### A Periodic Table of Trust Elements

**Draft Rev. 20131108**

#### Operational Federated Trust - contracts and policy (operator to member and operator to operator)

- Terms of Use (IdP)
- Terms of Use (SP)
- Liability and Indemnification
- Interfederation / Publish rights
- Economics, settlements, etc.
- Incident reporting and response
- Change Management
- Obligations and Rights of Federation Operator
- Obligations and Rights of Federation Members
- Termination / Dispute Resolution
- Data Protection

#### Operational Federated Trust - technical issues (operator to member and operator to operator)

- Identity setting of members
- Signing Key strength of members
- Protection of member’s signing key
- Submission process for member keys and other metadata to federated registry – technology, LOA
- Operation of the federation registry – protection of federation key strength of signing key
- Exchange protocols and policies in interfederated instances of metadata consumption
- What tags are RP authorized to assert?
- What tags are the IdP authorized to assert?

#### Operational — Federated-defined metadata (either operator or third party)

- Metadata tags for end-entities
- Member responses to various common metadata tags
- Technology profiles supported
- Common schema and Normative attributes, e.g. eduPerson
- Audits of members
- Liability for losses
- Termination rights
- Enforcement mechanisms
- Warranties
- Dispute resolution
- Measure of damages

#### Community of Interest (member to member)

- Member responses to various common metadata tags
- Technology profiles supported
- Common schema and Normative attributes, e.g. eduPerson
- Audits of members
- Access controls and access management to AP
- Facilities, Management and operational controls, including technical security
- Compliance Audit and other Assessments
- Other business and legal matters, including liability, dispute resolution, fee schedules etc
- Governance of COI, including COI policy/standards processes
- Levels of assurance supported
- Community LOA agreements (e.g. MFA failover approaches) and other community of practice issues

#### Attribute authorities/providers to COI members (AP to IdP, AP to RP, AP to middlebox/broker)

- Attributes published and publication methodologies supported
- Revocation/Refresh issues
- Methodology of enrichment of identifier into AP domain
- Methodology of validation of attribute values, along with a possible assurance indicator
- Access controls and access management to AP
- Facilities, Management and operational controls, including technical security
- Compliance Audit and other Assessments
- Other business and legal matters, including liability, dispute resolution, fee schedules etc
- Privacy - Individual control/use limitation, tools for management, support of consent, etc.
- Privacy - User Access to their own data and recourse for data accuracy
- Privacy - Retention
- Privacy - Reuse of information by RP to third parties and downstream services

#### Enterprise/organization/IdP/RP/AA/AP to user (member to user)

- Assurance - Identity proofing
- Assurance - Credential issuance
- Assurance - Credential management
- Authentication rules
- Audit
- Privacy - T&Cs
- Privacy - Transparency of operations
- Privacy - Retention

**NOTE:** The table is based on a multi-lateral full-mesh federation model. A hub-and-spoke federation model would move certain elements into other rows of relationships. A dynamic federation model, not yet well understood, could move elements around as well or recast elements.

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.