privacy and individual control.

To reinforce accountability and individual protections, Utah should also mandate periodic independent audits of the SEDI ecosystem, require issuers and wallet providers to maintain detailed event logs, and ensure that holders are promptly notified of any revocation actions with clear processes to contest them.

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.**

We recommend a framework model for SEDI because it supports iterative rollout, prioritizes adoption, aligns with Utah's emphasis on individual choice, and reduces risk of lock-in. If a monolithic approach is preferred, it should rely on broadly adopted, widely supported standards to ensure long-term security and scalability. The table below compares these models across key factors.

Factor	SEDI Monolith Credential	SEDI Framework for Credentials (Our Recommendation)
Description / Qualities	A single, canonical SEDI credential, or a single identifier (self-sovereign or state-provided) to which all credentials accrue. This is likely to be implemented by an entirely uniform stack of technical standards.	A framework of technical controls (proofing, privacy, minimization, etc.) applied consistently across multiple credential types to meet obligations in § 63A-16. A "SEDI credential" is any credential that meets the full framework requirements (e.g. Veteran ID, digital driver's license, state photo ID), while other credentials may implement an appropriate subset of controls or require co-presentation with a SEDI credential.
Budget	Depends on the complexity of the chosen format or identifier. Likely lower short-term cost and complexity for a single credential (e.g. mDL). For a self-sovereign identifier, likely as complex or more than a framework model. Long-term changes would require costly, system-wide redesigns.	Incremental and use-case driven. New SEDI-compliant credential types can be introduced iteratively without disrupting existing ones, reducing long-term risk. Older credential types may be gradually deprecated as newer technologies become available, such as to add post-quantum cryptography. A subset of framework controls can be applied to additional non-SEDI credentials where appropriate.
Security	Consistency and standardization simplify enforcement. Security/privacy tradeoffs are inherited directly from the chosen credential format and exact implementation.	SEDI credentials must meet baseline security requirements, including IAL2/IAL3 assurance. Implementations may differ in how they balance usability and additional security features, provided the framework controls are met. Other credentials can adopt only the controls needed for their use cases. Avoids a single point of failure.
Adoption	Simple in that holders only need one credential, and verifiers only accept one. Riskier as an all-or-nothing approach if residents resist that credential (e.g., due to privacy concerns or technical barriers) or if it	Utahns can adopt relevant credentials piecemeal , lowering holder adoption barriers. The State must also ensure verifier acceptance of different SEDI-compliant credentials across use cases so holders have confidence their chosen SEDI

	fails to meet diverse needs.	credential will be recognized.
User Choice	Limited: holders either accept the canonical credential or are excluded from SEDI benefits.	High: holders can select among SEDI-compliant credentials, all of which meet baseline security and privacy requirements. For example, one resident might opt for a State-endorsed Veteran ID, while another prefers a digital driver's license. The State should guide residents on available options and their tradeoffs (e.g. usability, privacy, security) so individuals can make informed choices.
Scalability	Scales only within the limits of the chosen protocol; new use cases may require major redesign.	Horizontally scalable by use case. New compliant credential types can be added without disrupting existing ones, as long as they meet framework controls. Different SEDI credential implementations might also compete on speed and efficiency.
Flexibility/Adaptability	Potentially inflexible and harder to adapt to emerging or complex use cases (e.g., guardianship, selective delegation).	Highly adaptable by adding new credential types while still enforcing common controls. Supports mirrored credentials as well as novel, unsolved use cases (e.g. guardianship) via iterative pilots and evolving standards.
Identifier Linking	Possible when all credentials attach to a single identifier, but this creates serious linkability concerns since users could be tracked across contexts.	Some credentials may be linked by a self-sovereign or state-provided identifier if permitted by the framework, but others can stand alone. The framework encourages unlinkability and minimal disclosure by default.
Decentralization	Centralized around a single state-issued credential or identifier. This concentrates authority and infrastructure, raising risk of bottlenecks or systemic failure.	Distributed across multiple issuers and credential types, all adhering to the SEDI framework. Supports separation of contexts, reduces reliance on a single operator, and allows interoperability across technologies.
Market Sustainability	Creates a winner-take-all vendor dynamic where a single vendor issues all the credentials, or several vendors are running near-identical technologies.	Allows for many vendors to participate in providing different aspects of SEDI compliance, as a subset of the controls defined in the SEDI framework are usable for a long tail of credential use cases that include permits, licenses, and even private sector uses like employee badges or student IDs.

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

SpruceID has direct experience delivering digital identity systems through our work with the California Department of Motor Vehicles. SpruceID provides the underlying technology for California's mobile driver license (mDL) program, which is among the largest and most advanced digital identity initiatives in the United States. A core design principle of our approach for this program was implementing safeguards to reduce the potential for issuer-verifier collusion and eliminating "phone-home" dependencies, so credentials can be validated locally without creating surveillance risks or exposing transaction metadata to issuers. Although this option is available in some technical specifications, SpruceID already takes measures to ensure that these kinds of behaviors are not possible at the implementation level, instead of relying on configuration flags or settings. These design choices directly align with Utah's statutory principles of minimal disclosure, unlinkability, and individual control, ensuring

that residents can trust their credentials to work securely without unnecessary oversight or data collection.

As part of this program, SpruceID deployed its Credible platform within the California DMV environment and integrated it with DMV backend systems to support issuance, lifecycle management, and verification of mDLs. In addition, SpruceID designed and built the consumer-facing CA DMV Wallet application, which allows residents to securely store and present their digital credentials. The application supports both in-person and online transactions and enables presentation in dual data formats: ISO/IEC 18013-5 and -7 mobile driver licenses, and W3C Verifiable Credentials. This dual-format issuance was a first-of-its-kind innovation that ensures Californians can use their digital IDs in TSA testing environments, interstate pilots, and broader digital interactions.

The California DMV Wallet has already been downloaded by millions of residents, with more than two million mDLs issued to date. It has earned strong ratings from users, with 4.8 stars on the Apple App Store (over 91,000 reviews) and 4.8 stars on Google Play (over 18,000 reviews), reflecting SpruceID's emphasis on usability, accessibility, and privacy-preserving design. In addition, the system was architected to support additional DMV use cases beyond driver licenses, such as vehicle registration and title credentials, creating a foundation for a multi-credential, multi-agency ecosystem. This has demonstrated the ability for the program to reach scale, maintain high levels of security and privacy, while also rapidly iterating on new functionality for users.

This experience demonstrates SpruceID's ability to work in close partnership with a state agency to deliver a production-grade, standards-compliant, and citizen-friendly digital identity program at scale. It also highlights our capacity to innovate in alignment with both international standards and U.S. federal pilots, while integrating deeply with legacy government systems to ensure reliability and continuity of service.

While not an identity credential, SpruceID has also deployed its technology in Utah through the State's Verifiable Digital Credential (VDC) program. Using the Credible platform, we worked directly with multiple agencies to issue digital permits and certificates, including off-highway vehicle permits and food handler cards. These credentials were delivered as verifiable digital credentials that can be securely presented online or in person, demonstrating the flexibility of the technology in a wide range of state service contexts.

This program has already reached tens of thousands of Utah residents, sent out hundreds of thousands of credential offers, and serves as a production pilot for how verifiable digital credentials can streamline service delivery, reduce fraud, and improve user experience while preserving holder privacy. It also reflects SpruceID's ability to collaborate effectively with Utah agencies, integrate with existing state systems, and deliver solutions that align with statutory privacy and security requirements, and solve real problems for Utahns. Our work on Utah's VDC program provides a proven foundation for expanding into higher-assurance use cases like a State-Endorsed Digital Identity.

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

The SEDI program should stay current with technology trends by anchoring its evolution on real-world use cases and allowing for a SEDI framework instead of a monolithic credential. By focusing on the

services most important to residents and relying parties (such as proof of age, secure online access to government benefits, and cross-jurisdictional interoperability), Utah can ensure that any updates to the program are driven by practical needs using a variety of technologies that all meet requirements around SEDI controls, interoperability, and sustainability. This approach allows technology churn to become more manageable, mitigates centralization risks across deployments, and prioritizes improvements that directly enhance usability, security, and trust.

To support long-term sustainability, Utah should adopt mature, widely supported, and interoperable technologies wherever available. By minimizing reliance on niche or proprietary technologies that lack broad market support, Utah can ensure that SEDI remains adaptable to future advancements while avoiding vendor lock-in and ecosystem fragility.

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.?

The State already participates in federal and state-level pilots around digital credentials, including the verifiable digital credential program and the mobile driver's license program. These existing investments provide a foundation that can be extended to support SEDI without requiring wholesale replacement of systems. The key is to layer SEDI atop these efforts while constraining implementations to remain compliant with § 63A-16-1202's privacy, unlinkability, and individual control requirements.

Under this model, SEDI is not a collection of all digital credentials, but a framework that sets the highest bar for credentials representing foundational identity. Credentials must meet the full set of technical and policy controls, including rigorous proofing, device binding, selective disclosure, and privacy-preserving revocation, to be classified as SEDI credentials. Other digital credentials issued by the State, such as professional licenses or permits, can continue to operate under their own issuance rules, but they may selectively adopt specific SEDI controls where appropriate. This ensures consistency of protections across the ecosystem without diluting the assurance level of SEDI itself.

To guide implementation, Utah should ground SEDI issuance practices in the TSA's mDL Final Rule, generalized to cover all SEDI credentials and disallowing features that may violate SEDI controls. These requirements, covering proofing rigor, secure credential delivery, and privacy-preserving verification, represent the clearest regulatory model in the U.S. and can be applied as the baseline for SEDI issuance, even beyond driver licenses.

Utah should also consider participation in NIST's National Cybersecurity Center of Excellence (NCCoE), particularly Track 3 pilots focused on vital records and other foundational credentials, as to increase awareness at the state and federal level of SEDI's benefits. NCCoE's model of aggregating verifier requirements and validating interoperability in controlled pilots is a best practice that Utah can replicate for SEDI, ensuring usability, scalability, and security are proven before broad deployment.

