HOUSE BILL REPORT
SB 5534

As Reported by House Committee On:
State Government & Tribal Relations

Title: An act relating to the use of verifiable credentials.

Brief Description: Concerning the use of verifiable credentials.

Sponsors: Senators Brown and Wagoner.

Brief History:
Committee Activity:
State Government & Tribal Relations: 2/21/22, 2/23/22 [DP].

Brief Summary of Bill

- Requires, by December 1, 2022, that the Consolidated Technology Services Agency (also known as WaTech), Department of Health, Department of Licensing, institutions of higher education, and the Secretary of State to each report which programs, services, and projects may be well-suited to the use of verifiable credentials as a means of improving efficiency, customer experience, and safeguarding privacy.
- Requires WaTech to create a process for developing a recommended trust framework for verifiable credentials (trust framework) in Washington, by October 1, 2022.
- Requires WaTech to develop and submit the trust framework, and any recommendations on legislation to implement the trust framework, to the Legislature by December 1, 2023.

HOUSE COMMITTEE ON STATE GOVERNMENT & TRIBAL RELATIONS

Majority Report: Do pass. Signed by 6 members: Representatives Valdez, Chair; Lekanoff, Vice Chair; Volz, Ranking Minority Member; Dolan, Graham and Gregerson.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Minority Report: Without recommendation. Signed by 1 member: Representative Walsh, Assistant Ranking Minority Member.

Staff: Desiree Omli (786-7105).

Background:

Blockchain Technology.

Adopted in Washington in 2020, the Uniform Electronic Transaction Act defines "blockchain" as a cryptographically secured, chronological, and decentralized consensus ledger or consensus database maintained via internet, peer-to-peer network, or other similar interaction. Blockchains are a type of database used to securely process and track the distribution of data across a large number of computers. Blockchain technology encrypts the contents of a record or a transaction, plus a few key pieces of metadata (such as the timestamp and the parties involved), into an output known as a hash, which is a short digest, or unique digital fingerprint, of the record. Changing the information recorded in a blockchain, or adding information to a blockchain, requires all the networks to cross-reference each other and a majority of the network to validate the information, thereby reaching "consensus," before the information entered is validated. This process allows the networks to identify potential tampering with information in a single block. In the private sector, while blockchain technology is most commonly associated with the cryptocurrency Bitcoin, other evolving applications can include insurance policies, property and real estate records, copyrights and licenses, supply chain tracking, and transactions in the financial services industry.

Trust Framework.

According to the National Institute of Standards and Technology (NIST) under the United States Department of Commerce, a "trust framework" is a set of rules and policies that govern how the members of the framework will operate and interact, including conducting identity management responsibilities, sharing identity information, using identity information that has been shared with them, protecting and securing identity information, performing specific roles, and managing liability and legal issues. In the context of identity verification, the NIST explains that a trust framework is used in federated identity management where organizations that share a common user base and transaction types develop a means to allow users to sign on and access multiple services through shared login and authentication processes. In other words, users are able to access the systems and applications of multiple organizations using one login credential. Organizations must trust the federated identity management processes of the other participating organizations in order to allow access to users that were authenticated by another entity. The rules for federated identity management are known as trust frameworks.

Summary of Bill:

By December 1, 2022, the Consolidated Technology Services (also known as WaTech), Department of Health, Department of Licensing, institutions of higher education, and the Secretary of State must each submit a report to the Legislature detailing which of the agency's programs, services, and projects may be well-suited for the use of verifiable credentials as a means for improving efficiency, customer experience, and safeguarding privacy. "Verifiable credential" is defined as a tamper-evident credential that has authorship which can be cryptographically verified.

In preparing its report to the Legislature, the named agencies must consult with appropriate technology industry representatives, including a Washington-based trade association, to ensure that the agencies are informed of the basic definitions and standards used by the technology industry in Washington for verifiable credentials.

By October 1, 2022, WaTech must develop a process for creating a recommended trust framework for verifiable credentials in Washington. The process should include public and private sectors and must involve participation with technology industry representatives, consumer protection advocates, and other similar stakeholders.

By December 1, 2023, WaTech must submit to the appropriate committees of the Legislature a recommended trust framework and any recommendations for legislation necessary to enact or implement the trust framework.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) This policy will promote the growth of verifiable credential technology within the state. Creation of this digital equivalency for verification of credentials such as transcripts and medical licenses is essential for efficient economical operation and saves thousands of hours of paperwork each year. Verifiable credentials are portable and provide efficiency. For example, in the field of education, verifiable credential technology can allow students to carry proof of diplomas, certificates, and transcripts in an electronic and secure way. Verifiable credential technology is currently being used in the medical field for patient privacy. This technology allows patients to carry their personal health information on their devices. The government issues many documents in paper forms to its citizens. The distribution of these documents can be done using verifiable credential technology. British Columbia has been implementing this work. The United States government has also supported this work through the Silicone Valley Innovation Program.

Creating a trust framework for verifiable credentials allows the state to proactively determine the standards used in this technology and requires a standard interoperability standard rather than require that each agency establish its own standards and definitions. The creation of a trust framework for verifiable credentials will establish an important regulatory framework that establishes the rules of the road to ensure that all parties have their needs met when using this technology. Without a trust framework for verifiable credentials, it could lead to commercial organizations deploying solutions which support their business needs over the needs of the community.

This bill creates a strong foundation for continued innovation. The technology anticipated by the bill does not necessitate the use of blockchain technology, but can use such technology.

(Opposed) None.

(Other) Verifiable credentials offer a path forward to solve problems with data security, privacy, bias, and discrimination. The Department of Licensing's recent breach is an example of the mess state agencies have with their current software. The policies in the bill might recreate or worsen today's problems because it leaves agencies that are responsible for creating the mess in charge of defining future pathways. It also prioritizes the technology industry's perspective rather than the needs of Washington residents. The involvement of a broader group of stakeholders is needed, such as communities historically impacted by technology discrimination and biases such as teachers, civil rights groups, small businesses.

Persons Testifying: (In support) Molly Jones, Washington Technology Industry Association; Arry Yu, Cascadia Blockchain Council; Kaliya Young, Verifiable Credentials Policy Committee-Washington State and California; and Michael Nash, Lumedic.

(Other) Jonathan Pincus, Washington People's Privacy Network.

Persons Signed In To Testify But Not Testifying: None.