Governance Role and Process Definitions

Contributors

- Scott Perry

Executive Summary

The following process and role descriptions were first derived from "The Trust Over IP Stack", a concept RFC issued by the Hyperledger Aries Project. The contents of the RFC can be found at https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0289-toip-stack/README.md. These definitions were created as a companion to Governance Authorities developing ToIP-compatible Governance Frameworks as a majority set for consideration.. It enables Governance Authorities to use consistent terminologies to describe stakeholders and their processes that participate in a ToIP ecosystem. These frameworks include an assortment of rules; there rules apply to roles which execute processes identified in this document. All of these roles and processes MAY NOT appear in governance frameworks and some roles and processes appearing in frameworks MAY NOT be listed in this document.

Roles

- **Roles Acting within Layer 4 - Ecosystem**
  - Ecosystem Governance Authority - An entity that establishes and operates a framework (Ecosystem Governance Framework (EGF)) of policies, rules, procedures and accountabilities of roles within Layer 4 (Ecosystem)
  - Interoperable Ecosystem Governance Authority - An entity that establishes a TSS (ToIP Standard Specification) that defines the standard requirements for the Ecosystem Governance Authority to conform.
  - Member Directory - Provides both human- and machine-searchable listings of the public DIDs and other searchable attributes of participants in the EGF.
  - Auditor - An entity which can independently attest to participants assertion of compliance with EGF requirements.
  - Audit Accreditor - An Entity that qualifies Auditors and provides auditing standards
  - Accreditation Authority - An authoritative entity responsible for declaring that a certification body under its assessment methodology has satisfies its vetting requirements
  - Certification Body - An authoritative entity responsible for declaring that an entity under its assessment methodology has satisfies its vetting requirements against a set of trust criteria
- **Roles Acting within Layer 3 - Credential**
  - Credential Governance Authority - An entity that establishes and operates a framework of policies, rules, procedures and accountabilities of roles within Layer 3 (Credential)
  - Credential Registry - are alternative holders of credentials to support other uses, such as public searchable directory services.
  - Authoritative Issuer - are credential issuers authorized by the ecosystem and/or credential governance authority to issue specific types of credentials at specific levels of assurance
  - Insurer - An entity which provides insurance to issuers operating under the terms of a governance framework.
  - Holder - An entity that owns the right to access and protect verifiable credentials for use
  - Verifier - An entity that seeks cryptographic and other evidence of the validity of claims on verifiable credentials.
  - Escrow Service - An entity that holds keys in escrow for legal. compliance and recovery purposes.
  - Biometric Service Provider - can be used to strengthen confidence in the binding between a credential and its authorized holder.
  - PII Controller
  - PII Processor
  - PII Third Parties
- **Roles Acting within Layer 2 - Provider**
  - Provider Governance Authority - - An entity that establishes and operates a framework of policies, rules, procedures and accountabilities of roles within Layer 2 (Provider)
  - Hardware Provider - An entity who provides ToIP-compliant hardware, e.g., secure enclaves, trusted execution environments, HSMs.
  - Software Provider - An entity who provides ToIP-compliant agents, wallets, secure data stores, etc.
  - Agency - An entity who hosts ToIP-compliant cloud agents for individuals, organizations, and guardians.
  - Secure Data Store - A database with three special properties:
    1. It is controlled exclusively by the DID controller (person, organization, or thing) and not by any intermediary or third party.
    2. All the data is encrypted with private keys in the subject's KMS.
    3. If a DID controller has more than one secure data store, the set of stores can be automatically synchronized according to the owner's preferences.
  - Digital Guardian - an individual or organization willing to take legal responsibility for managing that cloud agent/wallet on behalf of a person under a guardianship mandate
  - Digital Delegate - One who receives digital authority and responsibility to carry out limited digital tasks on behalf of another
  - Digital Dependent - An Individual whose circumstances or capabilities, in a given context, requires dependence upon another operating under a guardianship mandate, to administer an that person's identity data
  - Thing Controller - An individual who digitally controls something that is by its nature incapable of acting on its own behalf
- **Roles Acting within Layer 1 - Utility** (Verifiable Data Registry)
  - Utility Governance Authority - An entity that establishes and operates a framework of policies, rules, procedures and accountabilities of roles within Layer 1 (Utility)
  - Transaction Author - An entity that initiates transactions to add records on a distributed ledger
  - Transaction Endorser - An entity that executes permission transactions for Transaction Authors
  - Steward - A node operator of a distributed ledger
- **Roles Acting Independent of Layer**
  - Jurisdictional Authority - A legal authority that has established laws in the geographic territory of a participating ecosystem
  - Industry Authority - A recognized body in the governance authority's industry (or related industry) that has established standards and reputation that governance authority desires alignment and/or conformance
  - Standards Authority - A recognized body that has established standards and reputation that an governance authority desires alignment and/or conformance