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

There are no inherent technological barriers preventing most credentials from being issued in digital form, but there are important constraints that Utah should consider when determining which credentials to digitize. Some constraints are legal and regulatory: federal acceptance of digital credentials, such as at TSA checkpoints, currently requires conformance to ISO/IEC 18013-5/7 mobile driver license standards and successful completion of TSIF testing. Similarly, state statutes governing proof of identity in age-restricted transactions or other regulated areas may need to be updated before digital-only acceptance is legally recognized.

Another constraint arises from ecosystem maturity. Credentials that rely on widely adopted standards, such as mobile driver licenses under ISO/IEC 18013-5/7, IETF SD-JWT, IETF CWT, or general-purpose identity credentials using W3C Verifiable Credentials, can be supported digitally with confidence. For more specialized credentials, such as certain professional licenses or permits, digital issuance is possible but requires careful attention to ensuring interoperability and verifier adoption. In these cases, Utah may find it necessary to issue credentials in both physical and digital formats during a transition period to ensure continuity of service.

Finally, Utah could benefit its residents by ensuring physical credentials are an easily available option (as required by SEDI) that also provide an important form of offline fallback. Not all verifiers, particularly in rural or resource-constrained environments, will have the technical capacity to validate digital credentials in the near term. Certain physical documents could also be upgraded to include cryptographic signatures, for example through verifiable bar codes, providing an optional way to enhance their security and enable compatibility with the same verification tools used for digital credentials. Maintaining issuances of documents in many different valid forms meeting the same security standards and SEDI control requirements, especially in the case of certain high-assurance documents, will ensure that residents retain universal access to services while the digital ecosystem matures, without getting left behind in a digital divide.

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

Based on our experience, there are advantages to both centralized and regional issuance, depending on how SEDI is defined.

If SEDI is treated as a framework, Utah could support both centralized and regional credentials within the same system. A central state-issued digital ID remains the most straightforward option for high-assurance use cases such as REAL ID compliance, banking, or TSA acceptance. These contexts require consistency of governance, technical controls, and trust anchors, which are best delivered by a single authoritative source. Central issuance also makes it easier for Utah to participate in interstate and federal trust frameworks without raising questions about which authority issued the credential or whether it meets the required standards. Within a central model, the State could still issue multiple forms of ID with varying assurance levels, giving residents flexibility while ensuring uniformity in high-stakes contexts.

At the same time, a SEDI framework approach can accommodate regionally scoped credentials, such as county or city IDs. These credentials could comply with the entire suite of specified technical controls or adopt only a subset relevant to their use case. These could provide access to local services or benefits while remaining clearly jurisdiction-bound. Importantly, there would be no requirement that a credential issued by a regional authority be accepted at the state or federal level; instead, they would be useful within their defined scope, under the judgment of the issuing jurisdiction. This allows for innovation and service expansion at the local level without creating confusion or undermining trust in state-level credentials.

Another important consideration is the costs and skillsets necessary to set up and maintain a public key infrastructure, which may be challenging for a county or city to manage if they lack dedicated IT experts and resources. In these cases, it could be possible to lean on another entity's public key infrastructure, such as the State, to finalize credential issuance. Some counties and cities may have no interest nor ability in maintaining their own PKI and root keys, and managing federation. However, we believe it is possible to pursue hybrid models where all the data are held by the locality, and the State lends its public key infrastructure without collecting additional data past pseudonymous metadata related to issuance. There may be ways to add light key management capabilities for IT leadership in localities without requiring a full PKI setup. This model would allow for fraud investigations to be conducted, but only if the locality and the State agreed to collaborate in reidentification of the transaction producing the credential.

By defining clear requirements, the SEDI framework can ensure consistency for state-issued foundational identity credentials, while also offering a reference point that regional authorities may draw from. Local credentials could choose to adopt relevant security and privacy best practices from the framework without being required to comply fully, allowing innovation at the local level while maintaining trust in state-level SEDI credentials.

However, if Utah chooses to approach SEDI as a single credential, state-endorsed digital identities are best issued centrally rather than regionally. Central issuance ensures consistency of governance, technical controls, and trust anchors, which are critical for high-assurance use cases such as REAL ID compliance, banking, and federal acceptance at TSA checkpoints. In these environments, verifiers depend on knowing that the credential originates from a single authoritative state source, with uniform policies for issuance, lifecycle management, and revocation. A centralized model strengthens Utah's position in interstate and federal trust frameworks by minimizing questions about which entity issued the credential and whether it meets required standards.

By contrast, a regional model introduces unnecessary complexity. If multiple regional authorities were to issue SEDIs under varying procedures or levels of capability, verifiers outside Utah would face difficulty in determining which issuers can be trusted. This fragmentation would reduce confidence in the credential, slow adoption, and complicate technical interoperability. While regional offices can and should continue to play a role in onboarding residents and verifying documents, ultimate issuance should remain centralized to ensure that every SEDI reflects a uniform standard of trust.

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

Ensuring accessibility and inclusivity in a SEDI program requires thoughtful technical design, clear policies, and supportive service delivery. First and foremost, the program should prefer simplicity wherever possible, ensuring that residents can use SEDI credentials without needing advanced technical knowledge. Digital credentials should remain optional, with physical credentials available for those who prefer them, so that no resident is excluded for lack of access to technology. Wallet applications should comply with WCAG and Section 508 accessibility standards, supporting screen readers, high-contrast modes, multiple languages, and intuitive, plain-language interfaces. These requirements should span interactions that the user has with issuer components and verifier components, to the extent they are run by the State. It should be generally encouraged as a best practice for the private sector as well. Accessibility requirements for state employee or contractor usage should apply to internal-facing interfaces such as dashboards and control panels.

Usability must also be treated as a component of security. A system that requires perfect user behavior to remain secure is, by definition, not a secure system. Secure mechanisms such as key management, rotation, and recovery must be usable in practice. For example, if residents are required to manage their own PKI or identifiers, the risks should be clearly explained, the user experience must be fully usable by someone with no technical experience other than familiarity with a mobile device through their day-to-day use. There must be robust account recovery and restoration mechanisms in place for worst-case scenarios like key compromise or loss of device. It is possible to add additional protection mechanisms to prevent unlawful situations such as device handover under SEDI. NIST guidance and established computer security principles emphasize this linkage between usability and security, and SEDI should adopt the same standard: mechanisms that are secure on paper but unusable in practice should not be deployed.

Education and transparency are also critical. End users should be informed not only about how to use SEDI-compliant credentials, but also about the technical risks, their responsibilities, and the protections available to them. In-person assistance at DMV and county offices, multilingual tutorials, and partnerships with community organizations can help reach populations with limited digital literacy or English proficiency. We recommend that the education is built into the user interfaces as part of the digital onboarding experience for digital wallets and any other user-facing components. Without training and awareness and effective visual indicators, it is difficult to prevent users from oversharing their data whenever they are requested, resulting in data privacy risks.

Finally, the program should build in user choice, recognizing that residents' circumstances differ. This includes providing both online and offline options for credential use, so that residents can decide what works best in their situation, as well as fallback options such as printed QR codes, smartcards, or service kiosks for those without personal devices. The State should evaluate uptake and use by various population segments to safeguard against leaving people behind. By combining simplicity, usability, education, and user choice with strong accessibility requirements, Utah can ensure that SEDI protects all residents while remaining consistent with the statutory principles of privacy, unlinkability, and individual control.

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

Utah should encourage a diverse ecosystem of vendors, including smaller companies and startups, by maintaining open certification and procurement processes. This ensures that the market does not consolidate around a single provider and that innovation continues. Under a SEDI framework approach, there is no requirement that every credential type be issued using the same vendor software. Instead, multiple issuers and technology providers can participate so long as they comply with the common trust framework, SEDI profile, and certification standards. This allows, for example, one vendor to issue digital driver licenses and another to issue Veteran ID, giving residents flexibility while keeping the overall system interoperable and cohesive.

The State can foster collaboration and interoperability by defining the technical controls that every SEDI credential must satisfy, including unlinkability and minimal disclosure, without mandating a single implementation approach. Solutions should be required to use open and widely adopted standards to meet those controls, ensuring interoperability across vendors and jurisdictions and avoiding lock-in to proprietary methods. By requiring the use of standards with broad ecosystems and publishing clear SEDI profiles that define attributes, disclosure rules, and certification requirements, Utah ensures that private-sector entities and other governments can readily integrate SEDI without custom one-off work. This lowers barriers to participation and strengthens trust in the program.

The State should also create structured avenues for ongoing engagement and collaboration with partners. This includes convening advisory groups with representatives from financial services, healthcare, education, retail, and consumer advocacy and social welfare organizations, as well as with federal and interstate partners. Early engagement allows Utah to validate real-world workflows, incorporate feedback into technical profiles, and demonstrate interoperability in pilot environments. Programs such as NIST's National Cybersecurity Center of Excellence (NCCoE) mDL initiative and TSA's TSIF testing have shown that sustained collaboration with relying parties is key to adoption. Utah can follow this model by scheduling staged interoperability demonstrations and publishing results to provide transparency and build confidence.

Finally, the ultimate strength of the SEDI framework approach is that the technical controls which must all be implemented for SEDI credentials, may be used piecewise as appropriate for other credential types for use cases like permitting and licensing, or even in the private sector. This also creates the opportunity for firms to specialize in managing aspects of SEDI, which lowers the barriers to market entry and creates opportunities especially for smaller and newer vendors to work on particular problem sets. It also allows deep specialization to produce best-in-class products, such as if a company wanted to focus primarily on aspects of guardianship and providing the best user experience, instead of also being required to implement all aspects of SEDI to provide a market solution for a smaller market.

We believe the framework approach to SEDI would produce a larger, more diverse market, ultimately allowing the State and its agencies and also the private sector to have many choices from vendors, with many of them local to Utah who are able to specialize the technologies to . This ability to create the best possible products even across non-SEDI credentials.

