A Periodic Table of Trust Elements

Draft Rev. 20131031

Policy setting & governance

Technical

Operations

Legal

Privacy

NSTIC Guiding Principles 1-4

http://www.idecosystem.org/page/adherence-nstic-guiding-principles

1. ***Identity solutions will be privacy-enhancing and voluntary.***
2. ***Identity solutions will be secure and resilient.***
3. ***Identity solutions will be interoperable.***
4. ***Identity solutions will be cost-effective and easy to use.***

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.	Change Management	Obligations and Rights of Federation Operator	Obligations and Rights of Federation Members	Termination / Dispute Resolution	Data Protection	Audit of federation operator
1, 2, 3	1, 2, 3	2	3	3, 4	2	2, 3	1, 2, 3, 4		1, 2	2

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

Identity vetting 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/ metadata – protection of federation key strength of signing key	Logging	Exchange protocols and policies in interfederated instances of metadata consumption
1, 2	2	2	2, 3	2	1, 2	2, 3

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

Metadata tags for end-entities	What tags are RP authorized to assert? How is that scoped and accredited?	What tags are the IdP authorized to assert? How is that scoped and accredited?
3, 4	3, 4	3, 4

Community of Interest (member to member)

Incident reporting and response	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
2	3, 4	3	3	1, 2	2	2	2	2	1, 2, 3, 4	1, 2, 3, 4

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
2, 3, 4	1, 2, 3	2, 3, 4

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

Semantics, including null, single or multi valued issues	Possible values and formats	Availability	Methodology of validation of attribute values, along with a possible assurance indicator
3	3	2, 4	3

Attributes published and publication methodologies supported	Revocation/Refresh issues	Methodology of enrollment of identifier into AP domain
1, 3	1, 2, 3	1

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
1, 2	2	1, 2	2

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+C's	Privacy - Transparency of operations	Privacy - Retention	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 -Reuse of information by RP to third parties and downstream services
1, 2, 3	1, 2, 3	1, 2, 3	1, 2, 3	1, 2	1	1	1	1, 2	1	1

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.