Virtualization of the Circle of Trust amongst Identity Federations

Latifa Boursas

Munich Network Management Team
Munich University of Technology
boursas@tum.de,
http://www.mnm-team.org/~boursas/

Abstract. This paper explores the concepts that enable a more dynamic setup and building of a *Circle of Trust (CoT)* amongst multiple and overlapped federations. It examines virtualization-building and driving trends, discusses some models of deployment of the CoT and shines a light on the work of the Liberty Alliance Project as a basis for an extended solution for enlarging dynamically the CoT with new entities. Other challenges of this research rely on the administration of the CoT as well as the life cycle of the participants, which imposes an inherent limit on how new Identity and Service Providers can be added to the CoT and how trust relationships can be established between them.

1 Introduction

Trust and security are key enablers of today's large distributed systems such as economic environment. For users to share and feel comfortable with e-commerce and e-business services they must have confidence that their online services are trustworthy and secure. Similarly for businesses and governments the need has grown to safely share sensitive information amongst different levels and each other and for balancing safety with accessibility. Federated Identity Management (*FIM*) techniques attempt to solve the balancing problem through successful authentication and authorization. FIM makes it possible for an authenticated identity, at his account partner organization, known as an Identity Provider *IDP*, to be recognized and take part in personalized services, collected in resource partner organization, known as Service Provider *SP*, across multiple domains. The users within their IDPs, which are called service requesters, are not identified only by unique names but also depend upon their attributes (usually substantiated by certificates) in order to gain accesses to the resources as it is known in Attribute Based Access Control ABAC [9].

Known industrial FIM standards, such as the OASIS Security Assertion Markup Language (*SAML*) [4] and Web Services Federation Language (*WSFL*) [1] often enhance privacy and trust aspects quite statically by means of SAML assertions, XML signatures and digital signed certificates in form of tokens for reliable authentication within a federation of Service Providers, usually linked together by business and contract relationships. Beyond those technical aspects, the federated identity vision in the Liberty Alliance Project [8] can also be articulated through the important concept of a *Circle of Trust CoT*, which is defined as a group of service providers SPs (based on Liberty enabled technology) that share linked identities at a single Identity Provider IDP and have pertinent business agreements in place, regarding how to do business and interact with identities in a secure and apparently seamless environment. Once a user has been authenticated by a Circle of Trust IDP, that individual can be easily recognized and

transact business and consequently take part in targeted services from other SPs within the CoT [7].

Usually once such a CoT has been created, doors are opened to formal and across-the-board trust relationships. The problem then occurs, when for instance the user disclaims providing his information or might not be willing to entrust certain personal data to a certain online service just because it is a member in the CoT. In previous work [2] we have shown how to effectively control and implement such a practice, by integrating the aspects of *Reputation Management* of tracking an entity's behaviors within the federation and other entities' opinions about those behaviors. Then again, we have shown, using a trust level algorithm, that the rating aspects significantly increase both IDPs' and SPs' trustworthiness, and furthermore involve dynamically end users and SPs on deciding how sensitive data can be shared and released. Because negative reputation may work as a sanctioning mechanism to punish dishonest behaviour by participants in the CoT.

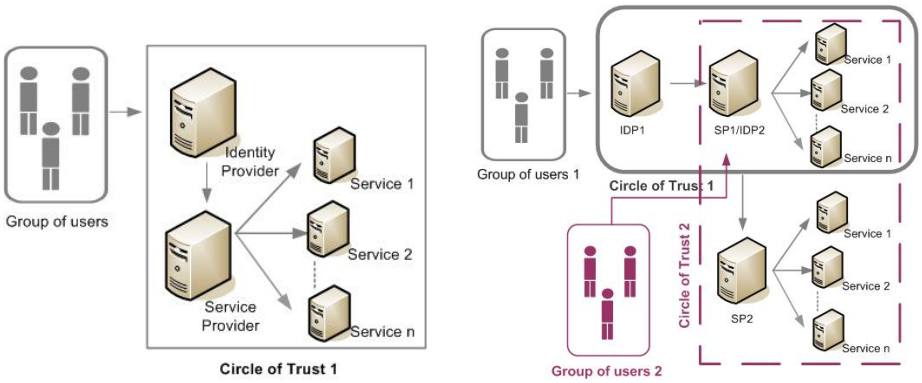
In this contribution, we want to address the problem of trust management beyond the borders of the CoT and analyse to what extend can the CoT be enlarged with new organizations, where a single organization may be both an IDP and a SP, either generally or for a given interaction. In this context, the ability to dynamically design the CoT and subsequently enforce virtual interpolation aspects driven by various levels of inter-organisational trust is very new and constitutes our research. We investigate particularly how additional IDPs can be dynamically concatenated to the original IDP, which has created a CoT among its affinity group of SPs, and how effectively new trust relationships can be established between all parties newly involved.