Processes

- **Layer 4 - Ecosystem Layer**
  - Governance Processes and Standards
    - Risk Assessment - A subjective process to identify potential threats of a Governance Framework's scope upon its purpose and objectives and derive a proportionate plan to address them.
    - Governance Authority
      - Governance Authority Establishment - activities to convene stakeholders aligned to oversee a layer of the ToIP stack.
      - Governance Framework Establishment - activities used to draft and enact an initial document containing key directives of a Governance Authority.
      - Governance Framework Government
        - Member Application
          - Member Contracting - the presentment and agreement of terms that a Governance Authority has with its participating members.
          - Member Fee Management - the billing and collection of financial obligations required by a Governance Authority with its members.
        - Member Vetting - the unbiased due diligence of prospect members against a set of acceptance criteria.
        - Member Voting - collecting and tabulating definitive choices made to members on proposed Governance Authority actions.
      - Policy Management
        - Policy Establishment - activities used to draft and enact an initial set of requirements and guidance a Governance Authority has upon its scope aligned with its purpose and objectives.
        - Policy Adoption - the acceptance of rules and guidance that a Governance Authority presents to itself and its members.
        - Policy Enforcement - activities that a Governance Authority takes to hold itself and its members accountable of its rules and guidance.
        - Policy Amendment - The reevaluation and change of previously established rules and guidance.
      - Governance Authority Communication
        - DID Publication - The presentment of availability of a decentralized identifier.
        - DID Whitelisting - The collection and enablement of decentralized identifiers specifically allowed actions specified by a Governance Authority.
        - Verifiable Credential Publication - the availability establishment of verifiable credentials to stakeholders within an ecosystem.
        - Levels of Assurance - the pre-defined tiers of risk mitigation afforded a class of transactions within an ecosystem.
    - Member Directory Designation and Recognition - The collection and enablement of approved Member entries available for transaction consideration within a Governance Authority.
    - Credential Registry Designation and Recognition - The collection and enablement of approved Credential Registries for transaction consideration within a Governance Authority.
    - Authoritative Issuer Designation and Recognition - The collection and enablement of approved Authoritative Issuers for transaction consideration within a Governance Authority.
    - Authoritative Verifier Designation and Recognition - The collection and enablement of approved Verifiers for transaction consideration within a Governance Authority.
    - Verifiable Credential Standards - The set of rules enacted by a Governance Authority that apply to a set of verifiable credentials under its scope.
    - Governance Trust Assurance Processes - The set of governance activities enacted by a Governance Authority to hold its stakeholders accountable for its governance rules.
  - Trust Mark Processes
    - Trust Mark Scheme Definition - The set of activities a Governance Authority defines to establish and regulate its issuance of Trust Marks.
    - Trust Mark Vetting Process - The evaluation of candidate actions against a pre-defined set of criteria to determine their eligibility for trust mark issuance.
    - Trust Mark Issuance Process - The presentment of Trust Marks to approved recipients.
    - Trust Mark Discovery Process - The search and identification activities of interested parties of a Governance Authority's Trust Marks
    - Trust Mark Revocation - The rescindment of a previously approved Trust Mark by a Governance Authority
    - Trust Mark Expiration - The state when a Trust Mark exceeds its stated approval period enacted by a Governance Authority
  - Trust Assurance Scheme Processes
    - Self-Certification - The assertion a stakeholder makes that it is compliant with trust criteria established by a Governance Authority. This MAY or MAY not be supported with evidence.
    - Internal Attestation - The opinion of an internally independent arbiter over asserted claims by a stakeholder of its compliance to governance authority trust criteria.
    - External Attestation - The opinion of an externally independent arbiter over asserted claims by a stakeholder of its compliance to governance authority trust criteria.
    - Certification - The declaration of an approved Certification Body that an entity under an approved assessment methodology has satisfies its vetting requirements against a set of trust criteria
  - Auditor Processes and Standards - The set of accepted practices guiding the attestation of of an entity's assertion over its compliance with established Governance Authority trust criteria.
  - Audit Accreditor Processes and Standards - The evaluation and oversight activities enacted by a an Auditor Accreditor to approve and regulate auditors for a Governance Authority
- **Layer 3 - Credential Layer**
  - Governance Processes and Standards - (See Layer 4)
  - Issuer Processes
    - Credential Enrollment Processes - The set of activities that establishes the initial application of a credential.
    - Issuer Vetting Process (Prior to Credential Issuance) - The due diligence activities an Issuer takes to validate evidence supporting information on a credential and/or the subject's rights associated with it.
    - Credential Lifecycle Processes
      - Credential Signing - The application of cryptographic keys upon a credential by an Authoritative Issuer asserting its claims.