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

- **Anchor on everyday use cases and make them visible.** Prioritize scenarios people already do: proof-of-age, traffic stops, airport screening, campus/health check-in, and benefits access. Colorado's myColorado program highlights everyday uses and publishes who accepts Digital ID, which normalizes usage and reduces uncertainty for residents and clerks. Utah can mirror this with a public "who accepts SEDI" directory and signage kits.

- **Line up marquee acceptance to create a flywheel.** Secure and publicize acceptance at TSA checkpoints and major employers/retailers recognized by consumers such as Amazon, CVS, and others. TSA now lists participating states and checkpoints where digital IDs are accepted with CAT-2 readers; being on that list materially boosts perceived legitimacy and travel utility. We suggest coordinating Utah's roadmap with TSA's TSIF/CAT-2 deployment and keeping residents informed. Foster adoption with verifiers by demonstrating how SEDI credential acceptance enhances and streamlines compliance, improves fraud prevention, and ultimately can lead to savings.

- **Enlist relying parties through a formal partner program.** For example, Colorado runs a Partner Program and publishes participating businesses and law-enforcement agencies; it also provides a simple "how to verify" guide for front-line staff (visual checks plus tech options). Utah could launch a SEDI Partner Program with logos, window decals, training one-pagers, and a searchable directory, plus an RP sandbox and sample code.

- **Use policy to unlock adoption, while keeping physical fallback.** Executive or administrative directives can authorize acceptance across state agencies, while clarifying that physical ID remains a fallback until digital ID is ubiquitous. Utah should pair statewide acceptance guidance with updates to ABC/bona-fide-ID rules so retailers can accept SEDI credentials legally.

- **Reduce verifier friction with certification and toolkits.** Offer a lightweight verifier certification, reference SDKs, and test suites so banks, hospitals, universities, and retailers can integrate quickly and confidently. Publish privacy-centric SEDI profiles (minimal disclosure, unlinkability) and require conformance for "trusted verifier" status.

- **Issue in dual formats to maximize utility across contexts.** Where appropriate, provision credentials in ISO/IEC 18013-5/-7 (for TSA and AAMVA ecosystems) and W3C VC/OpenID4VC (for web and app flows). This mirrors the emerging best practice in U.S. pilots and ensures one credential works both in person and online, today and cross-border tomorrow under EU-style wallet models.

- **Stage adoption with pilots and public scorecards.** Follow the "test-prove-scale" pattern used by TSA/NCCoE: run multi-party pilots, publish interoperability results, and expand in waves. Public scorecards (on uptime, pass rates, and RP adoption) build confidence and keep vendors aligned with Utah's SEDI profile.

- **Incentivize participation via carrots, not just mandates.** Offer small integration grants or fee waivers for early verifiers; pre-certify point-of-sale and age-check vendors; and recognize "SEDI-Ready" partners in a public directory to drive foot traffic.

- **Design for accessibility and inclusion.** Utah should ensure wallets/verifiers meet accessibility requirements from day one to broaden eligible users and avoid exclusion.
- **Communicate clearly and often.** Provide resident-facing guidance that SEDI complements, not replaces, physical ID during the transition, including plain-language FAQs. Use simple explainer pages and in-app education to demystify where SEDI credentials are accepted and why privacy protections are stronger online than showing a full physical card. Educate users about security risks and how to use their SEDI safely, to promote trust and transparency.
- **Prioritize ease of use and low barriers to entry.** Making SEDI easy to use safely is a key prerequisite to adoption. The more complicated SEDI is to set up and use, the higher the risk of compromised credentials and a loss of trust.

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

Utah should ensure that residents can access services equally whether they present a physical or digital credential. Service delivery should not depend on whether someone has adopted digital ID, and government offices must be designed so that both options are supported consistently. The most effective way to achieve this is to make SEDI credentials and physical IDs interchangeable at the point of service by anchoring both in the same authoritative data sources.

Some physical documents and credentials could be augmented with verifiable bar codes, providing enhanced security and leveraging the same verification tools used for equivalent digital SEDI credentials. This allows agencies and businesses to use the same workflows for both physical and digital transactions. At the same time, issuing credentials in widely adopted formats such as ISO/IEC 18013 and W3C Verifiable Credentials ensures interoperability with TSA, interstate frameworks, and online services. Additionally, it could be possible to have hybrid approaches such as DoD's CAC program, which has physically verifiable authenticity features such as watermarking and holograms, but also cryptographically signed credentials that are machine verifiable, containing biometrics for verification as well. Smart cards are also candidate form factors for this hybrid approach, which could hold many different credentials and support stronger privacy features as well, in addition to physical authenticity features.

It will be very important to educate those working in government entities on how to validate SEDI credentials. We recommend an official knowledgebase that describes all the acceptable SEDI credentials that can be obtained, and instructions on how to validate each one and qualified products to use for attaining different levels of identity proofing. These different verification processes for SEDI credentials can be given referenceable codes that are useful to agencies in their own rulemaking, so that they do not have to define a new verification process when an existing one is fully defined and well-supported.

By designing for dual-format acceptance and equipping agencies with standardized verifier toolkits, Utah can support both physical and digital populations efficiently, reduce complexity in service delivery, and maintain compliance with statutory requirements.

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

Utah should recognize wallet certifications that are widely established in digital identity and security ecosystems to ensure interoperability, privacy, and trust. The following certifications represent strong options the State may choose to recognize, while not being an exhaustive list:

- **State direct audit or State delegated audit:** The state can run its own certification program using existing audit professionals who are qualified to cover the necessary aspects of organizational security and technical compliance in a State-defined certification program. With this approach, it is possible to have safety and compliance for iteratively developed systems before industry creates a complete audit process for the technologies, ensuring a faster pace of development and overall better safety outcomes. The downside of this approach is increased resourcing necessary to collaborate with industry and define the necessary controls and enforcement protocols. This downside can be mitigated by relying upon existing frameworks which have completed audits, such as NIST's identity-related standards or the relevant controls in TSA's rulemaking around mDLs, and incorporating them as they become available.

- **FIDO Alliance certifications**: Provide assurance for authentication mechanisms and secure key management. FIDO Certified implementations demonstrate the use of hardware-backed keys, phishing-resistant authentication, and proven cryptographic protections that align with Utah's statutory requirements for security and individual control. We believe that the FIDO working groups are beginning to consider wallet certification.

- **Kantara Initiative certifications**: Cover governance and operational practices such as identity proofing, credential lifecycle management, and privacy protections. Kantara's Identity Assurance Framework and CSP assessments are leveraged by U.S. federal programs and offer a strong model for evaluating wallet compliance with policy and governance requirements. They, or an adjacent body, are well positioned to consider wallet certification.

- **FIME certifications**: Focus on technical interoperability with ISO/IEC 18013-5 and related mDL/mDoc standards. FIME is the established certification body for mobile driver license and mdoc conformance, which is particularly important for ensuring Utah-issued credentials can be accepted at TSA checkpoints and in regulated environments.

- **Other government or international certifications.** Utah may also consider recognizing certifications developed by other governments or international bodies, such as those associated with the European Union's eIDAS 2.0 framework or emerging ISO/IEC conformance programs. However, any such certifications must first be reviewed against Utah's SEDI framework to confirm alignment with statutory principles. Certification schemes that lack explicit requirements for unlinkability, no phone-home, or minimal disclosure cannot be adopted wholesale; they must be adapted or supplemented to ensure conformance with Utah law. This safeguard ensures that Utah can benefit from global best practices while maintaining the higher bar of privacy and resident control that SEDI requires.

Utah may require wallets to demonstrate compliance with one or more of these certifications depending on the assurance level and use case. The general approach should be to rely upon relevant industry standards and/or substandards as much as possible, have the Utah certification evolve to incorporate new developments as the industry evolves, to the extent they improve alignment with SEDI controls.

The State could also layer Utah-specific certification criteria on top, to ensure statutory requirements such as unlinkability, minimal disclosure, and prevention of issuer tracking are enforced consistently.

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

We recommend that the state consider doing so, either (i) as part of a broader citizen portal initiative for secure and convenient access to state services or (ii) as an open-source standalone wallet that serves as a usable reference implementation that is fully SEDI compliant, with a high focus on accessibility, and limited feature sets. However, whether Utah should issue its own digital wallet as part of the SEDI program is ultimately a policy decision for the State and its residents.

Providing an optional state-issued SEDI wallet component as part of a larger citizen portal application can help Utahns access to government services securely and conveniently, while also being able to use the SEDI credential in other places too. This approach can help the agencies better accomplish their mandates while also reducing fraud. However, if this approach is taken, we would recommend ensuring that those government services can be used with other SEDI wallets as well, and that it would be possible to disable the SEDI wallet component in the government maintained application if the user wishes.

The standalone open-source digital wallet approach creates an opportunity to create a public option that is fully aligned with the mandate and principles outlined in SB 260, without the additional commercial incentives that may influence private-sector wallet providers. A state wallet can be designed to maximize compliance with statutory requirements for privacy, unlinkability, and minimal disclosure, ensuring a baseline level of trust and accessibility for all Utahns. However, thought must be given to this approach, as not to disencourage private sector adoption and participation for SEDI wallet certification.

A state-issued wallet, whether standalone or integrated into a citizen portal app, would also benefit from independent review and public transparency. By publishing the code or subjecting the wallet to third-party audits, Utah could demonstrate that it adheres to the necessary technical controls and does not introduce hidden risks. This level of reviewability would complement the private wallet certification program, where third-party vendors can compete to innovate while being held to the same statutory and technical standards.

Together, the two approaches would provide residents with both choice and assurance. In practice, this model mirrors approaches seen in other jurisdictions where a public wallet is offered alongside certified private wallets, ensuring broad adoption while preserving competition and innovation.