The paper is organized as follows, section 2 first presents an abstract scenario that summarizes the requirements for dynamic management and expansion of the CoT with new organizations; section 3 provides a discussion for designing such a CoT and considers some broader structural issues of virtualizing the CoT; Section 4 gives a short insight in some organizational models that deal with the same part of the problem and finally summarizes and concludes the paper.

2 Scenario

From a FIM perspective, the distinguished actors are the users (known as principals), SPs, and IDPs. The SP is the organization offering Web-based services to the principals, and the IDP is the authoritative source organization for issuing, managing and validating principals identities so that other SPs can affiliate with them. Establishing such relationships creates the CoT shown in Fig1.a, which refers to the contractual relationship (or federation) formed between the IDP and the SP. In this scenario, when the principals are considered to be authenticated, the IDP will notify its eligible principals of the possibility of federating their local identities among the members of the affinity group of the SP and will solicit permission to facilitate the introduction of the principal to the members of the affinity group within the CoT. Soliciting the principal's consent to his identity federation is usually handled via Attribute Release Policies (ARPs) that are used to control this flow of personal data, e.g. for SAML conformance, various implementations exist [3].

In other scenarios, it happens quite often that the SP itself acts as an IDP in other CoT contexts. Therefore the scenario, presented in Fig1.b, envisions that the SP1 from the CoT2 will authenticate the principals from the *Group of users 2*, prior to providing services to this group of principals. By this overlapping of the two CoTs, the principals



a. Standard Circle of Trust b. Overlapped CoTs

Fig. 1. Representation of the Circle of Trust

from the CoT1 may try to sign on with a member of a federated group of CoT2. Hence, it is important to investigate, whether it is possible to extend the first CoT1 over the second one in order to comply with the principal's request from the *Group of users 1* to access the resources in the CoT2. By taking profit of the prospective virtual CoT, these principals will not have to reauthenticate at the CoT2, because the SP1 vouches that they are entitled to access the resources of the CoT2, and accordingly the SP2 trusts the CoT1 regarding this assertion.

Various requirements for the technical design of the joined CoT arise from this scenario:

- The first part of coupling the CoTs investigates relationships between and within an organization to create a scope for the virtual CoT that should also be driven from business objectives.
- Requirements on the type of information that will be shared among the organizations, how and when it will be shared and possibly how it will be treated are also of a big relevance.
- Requirements on the security procedures that have to be additionally used to maintain the confidentiality of such information as well as the level of confidentiality and trust that should be imposed on the participants. A fitting research direction for this issue, as we demonstrated in [2], is the enhancement of the so-called trust acquaintance graph that is based on trust level algorithms, where static and local CoTs can also be represented as nodes in the graph. The edges that connect them define the trust relationships between them.
- Requirements on the organizational rules and policies, for example on the manner participants may join or leave the CoT and how the CoT will be administered.

The fulfilment of those requirements on the life cycle establishment of the virtual CoT can be then broken down into three general phases: *design*, *deployment* and *maintenance*.

3 Our approach for the CoT Life Cycle

In this short contribution, we mainly focus on the *design phase*, during which data about the whole environment and data sources, principals groups and the federation-enabled application have to be collected. This phase is aimed at designing the virtual joined CoT dynamically through the following areas:

- *Directory Design*, we intend to design the CoT in an LDAP structure [5] as a hierarchal tree. This tree contains classifications to denote federation object's positions within a hierarchy. As can be seen in Fig 2, at the top of an tree a root must be designed as the virtual CoT, which by means of the children nodes may be continuously extended. Each federation may branch consequently to organizational units which are represented by the local static CoT of each federation. Those organizational units may contain other organizational units that can be defined as IDPs and SPs, where groups of users, services and other relevant entities may be chained together at the same level of the sub-tree.