- Credential Issuance - The presentment of a credential making it available to stakeholders.
- Credential Modification - The amendment of information (not keys) of a credential.
- Credential Re-Keying - the replacement of cryptographic keys upon a previously issued credential.
- Credential Renewal - the set of re-approval activities made to a previously issued credential upon reaching the end of its validity period.
- Credential Suspension - The subjective segregation of a previously approved credential to a non-available condition.
- Credential Revocation - The set of denouncement activities that renege a credential's approval state.
- Credential Distribution - The transfer activities of a credential from an Issuer to a Holder or other stakeholder.
- Credential Expiration - The state when a credential exceeds its stated approval period enacted by an Authoritative Issuer.
- Credential Purge - The removal activities of a credential from an active repository after it has exceeded its useful life
- Credential Archival - The long-term storage in an inactive repository of credential for the purpose of providing evidence to a claim.

- Credential Status Services
  - Enabling Discovery of Invalid/Revoked Credentials - Presentment activities to allow Verifiers to check the revocation status of a credential.
  - Maintenance of Credential Status - The activities to amend revocation status of credentials and make them available to interested Verifiers.
  - Availability Processes of Credential Status - The infrastructure activities enacted to maintain availability of credential status according to governance rules.
- Issuer Infrastructure Processes
  - Physical Protection - the set of physical security activities employed to preserve the operation of information technology assets needed by an Issuer
  - Environmental Protection - the set of environmental security activities employed to preserve the operation of information technology assets needed by an Issuer
  - Systems Development Life Cycle Processes - The set of activities that a developer of Issuer software employs to make approved changes and preserve the operational integrity of Issuer software.
  - Network Security Processes - The set of communication and perimeter protection activities employed to preserve the operation of information technology assets needed by an Issuer.
  - Trusted Personnel Processes
    - Hiring Practices - The set of pre-employment hiring activities employed by an Issuer to perform due diligence of Trusted personnel candidates that are slated to be involved with Issuer processes.
    - Vetting Processes - The set of due diligence process activities employed by an Issuer to validate that those personnel candidates slated to be involved with Issuer processes meet minimum standards.
    - Training Processes - The set of education process activities employed by an Issuer to ready personnel involved with Issuer processes to perform job responsibilities.
    - Removal Process - The set of activities involved with evaluating performance of Issuer personnel and removing them from their job responsibilities if they do not meet minimum standards.
  - Transaction Logging - The collection of Issuer activity records need to monitor Issuer performance and retain evidence for later claim adjudication.
  - Records Archival - The storage of activity attributes in a separate protected repository for the purpose of potential historical claims adjudication.
  - Compromise / Disaster Recovery - The declaration that an Issuer's ability to properly perform its duties has been severely impaired and must be restored to a previous state of acceptable operation.
  - Private Key Management
    - Private Key Access - The activities whereby a rightful owner obtains access to a cryptographic to be used for signing activities.
    - Private Key Storage - The safekeeping activities of a cryptographic signing key by its rightful owner.
    - Private Key Backup - The duplication activities of a cryptographic signing key by its rightful owner to ensure its continued use in the event of loss.
    - Private Key Activation - The unveiling of protection measures that enables a rightful owner access to their cryptographic signing key.
    - Private Key Deactivation - The activities that make a cryptographic signing key unavailable for use by its rightful owner.
    - Private Key Destruction- The permanent disablement activities of a cryptographic signing key.