In addition, we recommend that Utah make it as easy as possible for others to create their own wallets that can interoperate with SEDI credentials. Even with a state wallet, adoption will only scale if multiple wallets interoperate smoothly with the same verifiers. Providing tools for third-party wallet providers ensures that SEDI credentials integrate into existing ecosystems and do not become an isolated solution. This could include providing verifier SDKs, example code, documentation, and compliance test suites so new wallet providers can build to Utah’s requirements with minimal barriers. Lowering the cost and complexity of participation will encourage a healthy ecosystem of wallet options and broaden adoption across residents and verifiers.

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?

Utah should design methods for updating SEDI credentials to reflect life events, such as legal name changes or the addition or removal of guardians, anchored in authoritative sources in a way that preserves accuracy and trust while recognizing the limits of purely technical solutions.

Under a SEDI framework model, updates flow through the specific credential type affected rather than through a single record. This opt-in, component-based structure gives residents flexibility while ensuring that each credential reflects authoritative source records.

Updates to authoritative records (such as court orders or DMV records) should automatically flow into the SEDI credential lifecycle, allowing the updated credential to be reissued or refreshed. At the same time, Utah should consider the requirement that expired or superseded credentials can still be presented from SEDI wallets, so relying parties can access information that could assist them make fully contextualized decisions upon the user's consent to disclose, even if the credential is expired or revoked. This maximizes individual freedoms while also providing mechanisms to fight fraud.

The SEDI framework should require that as much credential validity information as is appropriate and necessary to be made available to the relying party, and that clear indicators of the credential's current status are available to holders. The role of the State is to provide reliable, verifiable data, while leaving the policy decisions as close to the edge as possible, where they naturally occur. For example, if a guardian presents a SEDI credential when picking up a child from school, the school should be able to view the authorization, assess the context, and apply human judgment. This requires not only technical safeguards but also training for relying parties on how to interpret digital verifications alongside existing procedures.

It is equally important to prevent abuse of the system. The State must ensure that guardianship credentials cannot be issued or accumulated in ways that could enable fraud, such as one person holding dozens of guardian endorsements to unlawfully access benefits or facilitate trafficking. Revocation and audit mechanisms must exist for fraudulently issued or abused credentials, while still preserving unlinkability and minimizing surveillance.

By anchoring each credential type in authoritative records and requiring updatability in the SEDI framework, Utah can ensure that SEDI remains both flexible, rights-respecting, and trustworthy across life events.

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?

To increase adoption of the SEDI program, Utah should prioritize use cases that deliver immediate value to residents and relying parties. Anchoring the program in common transactions such as proof-of-age, airport security, and access to state services ensures that SEDI becomes relevant in daily life. The State should also make SEDI credentials easy for organizations to adopt by providing standardized verifier toolkits, SDKs, and certification pathways. Early engagement with banks, healthcare providers, schools, and retailers will help Utah align requirements with existing workflows

and reduce the integration burden. Clear public education on the privacy protections built into SEDI will further build trust and confidence.

A decentralized identity approach strengthens these adoption efforts by giving residents confidence that their credentials remain under their control, not stored in centralized databases. SEDI framework requirements such as selective disclosure, unlinkability, and cryptographic proofs would make participation safer for both residents and verifiers, while reinforcing statutory principles around privacy and minimal disclosure. This model also enables an ecosystem of vendors to flourish, since multiple wallets, issuers, and verification tools can operate under the SEDI framework so long as they conform to the same trust standards. In this way, Utah can increase adoption by demonstrating both security and choice for users and partners alike.

Utah should also avoid approaches that could hinder adoption. The most significant barrier for relying parties is complexity or cost in implementation. If verifier solutions are hard or expensive to deploy, organizations (especially smaller businesses or local agencies) will be reluctant to participate. It could also lead to centralized verifier APIs or services being used, which may introduce risks around overcollection of data, tracking, and user data privacy. Adoption could also be undermined if digital credentials are positioned as a mandatory replacement for physical IDs, or if residents perceive the system as surveillance-oriented.

Therefore it is also critical that full transparency about the program and its operation are made available to the public, but also explained in a way that assumes no technical background. This might also be combined with campaigns where trusted members of the local communities and notable figures who have high integrity, reputation, and concern for citizen privacy engage with the program, educating the public on SEDI controls. Public engagement is critical, and we would like to see the town halls continue adding diversity of thought, ideology, and geography by having more local communities in Utah participate and engage.

Additionally, if digital credentials are more cumbersome or complex to set up and manage than paper credentials, holders may be disincentivized from using digital ID entirely. Another risk is choosing a niche technology that lacks cross-jurisdictional acceptance or a healthy community of support; such a choice would limit interoperability, restrict innovation, and weaken Utah's ability to integrate with federal and interstate trust frameworks.

V. 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 should recognize that there are multiple technical standards and architectures capable of supporting the goals of the SEDI program. Each approach—whether based on ISO/IEC mobile documents (mdocs), W3C Verifiable Credentials, X.509 PKI, or event-log systems such as KERI—offers different strengths and tradeoffs. The role of the SEDI framework should be to clearly

outline and encode policy goals (e.g. security, privacy, unlinkability, and minimal disclosure, use of open standards), describe technical controls ("SEDI controls") which have been proposed, reviewed, and confirmed to achieve those policy goals without "picking winners" in the market of technology, and leave flexibility in how they are achieved. Each foundational identity use case can then adopt the technical standard best suited to its context, provided it complies with the framework's required controls. What matters most is not prescribing a single technology, but ensuring that any future solicitations anchor to the statutory principles in Utah Code § 63A-16-1202: individual control, unlinkability, minimal disclosure, and technological enforcement of privacy.

By framing requirements around these principles, Utah can remain open to innovation, avoid vendor or protocol lock-in, and maximize interoperability across jurisdictions and sectors. This approach ensures that vendors can propose solutions aligned with mature, well-supported ecosystems while also leaving room for emerging technologies to demonstrate value. The following section highlights the standards, technologies, and frameworks that should be considered across the full SEDI issuance, holding, and verification lifecycle while maintaining the flexibility necessary for sustainable and future-proof procurement.

ISO/IEC 18013 mDLs and ISO/IEC 23220 mdocs

1. **Issuing:** Well-suited for high-assurance credentials such as driver licenses and state IDs. Already supported by TSA through TSIF pilots and by AAMVA's Digital Trust Service for cross-state interoperability.
2. **Holding:** Wallets can store ISO-compliant mDLs and other mdocs, with privacy-protective offline validation. Consumers benefit from strong device security and offline functionality.
3. **Verifying:** Readers can validate credentials without contacting the issuer, minimizing surveillance risks. Certification programs (e.g., Fime) exist to ensure interoperability. Independent projects such as Longfellow, an open-source implementation, have demonstrated that ISO standards can support unlinkable, privacy-preserving presentations rather than relying on "phone-home" modes.

Pros: Mature standards with proven interoperability in the U.S. which will accelerate adoption; required for TSA acceptance; offline verification aligns with Utah's unlinkability mandate; open-source tools like Longfellow illustrate that unlinkability can be achieved within the ISO framework.

Cons: Primarily designed for identity documents, less flexible for permits or benefits; requires Utah to define a "SEDI profile" for consistency. The current version also permits an optional "server-retrieval" mode which may be incompatible with SEDI, so this mode may need to be explicitly disallowed in the SEDI profile, and/or the data model would need to be extracted to ensure binary compatibility.

IETF Selective Disclosure JWTs

1. **Issuing:** Based on the widely adopted JSON Web Token (JWT) format, SD-JWTs allow issuers to provide credentials where attributes can be selectively disclosed by the holder. SD-JWT+KB additionally enables holder key binding. Issuance is transport-agnostic and can be performed over existing protocols such as OID4VCI.
2. **Holding:** Wallets store SD-JWTs and its disclosures, and at presentation time reveal only the requested claims. Pairwise identifiers can be supported depending on the cryptographic scheme used.

3. **Verifying:** Verifiers request only the specific attributes required, and the holder's wallet returns the SD-JWT (with blinded claims) along with the minimal disclosures. If key binding is required, the holder signs a verifier challenge with the bound key. Revocation and status can be managed through IETF-defined mechanisms such as Status List 2021.

Pros: Leverages the existing JWT ecosystem widely used in government and enterprise IT; low implementation barrier since many platforms already support JWT libraries; strong alignment with privacy goals such as minimal disclosure; an active IETF working group ensures ongoing evolution and interoperability; SD-JWT VC is actively supported in the ongoing EUDI Wallet program.

Cons: Interoperability depends on well-defined profiles that constrain SD-JWT's flexibility; still emerging in production-scale deployments compared to ISO mDL; requires policy guardrails and rigorous wallet enforcement to prevent verifiers from requesting unnecessary attributes and causing over-disclosure.

W3C Verifiable Credentials (VCDM 2.0)

1. **Issuing:** Flexible issuance process over web protocols using OID4VCI. Works for both high- and low-assurance credentials. SD-JWT can be used as a VC format under VCDM 2.0.
2. **Holding:** Wallets can store multiple credential types. Selective disclosure is supported by formats such as SD-JWT VCs, while the Data Integrity BBS Cryptosuite v1.0 enables BBS+ signatures that add unlinkability properties in addition to selective disclosure.
3. **Verifying:** OID4VP enables verifiers to request only necessary attributes. Presentation Definitions ensure minimal disclosure. Status lists allow privacy-preserving revocation checks.

Pros: Highly flexible across use cases, strong fit for online and cross-sector adoption, global ecosystem of implementers which will accelerate adoption

Cons: Flexibility can lead to fragmentation unless Utah defines its own SEDI profile; certification ecosystem is less developed compared to ISO mDL.

X.509 / PKI-based credentials

1. **Issuing:** Uses existing CA infrastructure to issue identity or attribute certificates. Well understood by IT staff and easy to integrate with current state PKI systems. Alternatively, X.509 certificates could be used to manage credential issuance keys in conjunction with other credential formats.
2. **Holding:** Wallets or secure devices can store identity and attribute certificates. Mature ecosystem for certificate storage and management.
3. **Verifying:** Verifiers validate certificate chains and status using CRLs or OCSP. Straightforward for existing enterprise and government systems.