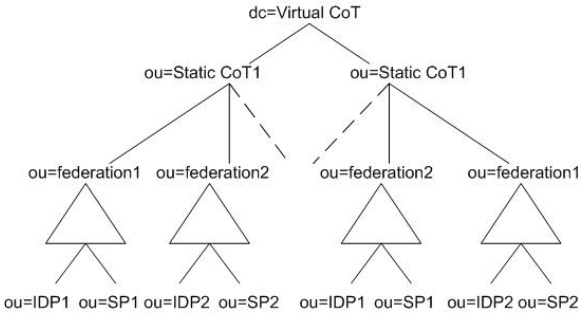


Fig. 2. CoT directory design

- *CoT Membership Data*, chances are good when information about previous relationships inside the organization can be stored, because cataloguing these information relationships, identifying their owners, and establishing an ongoing relationship may prove useful. For example, on the basis of the previous scenario, the principal has to specify which IDP outside the local CoT has authenticated him. Trust and reputation algorithms as well as rating mechanisms can be applied to build an opinion about the new IDP and if the trust requirements of both parties converge, an instance of the object may consequently be moved to the corresponding federation in the tree. According to the estimated trust value ACL placements in the branch have to be revised as well.
- *Namespace*, after determining what data has to be put in the directory, the way to recognize and to reference this data still has to be defined. To find federation objects within a hierarchy queries of a certain format with a string of (key, value) pairs must be issued.
- *Data Schema*, the different federations may have different requirements concerning the data contained in the Directory Tree, its format, and how the data is interpreted. Therefore constraints on the size, range and format of data values shared between the federations have to be treated with an adequate care.

4 Related Works and Conclusions

In addition to the FIM standards, mentioned in section 1, there are a number of initiatives in this direction to simplify challenges of achieving trust in multi-domain collaborative environments. Liberty Alliance Project [6] is one of the few industrial solutions that have developed specifications and guidelines to help businesses, governments, and individuals establish a legally binding CoT, which has legally enforceable contractual forms between the parties implementing the Liberty specifications. Liberty has specified three static approaches to the contractual framework, called *Organizational Models*: Collaborative Model, Consortium Model and Centralized Model. A similar approach is found in the *FIXS* Project [10] that conveys an initial trust to all the participating members. Formally, direct relationships between the participants are established through acknowledgment and agreement to the 'Terms of Use', thus enabling distributed and trusted authentication. Many existing other approaches to trust management in virtual communities, such as [11], require a centralized architecture and thus do not fit well in the distributed nature of the Internet.

In our work we explored more dynamic trust negotiation by means of the virtual CoT, which makes it possible for a new trusted entity to be recognized and take part in personalized services dynamically across the virtual CoT. Our Directory design avoids pitfalls of centralized and redundant storage of personal information, while allowing federations to link identity information between different tree levels and branches. In future work, we plan to analyse the *design* phase of the virtual CoT by means of the *deployment* and *maintenance* phases, associated with a prototype implementation showing the benefits and limitations in supporting n-tier delegation of trust relationships in multi-domain federations.

References

1. S. Bajaj, G. Della-Libera, Brendan Dixon, and M. Dusche: Web Services Federation Language (WS Federation) Version 1.0. (2003)
2. L. Boursas and H. Reiser: Propagating Trust and Privacy Aspects in Federated Identity Management Scenarios. In Proceedings of the 14th Annual Workshop of HP Software University Association. Munich, Germany (2007)
3. S. Cantor: Shibboleth v1.2 Attribute Release Policies. http://shibboleth.internet2.edu/guides/deploy-guide-origin1.2.html (2004)
4. S. Cantor, J. Kemp, R. Philpott, and E. Maler (Eds.): Assertions and Protocols for the Security Assertion Markup Language (SAML) V2.0. OASIS Security Services Technical Committee Standard. (2005)
5. T. Howes, M. Smith and G. Good: Understanding and deploying LDAP Directory Services. Second Edition Addison-Wesley (2005)
6. Victoria Sheckler, Hogan and Hartson (Ed.): Liberty Alliance Contractual Framework Outline for Circles of Trust. Liberty Alliance Specification (2005)
7. Christine Varney and Hogan and Hartson (Ed.): Liberty Alliance Privacy and Security Best Practices v. 2.0. Liberty Alliance Specification (2005) ■
8. T. Wason: Liberty ID-FF Architecture Overview v1.2. Liberty Alliance Specification (2003)
9. E. Yuan and J. Tong: Attributed based access control (ABAC) for Web services 2005 IEEE International Conference on Web Services (2005).
10. The Federation for Identity and Cross-Credentialing System (FIXS) Trust Model. FIXS Specifications (2007) http://www.fixs.org/
11. A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities Conference on System Sciences 33, Maui, Hawaii, January 2000.