

Trust Frameworks

Work of the MIT CFP Privacy and Security Working Group

Karen R. Sollins, MIT CSAIL,

April 25, 2014



Trusting Trust



“You can’t trust code that you did not totally create yourself.”

--- Ken Thompson, **Reflections on Trusting Trust**,
Turing award lecture, 1984

What is “trust” about?



▶ Assurance

- ▶ Identification of assurance: Trustmark
- ▶ Domain of applicability: identification, authorization, privacy, anonymity... Symantec
- ▶ Context: risks, kinds of activities or transactions, players, etc.
- ▶ Underpinnings for assurance
 - ▶ Technical
 - ▶ Business
 - ▶ Legal



Symantec

▶ Framework for trust

- ▶ Definition of rights and restrictions
- ▶ Boundaries on those definitions
- ▶ Specification
- ▶ Publication/applicability of specification

Identity Management ecosystem



- ▶ Multiple authorities: resiliency, domains of applicability, different legal bases
- ▶ Multiple providers: Canadian example: TD Bank, Scotia Bank, BMO Financial
- ▶ Multiple business opportunities: decomposition of responsibilities, e.g. NSTIC
 - ▶ Identity Ecosystem Framework: includes transaction participants (2 or more), identity provider, attribute provider
 - ▶ Trust frameworks
 - ▶ Accreditation authorities
 - ▶ Trustmark schemes: framework and level of compliance

Key elements



- ▶ **Representation** of stakeholders in trust: e.g. NSTIC community, USGSA ICAM, USPS FCCX, Telcom Data Trust Framework, Pharma Trust Framework
- ▶ Definition of domain of trust (topic, levels, etc.)
- ▶ Specification of framework: technical, business, legal: one example context is the Kantara Initiative Identity Assurance program
- ▶ Accreditation: service providers and trust element providers, e.g. at Kantara this includes Deloitte, Electrosoft, Europoint, Zyigma
- ▶ Registry: Open Identity Exchange
- ▶ Enforcement: technical, business, legal (contract based)

Multi-dimensionality of framework and multiple frameworks

Applicability to Spectrum WG



- ▶ ASA/LSA/PA propose multiple legitimate users under varying conditions and agreements
- ▶ Based on distributed databases: identifying who can do what under which circumstances
- ▶ Challenges
 - ▶ How to trust identities to verify adherence to the agreements: authentication/authorization
 - ▶ How to trust with respect to privacy
 - ▶ Dynamic definitions of the database capabilities

Looking forward



▶ Trust ecosystem

- ▶ Participants
 - ▶ Stakeholder groups
 - ▶ Framework assistance
 - ▶ Accreditation organizations
 - ▶ Infrastructure, e.g. infrastructure
 - ▶ Trust providers
- ▶ Trust framework specifications

▶ Trust in context

- ▶ External conditions
- ▶ Risk or cost vs. benefits or rewards
- ▶ Can this be formalized?
- ▶ Composition?

Recent Speakers



- ▶ Hannes Tschofenig, IETF Privacy, NSN => ARM, Trust background
- ▶ Don Thibeau, Open Identity Exchange, Trust Framework registry
- ▶ Lori Brennan, Kantara Initiative, Trust Frameworks: specification, accreditation
- ▶ Sibal Adali, Rennsalaer, Trust in Context
- ▶ Scott David, U. Washington, Legal Frameworks for Trust
- ▶ Jean Camp, U. Indiana, User Trust
- ▶ Andre Boysen, SecureKey, Trusted Identity Management
- ▶ Rebecca Nielson, Booz Allen, The Business of Trust