Pros: Decades of use in government and enterprise environments; strong baseline authenticity and revocation mechanisms. Composable as a form of identifier or key management with other standards for credential issuance.

Cons: Not designed for selective disclosure or unlinkability; centralized revocation can expose usage patterns; attribute certificates are not widely used in consumer contexts.

KERI (Key Event Receipt Infrastructure)

1. **Issuing:** Issuer's key events are tamper-evident and auditable without requiring central registries. KERI ACDCs support chaining credentials together.
2. **Holding:** Wallets store credentials issued to identifiers (AIDs) backed by cryptographic event chains. Controlling keys of an AID can be rotated without breaking continuity. Holders must use an agent (or use a wallet that integrates one for them) in order to interact with other identifiers, and to receive and present credentials.
3. **Verifying:** Verifiers use an agent to fetch and validate other identifiers' KELs, manage an identifier, and engage in exchange and presentation protocols to verify ACDCs. Alternatively, they can use APIs provided by issuers or third parties to resolve the necessary event logs and do full business logic verification, but this raises "phone home" concerns.

Pros: Strong support for auditable key management and rotation, self-sovereign identifiers, and chaining credentials to connect multiple claims into one graph.

Cons: Ecosystem still maturing, with fewer off-the-shelf tools and production deployments at scale; limited cross-jurisdictional adoption today which may hinder adoption significantly; requires investment in verifier education and readiness. To truly realise the proposed benefits of a KERI-based system, every holder would likely need to maintain multiple sets of keys (assisted by wallets) at different levels of security.

FIDO2 / WebAuthn (Passkeys)

Passkeys are not a verifiable credential format, but should be considered as a technology component necessary for ensuring the security and privacy of digital identity holders. Aligned with NIST 800-63B-4 terminology, passkeys are considered a multi-factor cryptographic authenticator, and can meet the highest levels of authentication assurance. Passkeys can be used during wallet enrollment, or SEDI credential issuance to strongly authenticate the individual to the state account system, and/or to their wallet provider.

Pros: Strong phishing resistance; eliminates reliance on shared secrets; widely supported across browsers and devices; device attestation enhances assurance; improves usability with passwordless flows.

Cons: Recovery and portability depend on platform ecosystems; risk of lock-in if not paired with interoperable migration standards; device loss requires robust recovery planning.

Cross-cutting considerations

Across all approaches, Utah should:

- Support SEDI credentials across multiple formats (such as the mdoc data model from ISO/IEC 18013-5 so that SEDI-conforming credentials can also be used natively with Apple Wallet, Google Wallet, and Samsung Wallets for a superior user experience and TSA acceptance, IETF SD-JWTs for evolving industry alignment (Google Wallet) and EU support, W3C VC for education credentials and/or EU acceptance, KERI ACDC for organizational identity) to maximize interoperability and portability.
- Require wallets to support selective disclosure, appropriate aspects of unlinkability, and user choice, regardless of protocol or data formats.
- Publish a Utah "SEDI Profile" to constrain attributes, proof types, and revocation methods for consistency, that may be specialized into each of the data formats and protocols.
- Rely on established certification programs and technical standards such as NIST (identity and security), FIDO (authentication security), Kantara (governance and privacy), and FIME (ISO conformance) to the extent possible and reasonable.
- Ensure verifier tools are simple and low-cost, so adoption by agencies and businesses is not hindered.

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

- **Ability to support all SEDI controls**: Utah Code § 63A-16 is the will of the people of Utah. The selected standards and technologies must be able to demonstrate support for all SEDI controls, or produce a suitable profile.
- **Alignment with use cases**: The standard should enable real-world transactions important to Utah residents and relying parties, such as proof-of-age, airport screening, or access to benefits.
- **Ecosystem size and maturity**: The standard should have a healthy base of adopters, with active participation from multiple vendors and demonstrated investment from both public and private sectors.
- **Number of vendors**: Multiple independent vendors should support the standard to ensure competition, innovation, and reduced risk of lock-in.
- **Level of investment**: There should be clear evidence of sustained investment in tools, reference implementations, and commercial deployments.
- **Standards body support**: The standard should be governed by credible and recognized standards development organizations (SDOs) such as ISO, W3C, IETF, or the OpenID Foundation.
- **Interoperability implementations**: The standard should have successful cross-vendor and cross-jurisdiction implementations, supported by conformance testing or certification programs.
- **Account/credential compromise and recovery:** The State should evaluate what worst-case scenarios look like under the technology in question, such as stolen private keys, lost devices, or malicious issuance, and how recovery is handled. Standards that support credential revocation, re-issuance, and user-controlled recovery mechanisms without excessive centralization are preferable.
- **Scalability:** The State should consider whether the technology has been proven in scaled, production use cases. If scaling requires custom infrastructure rather than standard techniques, the risk of operational challenges increases. Technologies with demonstrated large-scale deployments and reliable infrastructure patterns should be prioritized.

The state should avoid including requirements for technologies where:

- Only a single or a few vendors offer the implementation, creating risk of lock-in
- No active or visible ecosystem of contributors, pilots, or deployments
- Limited or no backing from established standards bodies
- Lack of conformance testing, certification, or interoperability demonstrations
- Recovery from compromise is unclear, dependent on a single vendor, or undermines unlinkability/privacy principles
- No evidence exists of scalable production deployments, or scaling requires bespoke solutions that increase complexity and risk

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

Yes. Our solution supports portability of digital credentials across jurisdictions by relying on open, widely adopted standards rather than proprietary formats.

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

Utah can reduce abuse and protect residents from unauthorized use of a SEDI by combining technical safeguards with policy and market incentives. One approach is to create an opt-in verifier certification process, where organizations that wish to request or accept SEDI credentials can voluntarily undergo certification to demonstrate compliance with Utah's privacy and security requirements. Certified verifiers could be published in a public directory to provide transparency for residents, while uncertified organizations would remain free to operate outside of the SEDI framework. This approach both raises the bar for verifiers who want the benefits of integration and gives residents confidence that their credentials are only being requested by trusted, certified entities without requiring the State to maintain a rigid "allow list."

The SEDI framework should require some form of cryptographic binding, for example device-binding, to ensure that credentials remain under the control of the provisioner with high confidence, and to make it difficult for a credential to be transferred and misused by a third party. Wallet-based checks can further strengthen protections: biometric authentication is one option, but alternatives such as PINs or knowledge-based prompts could help maximize accessibility and choice.

Modern credential standards also provide mechanisms such as nonces and challenge-response protocols to prevent replay attacks, ensuring each presentation is unique and cannot be reused fraudulently. In addition, the use of cryptographic signatures guarantees the authenticity of SEDI credentials in a way that far surpasses visual inspection of a physical license or a photo of one.

To monitor and deter abuse, the State can require wallets to collect anonymized statistics on verifier requests, aggregated across users. These data can highlight systemic risks, such as a particular verifier requesting excessive attributes, without exposing individual transaction histories. Finally, Utah should establish risk-based obligations for relying parties. Relying parties that collect SEDI data should be required to carry insurance to cover potential breaches, creating a financial incentive to minimize the amount of data they store.

Some standards, such as KERI, utilize issuer registries and signed event logs that make it easier to detect fraudulent issuances, since every valid event is anchored in a verifiable log. Similar mechanisms, including transparency logs or public issuance registries (as seen in approaches like Estonia's use of a private blockchain for government records), could also be layered onto existing standards to provide Utah with additional monitoring capabilities.

Finally, we recommend that these systems are designed to expect failures. We believe that even the best-run digital identity systems (and software at scale, more generally) will have flaws and defects. Therefore, it is important to take a systems-level design perspective such that no single compromise is able to debilitate or compromise the entire system, ensuring resiliency and defense in depth.These tools must be balanced carefully against privacy requirements and overall system complexity.

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, our proposed solution can support unlinkability so that the use of a SEDI credential by an individual cannot be tracked across verifiers when used for attribute disclosures, such as "over 21" or "is Utah resident" checks. Technically, this can be achieved through privacy-preserving proof formats such as zero-knowledge proofs (ZKPs) that allow specific fields to be selectively disclosed without revealing the full credential, and also through trusted execution environments (TEEs) that ensure cryptographic operations are performed securely on the device. Single-use (per-verifier) or batch issuance can also mitigate holder correlation across presentations, though this does introduce additional operational burden and may not be reasonable for all use cases. These measures allow a verifier to confirm the validity of the credential while preventing linkage across multiple presentations.

It is important to recognize the limits of unlinkability. We can mitigate tracking risks within the credential formats and protocols, but cannot obfuscate factors outside the system's scope, such as surveillance camera face captures, IP addresses, or network metadata. Further, if the user's PII is shared to access a service, then technical controls alone will not be effective. For that reason, unlinkability must be managed both technically and through policy. Utah should adopt a SEDI profile that mandates privacy-preserving proof types, requires wallets to default to minimal disclosure, and restricts verifiers from requesting excessive attributes. Policy enforcement is essential to ensure that unlinkability protections are applied consistently across the ecosystem, while technical controls make those policies enforceable in practice. In addition, Utah should clarify which dimensions of unlinkability are most important, such as preventing correlation when the same credential is presented repeatedly to one verifier, when the same credential is presented to multiple verifiers, or when different credentials about the same subject are linked; different technical approaches present different tradeoffs.

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

The SEDI framework should include revocation and status best practices as baseline requirements, ensuring that any compliant credential supports privacy-preserving status checks. Our recommended approach relies on standards-based status lists (W3C/IETF), which achieve herd privacy by batching tens of thousands of credentials together. Each credential receives a randomized index within the

batch, so verifiers can check revocation status locally without revealing which individual credential is being verified. This allows revocation checks to be performed in a privacy-preserving manner. Trust is reinforced through audits, transparency logs, and legal safeguards, and selective disclosure protocols minimize the exposure of personal data during checks. The State may also choose to issue multiple versions of the same credentials in specific cases, though this introduces additional overhead.

