



Go

7 captures

31 Aug 13 – 24 Aug 14

OCT DEC AUG

27

2012

2013

2014

Close

Help



CIVICS.COM

A Public Information Resource of Dazza Greenwood, JD

[ABOUT](#) [BLOG](#) [IDENTITY](#)
[MODEL RULES & AGREEMENTS](#) [CONTACT](#)

Identity System Rules: FAQ

Under Development.

[Below are the initial FAQ topics being drafted for the first version of this page]

1. What are “System Rules” and how do I know if I need them?
2. How do I develop a set of business, legal and technical rules defining and governing an identity and/or data sharing system?
3. How can liability and other risk allocation approaches be developed in a way that will work in the specific context of the parties and transactions involved in our identity system while still keeping the framework as standard as possible?
4. How does Accreditation and Certification work with System Rules?
- 4.a: How can a collaborative organization comprised of government and private sector entities jointly define, operate and enforce Accreditation and Certification of a common identity federation or system?

The US Federal Government and a range of private sector banks, technology and other companies known as the eAuthentication Partnership (EAP) published a [federated identity Trust Framework](#), and both Section 1. Business Rules and Section 4 covering Accreditation and Certification Rules demonstrate an example

This memo developed as part of facilitation and drafting of the EAP Rules describes the basic landscape of “[Accreditation, Certification and Assessment Models](#)”. The memo was an important grounding for the strategic and tactical choices by the government and corporate participants about the best value and practical fit of Accreditation and Certification for their needs and purposes.

The [FiXs Certification and Accreditation Process](#) provides a good example of how a mature certification scheme looks for a production grade and secure identity system

4.b: What are the foundational issues and options to consider when establishing a governance and rules for certifying and approving identity system components, parties and services?

The [CARAT Guidelines](#) (especially Sections B, C and D) set out building block concepts and considerations for public/private identity system certification and approval of parties, services and components. The document provides basic background on how governance, business, legal and technical dimensions of a large scale identity system can be designed and architected for public/private partnerships. While this document was tailored to PKI systems, the vast majority of the content referenced above remains relevant and foundational.

These [background materials on the CARAT Guidelines](#) demonstrate how a group of organizations can organize a request for proposals by trade associations so as to determine the best value and best fit to provide secretariat, administrative, intellectual property and other basic functions (today’s equivalents might be OIX, Kantara and the like). Absent an “apples to apples” review of more than one potential trade association, it is difficult or impossible to establish best value and appropriate fit (e.g. regarding how much staffing and resource it provides, how restrictive or flexible it is regarding the organizational and legal arrangements and whether it supports or inhibits the parties right to choose later to spin off if the project is successful and to take their IPR with them when joining a different more suitable group or creating a new specially tailored association).

4.c: How can self-asserted statements form the basis of an approval for identity providers within a federation?

InCommon is widely regarded as one of the most successful and exemplary identity federations in the world. However, this federation does not require or depend upon third party certification as the basis of trustworthiness. The [Operational Practices](#) demonstrate how self asserted statements, in the context of broader business arrangements, legally enforceable contracts and technical security and interoperability conformance can be structured for an effective, efficient, secure and scalable identity system across many parties, jurisdictions, networks, platforms, services and applications.

5. How do I get from “final rules” to “full production” for my system?

6. What if something major changes in my business, legal and/or technical system and the Rules don’t address the new situation?

Copyright © 2013 | CIVICS.com is proudly powered by WordPress.org - 