Classes of Verifiable Credentials

Purpose

In order to be properly relied upon, every verifiable credential must be associated with a stated level of assurance. Since there are infinite variables in play to determine the level of assurance to be assumed, it is best to classify verifiable credentials in discrete class levels. This will allow a set of policies, practices and infrastructure to be defined and associated with specific classes. In the pre-verifiable credential world of the internet a variety of difference class structures are loosely defined depending on where a credential is stored and the level of authentication is used on the contents of a digital certificate. Multi-factor verification techniques are also used to upgrade amorphous classes of certificates and traffic.All Internet transactions and Verifiable Credentials have different purposes.

In the context of today's Internet traffic, transaction are mostly untrusted which has led to digital identity theft, spoofing, man in the middle attacks and ransomware. The advent of verifiable credentials brings the promise of a more trustworthy infrastructure for reliable transactions. When that infrastructure is combined with other trust assurance elements, verifiable credentials can be highly trustworthy and relied upon for a myriad of transformative digital applications.

The concept of classes for credentials is far from new. Back in late 1990's the US Office of Management and Budget had issued guidance, OMB M-04-04, which defined four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of identification credentials:

- **Level 1** - Little or no confidence in the asserted identity's validity;
- **Level 2** - Some confidence in the asserted identity's validity;
- **Level 3** - High confidence in the asserted identity's validity; and
- **Level 4** - Very high confidence in the asserted identity's validity.

The OMB guidance defined the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provided US Federal agencies with the criteria for determining the level of authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

An example of assigning class levels to digital credentials exist for SSL/TLS certificates that encrypt traffic from clients to web servers to protect web traffic. Classes of server authentication certificates have ben established as follows:

- **Class 1** Certificates are considered to be low assurance, as the verification method simply confirms that the Subscriber controls the asserted email address. No verification checks of the Subscriber's identity are performed. This level of validation is referred to as Domain Validation (DV).
- **Class 2** Certificates are considered to be medium assurance. They provide a greater level of assurance over Class 1 Certificates, because in addition to email address control, basic verification steps are performed to confirm the identity of the Subscriber. This level of validation is referred to as Organization Validation (OV). The following Certificate types qualify as Class 2 Certificates:
    - Standard SSL
    - Wildcard SSL
    - Code Signing
    - Document Signing
- **Class 3** Certificates provide a high level of assurance. They are issued only after rigorous validation of the identity of the Subscriber. This level of validation is referred to as Extended Validation (EV). The following Entrust Certificate types qualify as Class 3 Certificates:
    - EV SSL
    - EV Code Signing

NIST has more recently published (https://pages.nist.gov/800-63-3/sp800-63-3.html) generally accepted associated classes as it relates to identity credentials. Digital identity as a legal identity further complicates the definition and ability to use digital identities across a range of social and economic use cases. Digital identity is hard. Proving someone is who they say they are — especially remotely, via a digital service — is fraught with opportunities for an attacker to successfully impersonate someone. The standards associated with identity assurance create a solid model for other claims made in a verifiable credential

The components of identity assurance detailed in the NIST guidelines are as follows:

- **IAL** refers to the identity proofing process.
    - **IAL1**: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such (including attributes a Credential Service Provider, or CSP, asserts to an RP).
    - **IAL2**: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
    - **IAL3**: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes can be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.
- **AAL** refers to the authentication process.
    - **AAL1**: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
    - **AAL2**: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.
    - **AAL3**: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

- **FAL** refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).
    - **FAL1**: Allows for the subscriber to enable the RP to receive a bearer assertion. The assertion is signed by the IdP using approved cryptography.
    - **FAL2**: Adds the requirement that the assertion be encrypted using approved cryptography such that the RP is the only party that can decrypt it.
    - **FAL3**: Requires the subscriber to present proof of possession of a cryptographic key referenced in the assertion in addition to the assertion artifact itself. The assertion is signed by the IdP and encrypted to the RP using approved cryptography.

Identity proofing establishes that a subject is who they claim to be. The process of identity proofing can be translated to other claims made in a verifiable credential. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously. This directly translates to the usage of verifiable credentials

In addition to NIST levels above, other standards have addressed levels of assurance that are applied to the classes of verifiable credeintials:

Pan-Canadian Trust Framework (PCTF) Levels of Assurance (LOA) Qualifiers: The current version of the PCTF conformance criteria use the four PanCanadian Levels of Assurance (LOA):

- Level 1: little or no confidence required
- Level 2: some confidence required
- Level 3: high confidence required
- Level 4: very high confidence required

eIDAS (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. eIDAS has established level of Assuarnce qualifiers which can be used in verifiable credential classification. eIDAS qualifiers may be based on the three levels of assurance defined by the European Regulation No 910/2014 on electronic identification and trust services for electronic transactions:

- Low: low degree of confidence
- Substantial: substantial degree of confidence
- High: high degree of confidence

Classes below also consider **Vectors of Trust**, a proposed IETF standard (RFC 8485, October 2018). Currently, the VoT proposal consists of four components that may be used as qualifiers:

- **Identity Proofing (P)**: describes how likely it is that a given digital identity transaction corresponds to a particular, realworld identity
    - P0: No proofing is done, and data is not guaranteed to be persistent across sessions
    - P1: Attributes are self-asserted but consistent over time, potentially pseudonymous
    - P2: Identity has been proofed either in person or remotely using trusted mechanisms (such as social proofing)
    - P3: There is a binding relationship between the identity provider and the identified party (such as signed/notarized documents and employment records)
- **Primary Credential Usage (C)**: defines how strongly the primary credential can be verified. The primary credential usage component of this attribute represents distinct categories of primary credential that MAY be used together in a single transaction. Multiple distinct values from this category MAY be used in a single transaction.
    - C0: No credential is used / anonymous public service
    - Ca: Simple session HTTP cookies (with nothing else)
    - Cb: Known device, such as those indicated through device posture or device management systems
    - Cc: Shared secret, such as a username and password combination
    - Cd: Cryptographic proof of key possession using shared key
    - Ce: Cryptographic proof of key possession using asymmetric key
    - Cf: Sealed hardware token / keys stored in a trusted platform module
    - Cg: Locally verified biometric
- **Primary Credential Management** :The primary credential management component conveys information about the expected lifecycle of the primary credential in use, including its binding, rotation, and revocation
    - Ma: Self-asserted primary credentials (user chooses their own credentials and must rotate or revoke them manually) / no additional verification for primary credential issuance or rotation
    - Mb: Remote issuance and rotation / use of backup recover credentials (such as email verification) / deletion on user request
    - Mc: Full proofing required for each issuance and rotation / revocation on suspicious activity
- **Assertion Presentation:** defines how well the credential information can be communicated across the network without information leaking to unintended parties and without spoofing
    - Aa: No protection / unsigned bearer identifier (such as an HTTP session cookie in a web browser)
    - Ab: Signed and verifiable assertion, passed through the user agent (web browser)
    - Ac: Signed and verifiable assertion, passed through a back channel
    - Ad: Assertion encrypted to the RP's key subject

In order to define discrete classes of verifiable transactions, it is key to identify the variables that make a credential more trustable. The following are factors embodied in the class definitions:

- Credential defined in a Governance Framework at a stated level of assurance
- The degree of assurance that the public key of the signer in a verifiable credential is matched to the possessor of the private key
- The degree of authentication of data that is performed on the contents of a verifiable credential
- The security and protection of the wallet containing the credential
- The security and availability of a registry containing in the credential (if not held in a wallet)
- The security and availability of the public key in a credential for verification purposes
- The trustworthiness of the personnel and infrastructure of the Issuer of a verifiable credential
- The asserted policies of the Issuer
- The degree that practices that meet the Issuer policies are part of a trust assurance scheme
- The rigor of a trust assurance scheme of the ecosystem that governs the credential

Proposed Classes of Verifiable Credentials

The next sections on this page present the proposed classes of credentials under Trust over IP guidance

Class 1 – Untrusted Credentials

Attribute of class: Credentials that are not under standard or ToIP guidance

Examples: Peer to peer transactions, convenience credentials

- Credential defined in a Governance Framework at a stated level of assurance: **No**
- The degree of commensurate assurance that the public key of the signer in a verifiable credential is matched to the possessor of the private key (early OMB guidance): **Level 1**
- The degree of authentication of data that is performed on the contents of a verifiable credential: **None**
- The security and protection of the wallet containing the credential: **None**
- The security and availability of a registry containing in the credential (if not held in a wallet): **No controls**
- The security and availability of the public key in a credential for verification purposes: **No requirements**
- The trustworthiness of the personnel and infrastructure of the Issuer of a verifiable credential: **No requirements**
- The asserted policies of the Issuer: **No requirements**
- The degree that practices that meet the Issuer policies are part of a trust assurance scheme: **No trust assurance scheme**
- The rigor of a trust assurance scheme of the ecosystem that governs the credential: **No trust assurance scheme**
- Mapped Level to other Standards:
    - NIST 800-63-3: **IAL1, AAL1, FAL1**
    - PCTF: **Level 1**
    - eIDAS: **Low**
    - Vectors of Trust: **P0, C0 Ma, Aa**