By contrast, a monolithic approach with a single SEDI credential or identifier introduces significant linkability concerns. Using a single canonical credential such as an mDL or SD-JWT with only one signature means that, even with selective disclosure, common subsets of data requested across contexts can allow correlation of a holder's activity. In identifier-based models such as KERI, revocation and key rotations are auditable through the Key Event Log (KEL) and issuer transaction logs (TEL). Anchored credentials like ACDCs deliberately link to the same identifier (AID), which is often necessary to realize the intended benefits of a unified identity. While the State could expect holders to manage many AIDs to reduce linkability, this adds complexity for both the state and user key management.

Future developments that involve use of advances in cryptography can add privacy and security. For example, zero knowledge proofs can demonstrate membership or nonmembership within a status list, and cryptographic accumulators can prove that a credential's issuance was authorized by a specific issuer and its revocation status without revealing which exact credential.

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

Yes, it allows a legal guardian to obtain and use a SEDI-compliant credential on an individual's behalf, minimizes collection of a minor's data, and adapts to specific use cases while aligning with Utah's principles of individual control and privacy. Both approaches described here rely on State agencies to determine guardianship and must integrate with existing systems and data sources; implementation requires authoritative guardianship evidence and timely updates across jurisdictions. The goals are to minimize collection of a minor's data wherever possible and to select techniques based on the use case while keeping privacy and individual control at the forefront. This proposal presents a practical baseline using verifiable digital credentials (VDCs) that should be refined with implementing agencies and subject matter experts.

(Recommended) Solution Outline 1: Simple VDC model

This solution fits into the SEDI framework model, and is not prescriptive of the exact technologies in implementation, with many possible paths that can achieve SEDI controls and interoperability.

Solution components:

- **Foundational record.** Birth certificate VDC issued on request; paper certificates may be augmented with a verifiable barcode or QR code containing signed data. Birth certificate VDC issuance would adhere to the relevant controls in the SEDI framework.
- **Guardianship credential.** Guardianship VDC issued to the guardian(s), either as a SEDI or potentially as a lower-assurance credential that requires co-presentation with a SEDI; these VDCs may reference the ward's birth certificate or other SEDI credentials but do not require

hard linkage in all cases. Default expiry at the age of majority; court-ordered changes trigger revocation or status updates.

- **Delegated authority.** Guardian can request the issuance to a third party of a scoped, time-limited delegation for specific tasks such as school registration. Verifiers define approval thresholds per use case when one or more guardians must consent.
- **Identity for minors.** Options include using a birth certificate VDC, issuing lightweight “low-data” minor SEDI credentials, and allowing guardian-backed attestations that pair a Guardianship VDC and SEDI with the ward’s records, or even issuing a full identification card-like SEDI credential to minors if appropriate.
- **Provisioning and use.** To obtain a vital record or other SEDI-compliant VDC for a ward, the guardian presents the Guardianship VDC as an additional proofing factor; during use, the guardian presents the Guardianship VDC with the ward’s credential. Optional device-binding can raise assurance while remaining non-custodial.
- **Transition.** Court-ordered removal revokes the Guardianship VDC; by default it expires at the age of majority, ending associated delegations.

These mechanics align with the State’s interest in guardianship, selective delegation, revocation, and minimizing linkability.

Pros: Simple to pilot and adapt to real-world needs; minimal complexity for holders; supports mixed digital and paper flows.

Cons: Linked identifier patterns are possible but less conventional in this model; self-sovereign identifier support can be more complex to operationalize at scale.

Solution Outline 2: KERI-based identifier model

One alternative model is based on KERI identifiers (AIDs) and is outlined below:

- **Identifier Setup.** Guardian manages AIDs for self and ward; the ward’s AID is multisig-controlled per policy so guardians hold threshold control.
- **Guardianship credential.** Guardianship ACDC issued to the guardian’s AID, with an edge to the ward’s birth certificate ACDC or a reference to its AID. Handle out-of-state births via defined intake.
- **Delegation.** Scoped ACDC schemas reference the root Guardianship ACDC. Guardians can directly issue these credentials to third-party AIDs. Verifiers check the validity of both the issued credential and the referenced (chained) root Guardianship ACDC.
- **Identity for minors.** Guardians may grant limited autonomy by rotating to a new multisig configuration, with careful configuration to protect guardrails and usability. This could enable minors to present credentials in conjunction with a guardian's approval.
- **Provisioning and use.** Guardianship ACDC serves as proofing to provision SEDI for the ward’s referenced AID; whoever controls the ward’s AID can present, assuming access to credential data.
- **Transition.** Court-ordered removal revokes the guardianship ACDC in issuer registries; guardians rotate keys to remove control. At majority, rotate until the ward holds full control, potentially through multiple rotations to cover pre-rotated keys.

Pros: Pre-rotation preserves identifier continuity; strong auditability of key events.

Cons: Higher complexity and operational burden; multisig thresholds may misalign with verifier-specific consent rules and can hinder presentations if misconfigured. One-AID-per-person creates linkability by default.

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?**

The State should evaluate a range of technology solutions both to inform which technical controls should be explicitly required in the SEDI framework and to confirm that those controls are achievable through existing standards. Each approach has unique advantages and drawbacks when measured against Utah's policy objectives of privacy, unlinkability, minimal disclosure, and citizen control. Through this evaluation, Utah can distinguish between controls that can be consistently enforced in practice and those that may require phased adoption or policy reinforcement. Under a technology-agnostic SEDI framework, different standards and technologies can be applied flexibly to achieve the same policy outcomes. For a single-SEDI model, evaluating standards becomes even more critical, since the State would need to select one primary technology stack; in that case, feasibility, interoperability, and long-term sustainability of the chosen standard carry heightened importance.

Decentralized identity (e.g., W3C Verifiable Credentials, DID-based approaches)

- **Strengths:** Enables selective disclosure and unlinkability through advanced cryptography such as zero-knowledge proofs; highly extensible to different credential types; supported by a growing global ecosystem of open-source and commercial implementations.
- **Weaknesses:** Ecosystem flexibility can lead to fragmentation without a Utah-specific profile; certification programs are less mature than ISO-based approaches; requires investment in verifier readiness.

Standards-based mobile documents (e.g., ISO/IEC 18013 mDL, ISO/IEC 23220 mdoc)

- **Strengths:** Mature international standards already deployed in U.S. state pilots; supported by TSA TSIF testing for federal checkpoint acceptance; backed by significant TSA investment in CAT-2 readers nationwide; privacy-preserving offline verification.
- **Weaknesses:** Requires Utah to define a "SEDI profile" to ensure consistency; less flexible for permits and benefits compared to VC models; requires Utah explicitly prohibiting implementation of any "phone home" functionality.

KERI (Key Event Receipt Infrastructure)

- **Strengths:** Provides cryptographic continuity of identifiers through event logs; native multisig support; strong key management and issuance auditability guarantees; promising in vLEI pilots.
- **Weaknesses:** Ecosystem is still emerging, with fewer off-the-shelf tools than ISO or W3C; limited cross-jurisdictional adoption today; would require verifier training and investment in supporting infrastructure. Significant upfront barriers to adoption for holders and verifiers, including AID setup and PKI management. If a goal is to give SEDI holder utility, then there needs to be lack of friction for the broader (including outside of Utah) relying party ecosystem.

Biometrics (device-based or verifier-assisted)

- **Strengths:** Ensures the rightful holder is presenting the credential; widely supported on consumer devices (Face ID, Touch ID, or front-facing camera with remote verification and liveness detection); can improve usability and reduce unauthorized use; familiar usability for consumers.
- **Weaknesses:** Must be implemented locally or through trusted third parties to avoid surveillance risks; cannot provide unlinkability or minimal disclosure on their own; accessibility challenges for some populations.

Digital wallets (state-issued and certified third-party)

- **Strengths:** Provide the user-facing layer for holding and presenting SEDI; can enforce statutory principles through UX such as disclosure warnings; certification ensures conformance to Utah's requirements.
- **Weaknesses:** Risk of wallet fragmentation without strong certification; wallet recovery and portability must be addressed to avoid lock-in; usability differences across wallets may confuse residents.

Traditional PKI / X.509 approaches

- **Strengths:** Well-established with decades of deployment in government and enterprise systems; strong authenticity and revocation support; easy to integrate into existing IT. Can be used to manage issuer identifiers in combination with other credential issuance standards.
- **Weaknesses:** No native selective disclosure or unlinkability; centralized revocation mechanisms can create privacy risks; attribute certificates not widely adopted in consumer workflows.

Hardware-based security (device attestation, secure enclaves, HSMs)

- **Strengths:** Ensures cryptographic keys are generated and stored in tamper-resistant environments; already supported by iOS/Android devices and standard HSMs; critical for high-assurance use cases.
- **Weaknesses:** Hardware trust can be uneven across device ecosystems; reliance on proprietary vendor ecosystems may limit transparency; cannot address unlinkability without higher-level protocols.

FIDO2 / WebAuthn (Passkeys)

- **Strengths:** Provide strong, phishing-resistant authentication with proven user experiences to traditional password + MFA; widely supported across platforms (Apple, Google, Microsoft); enable passwordless user experiences; can integrate with device attestation for assurance of wallet integrity.
- **Weaknesses:** Usefulness in context of SEDI is only relevant to account access and account management. Portability of passkeys may be limited without credential backup or migration; dependency on major platform ecosystems raises supportability concerns; device loss or compromise requires robust recovery mechanisms or dependence on additional consumer accounts.

Trust frameworks (AAMVA DTS, TSA TSIF, interoperability agreements)

- **Strengths:** Provide the governance and certification layer to make credentials usable across jurisdictions and sectors; AAMVA DTS is already live for mDL trust; TSA TSIF provides a federal acceptance path.
- **Weaknesses:** Scope is limited to particular credential types; participation requires investment and governance alignment; does not substitute for local statutory compliance.