- Holder Processes
  - Credential Request - The solicitation activities of a potential subject of a verifiable credential to an Authoritative Issuer.
  - Proof Presentation - The presentment activities of a verifiable credential to a Verifier.
  - Credential Acceptance - The acknowledgement activities of a Subject of verifiable credential to its pertinence.
  - Credential Loading - The injection activities of a verifiable credential by a holder into ToIP-compatible digital wallet.
- Verifier Processes
  - Proof Request - The solicitation activities by a Verifier seeking evidence to support claims embedded on a verifiable credential.
  - Signature Verification - The validation activities performed by a Verifier in matching a cryptographic public key to an independent source (e.g. DID record on a ToIP-compatible utility).
  - Credential Status Services
    - Credential Status Request - The inquiry activities of a Verifier seeking to determine whether a verifiable credential has been revoked after issuance.
    - Responses to Invalid/Revoked Credential - The feedback activities directed to a Verifier as a result of a Credential Status Request.

- **Layer 2 - Agent Layer**
  - Governance Processes and Standards (See Layer 4)
  - Agent Processes
    - Agent Activation
    - Agent/Data Store Pairing
    - Data Store Synchronization
    - Agent Deactivation
    - Key Pair Storage
    - DID Exchange
    - Key Management System (KMS) Creation

        - KMS Recovery
    - Guardianship Processes
        - Guardianship Inception - Activities to identify the need for a guardian and assess if the need is legitimate.
        - Guardianship Creation - Activities to create the actual guardianship relationship by creating the digital wallet the guardian will use for the dependent and issuing the necessary guardian, dependent, and delegation credentials.
        - Guardianship Usage - Activities to cover the real-life usage of the digital wallet and credentials the guardian holds on behalf of the dependent
        - Guardianship Termination - Activities justifying and ending with the revocation of all guardianship credentials for a given dependent
    - Hardware Developer Processes
        - Systems Development Life Cycle - processes for planning, creating, testing, and deploying an agent hardware-based system
    - Software Developer Processes
        - Systems Development Life Cycle - processes for planning, creating, testing, and deploying an agent software-based system
- **Layer 1 - Utility Layer**
    - Governance Processes and Standards (see Layer 4)
        - Permissioned/Permissionless Blockchains: A permissioned blockchain needs prior approval before using whereas a permissionless blockchain lets anyone participate in the system.
        - Steward (Node) Configuration - The architecture of number and types of stewards (nodes) to create and endorse the transactions that are proposed on the network.
        - Consensus Model - The synchronization algorithm that a DLT Network deploys to ensure that ledgers only approve additions when the participants confirm transactions.
        - Data Structures
            - Schemas - a machine-readable definition of the semantics of a data structure that define the claims (attributes) that can be included in verifiable credentials
                - Overlays - Multi-dimensional object layer consisting of a set of data objects that serve a specific function in an overall schema definition which, when amalgamated, provide a set of metadata that adequately describes a single set of data.
                - Base - stable data construct that defines a single set of data in its purest form thus providing an anchor from which to flexibly build a decentralized data definition.
            - Credential Definitions - specify the claims and related metadata needed by an issuer of verifiable credentials
        - Data Security Methods - Activities that a utility layer provides to protect against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.
        - Data Privacy Methods - Activities that a utility layer provides to ensure that personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.
    - Transaction Initiation - The presentment activities of a new transaction for consideration of inclusion on a distributed ledger.
    - Transaction Endorsement - Activities that validate candidate transactions and declare their validity for addition to the distributed ledger.
    - Steward Operational Processes - Activities that a steward (Node) performs to receive, endorse and add transactions to a distributed ledger.