Class 2 – Minimum Internet Grade Credentials

Examples: College transcripts, professional credentials, loyalty credentials

- Attributes of Class:
    - Credentials covered under minimum guidance of the ToIP Foundation : Includes most unregulated verifiable claims
- Example credentials: College degree credentials, non-title provenance claims
- Credential defined in a Governance Framework at a stated level of assurance: **Yes at Class 2**
- The degree of commensurate assurance that the public key of the signer in a verifiable credential is matched to the possessor of the private key (early OMB guidance): **Level 2**
- The degree of authentication of data that is performed on the contents of a verifiable credential: **Authentication Procedures are in place and self-asserted**
- The security and protection of the wallet containing the credential: **ToIP Compliant Wallet Optional**
- The security and availability of a registry containing in the credential (if not held in a wallet): **Moderate controls identified in Class 2 Credential Policy**
- The security and availability of the public key in a credential for verification purposes: **Moderate controls identified in Class 2 Credential Policy**
- The trustworthiness of the personnel and infrastructure of the Issuer of a verifiable credential: **Moderate controls identified in Class 2 Credential Policy**
- The asserted policies of the Issuer: **Class 2 Credential Policy**
- The degree that practices that meet the Issuer policies are part of a trust assurance scheme: **A Defined Trust Assurance Framework**
- The rigor of a trust assurance scheme of the ecosystem that governs the credential: **Self-Assertion by ecosystem roles**
- US Federal PKI equivalence: Basic Assurance
- Mapped Level to other Standards:
    - NIST 800-63-3: **IAL2, AAL1, FAL1**
    - PCTF: **Level 2**
    - eIDAS: **Between low and substantial**
    - Vectors of Trust: **P2, Ce, Mb, Ab?**

Class 3 – Asset Value Grade Credentials

Examples: Digital driver's license, bank transfer credentials. Title claims

- Attributes of Class:
    - Identity Credential Used for Asset Transfer such as digital driver's license, passport or bank identity credential, title claims
- Credential defined in a Governance Framework at a stated level of assurance: **Yes at Class 3**
- The degree of commensurate assurance that the public key of the signer in a verifiable credential is matched to the possessor of the private key (early OMB guidance): **Level 3**
- The degree of authentication of data that is performed on the contents of a verifiable credential: **Authentication Procedures are in place, asserted and attested by a third party**
- The security and protection of the wallet containing the credential: **ToIP Compliant Wallet Required (Layer2)**
- The security and availability of a registry containing in the credential (if not held in a wallet): **Medium level controls identified in Class 3 Credential Policy**

- The security and availability of the public key in a credential for verification purposes: **Medium level controls identified in Class 3 Credential Policy**
- The trustworthiness of the personnel and infrastructure of the Issuer of a verifiable credential: **Medium level controls identified in Class 3 Credential Policy**
- The asserted policies of the Issuer: **Class 3 Credential Policy**
- The degree that practices that meet the Issuer policies are part of a trust assurance scheme: **A Defined Trust Assurance Framework**
- The rigor of a trust assurance scheme of the ecosystem that governs the credential: **Assertion by ecosystem roles and attestation by independent third party**
- Mapped Level to other Standards:
    - NIST 800-63-3: **IAL2, AAL2, FAL2**
    - PCTF: **Level 3**
    - eIDAS: **Substantial**
    - Vectors of Trust: **P2, Cf, Mc, Ac?**

Class 4 – High Assurance Grade Credentials

Examples: Clearance credentials, Military operations, access to Coke recipe.

- Attributes of Class:
    - Identity Credential Used for High Assurance, High Value, Sensitive Purposes
- Credential defined in a Governance Framework at a stated level of assurance: **Yes at Class 4**
- The degree of commensurate assurance that the public key of the signer in a verifiable credential is matched to the possessor of the private key (early OMB guidance): **Level 4**
- The degree of authentication of data that is performed on the contents of a verifiable credential: **Authentication Procedures are in place, asserted and attested by a third party and certified by a recognized certification body**
- The security and protection of the wallet containing the credential: **ToIP Compliant Wallet Required (Layer2) that is FIPS 140-2 3 compliant**
- The security and availability of a registry containing in the credential (if not held in a wallet): **High level controls identified in Class 4 Credential Policy**
- The security and availability of the public key in a credential for verification purposes: **High level controls identified in Class 4 Credential Policy**
- The trustworthiness of the personnel and infrastructure of the Issuer of a verifiable credential: **High level controls identified in Class 4 Credential Policy**
- The asserted policies of the Issuer: **Class 4 Credential Policy**
- The degree that practices that meet the Issuer policies are part of a trust assurance scheme: **A Defined Trust Assurance Framework**
- The rigor of a trust assurance scheme of the ecosystem that governs the credential: **Assertion by ecosystem roles and attestation by independent third party and certified by a recognized certification body**
- Mapped Level to other Standards:
    - NIST 800-63-3: **IAL3, AAL3, FAL3**
    - PCTF: **Level 4**
    - eIDAS: **High**
    - Vectors of Trust: **P3, Cf, Mc, Ad?**