In practice, Utah will likely need to combine multiple of these technologies rather than rely on a single solution. A multi-format issuance approach, supported by wallets certified for disclosure controls, device-based biometrics for holder authentication, and state-controlled PKI for trust anchors, offers a comprehensive path forward. Emerging protocols like KERI may play an important role in advanced use cases such as self-sovereign identifiers or auditable key management, once ecosystems and verifier support mature.

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

There are multiple ways privacy-enhancing technologies (PETs) can be incorporated across the SEDI program, spanning issuance, storage, presentation, revocation, and oversight. By embedding PETs into each layer of the ecosystem, Utah can ensure that privacy protections are not just policy commitments but are technically enforced.

Guiding approach

Adopt a SEDI Privacy Profile that requires minimal disclosure, unlinkability across verifiers, offline validation where feasible, and default-off telemetry. PETs should be mandatory for core flows, measurable through certification, and modular so Utah can upgrade components without redesigning the system.

Issuance

- Selective disclosure by design. Issue credentials that support field-level proofs so residents can share only what a transaction needs.
- Device attestation and hardware-backed keys during provisioning to prevent key export and impersonation without storing user data centrally.
- No centralized credential copies at the issuer. Retain only existing authoritative records, not wallet contents.
- Consider use of Trusted Execution Environments (TEEs) to ensure sensitive cryptographic operations during provisioning occur in isolated, tamper-resistant environments, reducing issuer or device compromise risk.

Holding (wallet and keys)

- Hardware security (Secure Enclave, StrongBox, or equivalent) for key generation and storage. All holder authentication local to the device using biometrics or PIN, with no server-side biometric retention.
- TEEs perform attested privacy-sensitive wallet operations, ensuring sensitive data and keys are handled securely even if the device OS is compromised.
- Pairwise identifiers. Derive per-verifier key material or identifiers so repeated use cannot be correlated across relying parties.
- Personal data licenses. Attach machine-readable usage terms to presentations (for example, one-time use, time-limited retention, no sharing) so limits are both visible and enforceable.

Presentation and verification

- Zero-knowledge and selective disclosure proofs for attributes such as age-over or entitlement-valid without revealing full identity data.
- TEE attestations to protect against tampering and create assurances for unlinkability across sessions.
- Verifier authentication before any disclosure so wallets can warn or block excessive or out-of-scope requests.
- Offline validation paths using published trust lists to avoid issuer lookups at time of use. When online validation is necessary, use privacy-preserving transports and short-lived tokens to reduce metadata exposure.
- Do not require device surrender. Use QR, short-range radio, or remote session handshakes that keep the phone in the resident's control.

Status and revocation

- Privacy-preserving status mechanisms. Use compressed, non-personal status lists or stapled proofs so verifiers can check validity without per-holder queries.
- Distinguish identity from entitlement. Suspend or revoke only what is necessary, allow presentation of expired or superseded credentials with clear status so relying parties can exercise judgment without tracing use.

Oversight, analytics, and verifier governance

- Anonymized ecosystem health metrics. Allow wallets to report aggregated, differentially private statistics on verifier requests to detect systematic over-collection without tracking individuals.
- Verifier obligations. Require minimal collection, short retention, breach insurance, and acceptance of personal data license terms to align incentives to hold less data.
- Privacy threat modeling and impact assessments as part of certification. Test wallets and verifiers for over-collection, linkage risk, replay, and telemetry leakage.

Certification and testing

- Wallet and verifier conformance tests for selective disclosure, unlinkability, audience binding, offline validation, and status privacy.
- Public documentation and independent audits of the SEDI Privacy Profile to maintain transparency and trust.

Together, these measures ensure that privacy is treated as a core design feature of SEDI, giving residents confidence that their data is protected while keeping the system adaptable to new technologies and emerging threats.

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

Within the SEDI ecosystem, UtahID should serve as the centralized single sign-on (SSO) platform to provide a consistent and user-friendly entry point for residents. By consolidating authentication under one state-managed system, UtahID can reduce credential fatigue, streamline access across services, and give the state centralized governance and monitoring of authentication events.

Identity verification (IDV) should be integrated into UtahID, with the flexibility to multiplex across different IDV providers. This allows the state to choose different proofing methods depending on program requirements, risk profiles, and assurance levels, ensuring both scalability and adaptability to evolving needs.

Support for multiple assurance levels is essential. Lower-assurance use cases, such as certain informational access or commercial permits and licensing, may implement only a subset of the SEDI framework controls (e.g. minimal disclosure without requiring IAL2/IAL3 proofing). By contrast, high-assurance use cases such as benefits administration or unemployment insurance should require credentials that comply fully with the SEDI framework, including proofing requirements. This tiered approach ensures resources are applied proportionally to the sensitivity of the transaction, while also allowing shared infrastructure between SEDI foundational identity and lower-assurance credential use cases driving interoperability and market development.

Risk-based authentication and escalation methodologies should be in place to dynamically adjust requirements based on transaction type, fraud signals, or behavioral analytics. This includes step-up authentication, such as moving from password-based login to MFA or requiring re-proofing, when risk thresholds are exceeded. These mechanisms help balance strong security with a smooth user experience.

Finally, the system must allow program-specific flexibility, since agencies face different compliance and fraud pressures. Each program should be able to configure IDV and authentication workflows to meet its own needs while maintaining consistency under UtahID. At the same time, the resident experience must remain accessible and privacy-preserving, with data minimization and transparency built into identity processes to maintain trust across the ecosystem.

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

Data governance and minimization should be explicitly defined as required controls in the SEDI framework. Credentials must only disclose what is necessary for a transaction, using selective disclosure and cryptographic proofs so verifiers see attributes like “over 21” without unnecessary personal details. For example, an immunization credential could demonstrate that a resident meets a vaccination requirement without revealing whether that status was achieved through a vaccination, a waiver, or another pathway — ensuring conformance without overexposure of sensitive health information. Wallets should enforce these principles by mediating every request, providing clear prompts, and warning residents when verifiers seek excess data.

The State should require verifiers to justify what they collect, retain only what is necessary, and carry liability or insurance if data is misused. Issuers should issue credentials with only the attributes needed for their purpose, guided by a Utah SEDI profile that defines allowed attributes, retention rules, and enforcement. By baking these principles into the SEDI framework, Utah can ensure that data minimization and governance are enforced through technical controls and policy requirements, protecting residents' privacy in practice.

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?

Long-term sustainability of the SEDI program requires defining a framework that effectively translates policy goals into technical controls. It further requires implementations that comply with this framework and build on technologies that are widely used, highly mature, and supported by strong ecosystems. Anchoring the program in well-established standards ensures that Utah benefits from global investment, interoperability, and vendor competition. By contrast, niche or experimental technologies should only be adopted in a modular way, so they can be swapped or upgraded without disrupting the entire system.

To prepare for future threats and evolving standards, the framework should capture goals and high-level requirements while leaving room for different implementation approaches to meet those goals as they see fit. Core requirements such as PKI management practices, wallet certification, and interoperability can remain stable, while implementation details such as cryptographic proof formats or revocation mechanisms can be updated over time to ensure SEDI compliance. Adopting an understanding of SEDI as a framework would further support this modularity, allowing piecewise and targeted upgrades without requiring disruptive and complicated full-system rollouts. The framework itself should also include a clear process for updates, so that new technical controls can be added or existing ones strengthened in response to emerging threats, while maintaining backward compatibility where possible.

Sustainability also depends on continuous monitoring and governance. Utah should participate in national and international standards bodies, track emerging threats like quantum computing and AI-enabled fraud, and run structured pilot programs to test new technologies in low-risk environments before broad adoption. By combining mature standards as the foundation with modular components for

innovation, Utah can ensure that SEDI remains resilient, adaptable, and aligned with statutory principles for decades to come.

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

Under a SEDI framework, other credential types can selectively adopt the framework controls that are most relevant to their use case. Foundational identity use cases, such as digital driver's licenses or Veteran ID, would need to comply fully with all SEDI controls, while lighter-weight credentials such as permits, professional licenses, or benefit entitlements could apply a subset of the controls (e.g. supporting selective disclosure).

This flexibility is supported by shared infrastructure. For instance, identity verification (IDV), wallet certification, and verifier tools can be reused across credential types, lowering the barrier to adoption and ensuring consistent experiences for residents. Issuers can focus on defining domain-specific attributes, eligibility criteria, and disclosure policies, while relying on the same trust, audit, and lifecycle mechanisms used for SEDI foundational identity credentials. In addition, other credentials can also leverage existing SEDI credentials directly, either referencing them for assurance or requiring that they be presented in conjunction.By adopting open, interoperable protocols, Utah can add new credential types without creating bespoke infrastructure for each one. This lowers costs, simplifies maintenance, and gives residents a single, consistent way to manage all their credentials.

We once again emphasize the benefits of creating a more decentralized and composable approach to SEDI, allowing each of the specific controls to be modeled across many different existing technologies, and for firms to specialize in their implementation and/or extension into new domains.

For example, one firm may decide to use KERI/ACDC for a very sophisticated guardianship system for SEDI credentials, and they may find that the guardianship feature is also usable for organizational credentials which do not require the entirety of SEDI controls. Instead, this is used to define corporate parenthood in a robust and cryptographically verifiable manner, preventing fraud in the financial sector. This allows for the same technologies and controls to be composed into new use cases.

In another example, a company that specializes in Bluetooth-transmittable mobile documents (mdocs) may have implemented a SEDI credential, but reuses the hardware security features developed to meet controls under the SEDI framework to also create physical access control credentials, which can be used to facilitate visitors' access across the entire hospitality industry for the 2032 Olympics in Park City.

By having a composable set of SEDI controls that can be repurposed for other use cases as they are appropriate, we can accelerate privacy, security, and usability within government agencies and the private sector alike. This increases the level of optionality, quality, and lowers the cost for SEDI credentials and all other credentials built on an aligned framework.

