Scope of Identity and Trust Federations

Abstract

Terminology

Identity Management is as core part of Trust Management. The latter extends the former by establishing confidence in data protection, privacy, non-repudiation and availability of identity services.

Problem statement

Electronic communication involving large communities of independent parties requires trust to be negotiated and established in standardized. Moreover, to allow for good scalability, policies and capabilities must be negotiated automatically to a high degree. Except for the case of a single publisher to anonymous clients that problem has not been solved yet in public networks. Identity federations and trust federations are key concepts to address this problem.
Different contributions to this field like EUGridPMA, Kantara IAF, NIST 800-63 and STORK address important parts of the problem domain, but the scope definitions and underlying models lack completeness and clear delineation.

Goal

To support the adoption, scalability and interoperability of Identity Federation frameworks, a more precise and comprehensive model of trust relationships and related requirement is proposed in this document than provided by previous publications. It shall provide a basis to

- define what subset of trust relationships and security objectives are addressed in a particular framework,
- check the completeness of the defined rules,
- sort out assignments of requirements to actors and
- map different frameworks to each other.

Conclusion

I. The scope of documents describing requirements in trust federations should be defined with 2 principles in mind:

a) Use the concept of “liable actors” to select the set of requirements and recommendations that are included;

b) Achieve completeness that all duties of that actor are described in the document.

II. Requirements should be elaborated in a formalized analysis to achieve a clean definition.

Common Principles

Trust management in electronic communication is generally not a business goal, but an auxiliary use case to other business cases. It is now best practice in IT architecture that identity management should go from the application to the infrastructure layer, like proposed in [Cameron-Laws-of-Identity].

Principle #1: Trust Management is not an application, but an infrastructure concern

Systems grow reasonable well as long as capacities scale in a linear fashion. If a network requires pairwise activity to set up legal or technical trust relationships, then a party will be a bottleneck if the capacity to handle additional contracts is exceeded. [Hoerbe-Scalability]
To handle trust relationships, there are 2 common measures:

a) General parts of the agreement are made common, by delegation to an intermediary, legislation or taking out to a standardized, widely accepted framework agreement.
b) Specific parts that cannot be covered in the common parts, are structured in a way that they can be negotiated (mostly) automatically. E.g. assurance levels have a common definition, but are automatically negotiated by matching policies of the Relying Party and that of the IdP for a particular user.

Any pairwise agreement involving human administration is not feasible beyond a certain number of services per client. Applied to the establishment of trust between the partners of a federation, all forms of trust and security agreements need to be interoperable on technical, semantic and legal levels. The structure of these agreements shall support computational contracts.

Principle #2: Negotiation of trust relationships must be automated

What are the properties of a trust relationship in the context of a federation?

- Trust is a subjective assessment by a relying actor of the expected behavior of an liable actor, hence uni-directional[1].
- A legal trust relationship is established when an entity becomes an actor of a federation[2] and assigns defined levels of trust to other actors, because the other actors accepted to fulfill a defined set of duties (requirements), and there are measures to enforce these requirements, like audits or liabilities.
- A technical trust relationship is established based on a legal one based on a common protocol, like cryptographic key exchange, and fulfills a legal requirement.

Principle #3: Trust in federations is based on the legal duties of the actors

The consequence from these three principles is: Trust management must be highly standardized and structured. Requirements must be assigned to actors.

[1] “Mutual trust” is an aggregation of separate trust relationships, which are not necessarily symmetric.

[2] By contract or law

Structuring Requirements

The complete set of requirements for a trust federation is too complex for a single document. A particular framework might need only a subset, depending on requirements and use cases. Therefore modularization and proper delineation is applicable to divide the topic in smaller units.

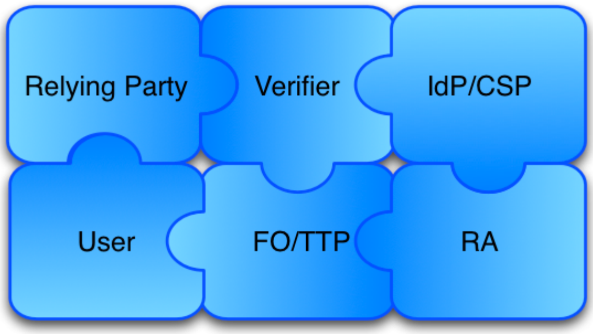
There are several possible viewpoints to structure requirements:

a) liable actor (i)	pro: unambiguous; structured by primary audience; 1:1 fit to legal duties and assessment criteria per actor
b) phases (ii)	con: each module would contain requirements for different actors; delineation not clear[3]; formally unclean as static requirements are related to a time-depended category, e.g. credential issuance and in-person verification relate to different phases but coincide in a single transaction.
c) relying actor (i)	pro: similar to a) con: requirements should primarily be written for those who implement them
d) security objective (iii)	pro: this would address the different domain experts, like privacy, authentication and ISO 27002 con: each module would contain requirements for different actors; delineation unclear
e) actor centricity (iv)	pro: as the term “Relying Party” already implies, the complete set of requirements in the service provider centric scenario could be wrapped up. con: There is not clear distinction between these models.

(i) like IdP, RP, subject, subscriber, registration officer, auditor, federation operator
(ii) like identity proofing and authentication phase
(iii) like confidentiality, authenticity, privacy, non-repudiation
(iv) service provider centric model or user-centric model See [KI-FIWG], C20 - C22

The delineation of modules by liable actor (option a) seems to be the best compromise for its unambiguity and structure.

> Recommendation: Modules compromising parts of a trust framework should set their scope to cover the duties of each actor.



Sample modularization of a trust framework by liable actor.

Acronyms: IdP and CSP are synonymous, the TTP (Trusted Third Party) is a subset of the FO Federation Operator), RA is the Registration Autothority.

[3] e.g. obliging the end user to handle particular token type with a certain rigor applies to both registration phase and the token which is part of the authentication phase.

Requirement Model

Separation of requirements and controls

Using the general structure of requirements per liable actor, the analysis of requirements should sort out controls[4] from requirements as much as possible. Some controls serve as a convenient shortcut, like requiring a certain process to prove an applicant's identity.

Isolating requirements

If several requirements a merged into a process description a lot of flexibility is lost. Mapping different frameworks becomes cumbersome. Therefore requirements should be separated to a reasonable extent. E.g.:

Amalgam of requirements	*Segregation of requirements*
Possession of a valid current primary Government Picture ID	Possession of a valid current primary Government Picture ID
Inspect photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Physical verification of Government Picture ID to detect falsifications
	Verification if picture of ID matches applicant
	Record ID number and address
	Verify address (either via address of record or delivery of the credential to the address)

References

[Cameron-Laws-of-Identity] Kim Cameron, The Laws of identity, 2006
http://www.identityblog.com/?p=352

[Hoerbe-Scalability]. Rainer Hörbe, Trust relationships and scalability, 2010
http://identityblog.portalverbund.at/en/node/16

[KI-FIWG] Kantara Initiative/FI-WG: Identity Federation Constellations and Use Case Overview, Nov. 2010 [work in progress]
http://kantarainitiative.org/confluence/x/8oh7Ag

[4] Controls is ISO 27000 terminology, synonymous to safeguards or security measures