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

The State can issue additional credentials alongside SEDI credentials through its instance of SpruceID's Credible platform. Each credential (whether a driver license, vehicle registration, hunting

permit, or professional license) can be issued independently, using the same trust framework, lifecycle management processes, and revocation mechanisms. This ensures consistency across credential types while still allowing agencies to tailor attributes and policies to their own use cases.

In some situations, it may be desirable to establish stronger ties between credentials. For example, Utah could enable cryptographic linking by including credential hashes, referencing a stable UUID (such as a W3C DID, KERI's AID, or other unique identifiers that persist), which could be provided by the user or an agency. Whether or not to link credentials should be driven by policy and use case requirements, not assumed by default. By maintaining flexibility in this way, Utah preserves privacy and unlinkability while still supporting use cases where coordinated credentials provide value.

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

Our proposed solution provides a full suite of verification tools to ensure that SEDI credentials can be validated securely, efficiently, and consistently across use cases. These can include:

- **Verifier SDKs and reference code** that organizations can integrate into their existing systems with minimal development effort. The SDKs enforce Utah's SEDI profile requirements for selective disclosure, unlinkability, and cryptographic validity.
- **Web-based verifier applications** that allow smaller organizations or low-volume verifiers to scan and validate credentials without requiring complex integrations.
- **Mobile verifier applications** for law enforcement or field-based staff, capable of performing offline validation where network connectivity is limited.
- **Conformance and certification test suites** that allow third-party verifier implementations to be tested against Utah's requirements, ensuring interoperability across vendors.
- **Trust list and status services** to confirm credential validity (e.g., not revoked, not expired), implemented in a privacy-preserving way to avoid issuer "phone-home" tracking.

Together, these tools give relying parties options suited to their operational scale while maintaining a consistent standard of verification aligned with Utah's statutory objectives.

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

Yes. Our solution supports flexible credential lifecycles, including both time-limited credentials and non-expiring credentials where permitted by policy. Issuers can define expiration dates, renewal intervals, or perpetual validity at the time of issuance, and these settings are enforced by the cryptographic structure of the credential and the associated status mechanisms.

That said, Utah should be aware of third-party limitations that may apply in certain environments. For example, some OEM wallets impose their own rules on how long credentials can be stored, and signing certificate policies may require periodic re-issuance or key rollover even for credentials intended to be non-expiring. These factors do not prevent Utah from supporting a range of expiration lengths, but they may shape implementation details depending on the chosen wallet ecosystem or cryptographic trust framework.

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

The SEDI framework ensures an appropriate level of security, privacy, simplicity, and transparency by defining baseline technical controls that all compliant credentials must follow, while allowing flexibility in how each foundational identity implementation meets those requirements. Each SEDI foundational identity use case can select the technical standards that best achieve the desired functionality, promoting simplicity while also guaranteeing a baseline level of security, privacy, and transparency. The framework-based approach also supports iterative rollout of different SEDI-compliant credentials, with each phase adjusted based on user feedback and real-world performance. Non-SEDI credentials can choose to comply with the minimal set of controls that are relevant to their use cases.This approach balances security and privacy with simplicity and transparency, while giving the State a clear path to evolve protections and update the framework as risks and requirements change.

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

The SEDI framework should incorporate the guidance of the National Institute of Standards and Technology (NIST) on post-quantum cryptography when outlining required technical controls for foundational identity credentials. One suggestion here is to encourage solutions to be crypto-agile, to ensure that SEDI credential issuances employ quantum-resistant algorithms as soon as these are finalized and standardized by NIST. This will ensure that SEDI credentials can be more quickly updated when needed, instead of requiring complex whole-system redesigns. Additionally, the framework model makes it possible to iteratively deprecate and upgrade older SEDI credentials piecemeal as new post-quantum technologies are finalized. This approach aligns with federal best practices and positions the State to remain resilient against future cryptographic threats.

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

The SEDI framework should mandate protection against "harvest now, decrypt later" attacks. Our proposed approach minimizes what can be harvested and shortens the value of any captured data. Credentials are stored under the control of the individual and transmitted only in response to explicit, authenticated requests from verifiers. Selective disclosure and minimal disclosure protocols ensure that only the required attributes are shared, reducing the surface area of exposed data. Utah should also require verifiers to limit retention of presented credential data, further minimizing what attackers could access in the event of compromise.

In addition, all credential presentations are bound to session-specific challenges and encrypted during transmission. This means that even if an adversary were to capture encrypted traffic today, it would not be able to reuse old presentations to impersonate the holder. Over time, as quantum-resistant cryptographic algorithms mature and are standardized, Utah can incorporate them into the SEDI profile to further strengthen long-term protections. For especially sensitive payloads, Utah could adopt application-layer post-quantum encryption (for example, wrapping credential presentations in PQC-based HPKE) to protect data even if TLS traffic is later decrypted. As hybrid post-quantum TLS becomes more widely supported, the SEDI ecosystem can transition seamlessly, ensuring long-term

resilience while maintaining crypto-agility. The combination of data minimization, confidentiality by design, and forward-looking cryptography ensures that SEDI credentials remain resilient against harvest-now, decrypt-later threats.

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

SpruceID's proposed solution emphasizes privacy-preserving analytics that give the State visibility into system health without creating surveillance risks. At the wallet level, anonymized and aggregated statistics can be collected to identify broad usage patterns, such as the number of verifications attempted, the prevalence of certain credential types, or verifier requests that consistently exceed expected norms. These reports are designed to highlight systemic risks or verifier misuse while ensuring that no individual transaction histories are exposed.

For issuers, lifecycle reporting tools can provide visibility into credential issuance, renewal, suspension, and revocation, with dashboards and exportable reports for monitoring compliance and capacity planning. These tools can integrate with existing state systems, enabling agencies to reconcile digital credential activity with authoritative records.

For verifiers, certification and conformance testing frameworks can generate reports that demonstrate adherence to Utah's SEDI profile. This ensures that verifier implementations are interoperable, privacy-preserving, and compliant with statutory principles.

All reporting is designed with SEDI's "no phone-home" principle in mind: data collection is performed either on-device in a way that can be voluntarily shared by the holder, or through aggregated, anonymized metrics that prevent issuer–verifier collusion or the creation of any new centralized user databases.

This approach provides the State with actionable insights into adoption and compliance trends while preserving Utah residents' privacy and aligning with § 63A-16-1202's mandates for unlinkability, minimal disclosure, and individual control.

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

No. Our solution does not require retention of digital user credential information, and we recommend that the framework prohibits issuers and verifiers from doing so; operational metadata about credential issuance and verification that does not contain PII should be allowed, in order to ensure reliable service delivery. Credentials are created and issued to the holder's wallet, where they are stored and controlled by the individual. The State or issuer maintains only the same underlying authoritative records it already holds for physical credentials, but does not keep a copy of the digital credential itself.

Verification relies on cryptographic proofs and status mechanisms rather than storage of user data by the issuer. This ensures that the State can fulfill its role without accumulating unnecessary personal information, reducing both privacy risks and the liability of managing a central database of digital credentials.

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

Yes. We recommend that the SEDI framework include explicit requirements governing centralized storage, so that any compliant implementation protects against the unnecessary accumulation of credential data. Our proposed solution is designed so that credential information is issued to and held by the individual, without requiring centralized storage of user data in issuer or endorser infrastructure. Once a credential is provisioned, the State's systems related to issuance retain only metadata and the minimal authoritative records they already maintain for physical credentials, but do not need to store or replicate the digital credential itself.

This means the State can operate without retaining user data beyond what is necessary for its existing statutory functions. Verification is performed against cryptographic proofs presented by the holder, validated with issuer public keys or status lists, rather than by querying a central database of user records. This approach eliminates the risk of a centralized repository of identity data becoming a surveillance tool or a single point of failure, and aligns with Utah's statutory mandate for unlinkability and privacy by design.

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

One approach is the concept of **personal data licenses**, a term we coined to describe a way for individuals to control not just what data is disclosed, but how that data may be used after it is shared. In this model, when a resident presents a SEDI credential, the presentation can carry attached terms of use that specify limits. These terms act as a "license" for the data, setting rules such as whether the verifier may retain it, for how long, and whether it may be shared with third parties.

Another safeguard is the principle of **reasonable disclosure**, where the context of a transaction defines what information is appropriate to request. For example, at a bar, verifying that a resident is "over 21" is reasonable, but requesting an email address or home address is not. Reasonable disclosure rules ensure that residents share only what is required for the specific service being accessed, and that requests beyond that scope are treated differently: flagged, blocked, or subject to additional user consent.

For example, when proving age to purchase alcohol, a wallet could present only the attribute "over 21" along with a personal data license stating "for one-time use only; no storage or redistribution permitted." The verifier would receive the cryptographic proof along with these usage terms, which establish both a legal expectation and a compliance obligation. Wallets can surface these choices to users in simple prompts, giving them confidence that their data is not only minimally disclosed but also governed by enforceable conditions.

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

Our proposed solution allows residents to present a SEDI credential without ever handing over their device. The design principle is that the wallet acts as an intermediary between the holder and the verifier, enabling the holder to approve a presentation and share only the necessary information. The verifier receives a signed data package, but never gains access to the device itself.

In practice, this can be achieved through short-range exchanges such as scanning a QR code or establishing a secure wireless session, or through remote channels such as a secure web connection. In all cases, the holder's device remains under their control. The wallet enforces selective disclosure, warns the holder if excessive data is being requested, and cryptographically binds the presentation to the verifier's request to prevent misuse.

It is also possible to build in additional protections and safeguards into digital wallets. For example, the accelerometer can be used in conjunction with other sensors to detect actions that seem like device handover, and require additional authentication prior to revealing any information if a threshold of cumulative detection is met.

This approach protects residents from being compelled to surrender their device, prevents verifiers from accessing unrelated data, and ensures that identity transactions remain consistent with Utah's statutory requirements for privacy, unlinkability, and individual control.