Mathematical Modelling of Trust Issues in Federated Identity Management

Md. Ferdous, Gethin Norman, Audun Jøsang, Ron Poet

Mathematical Modelling of Trust Issues in Federated Identity Management

Md. Sadek Ferdous[1], Gethin Norman[1], Audun Jøsang[2] and Ron Poet[1]

[1] School of Computing Science, University of Glasgow, Glasgow, G12 8QQ, Scotland
[2] Department of Informatics, University of Oslo, Oslo, 0316, Norway
{sadek.ferdous,gethin.norman,ron.poet}@glasgow.ac.uk, josang@mn.uio.no

Abstract. With the absence of physical evidence, the concept of trust plays a crucial role in the proliferation and popularisation of online services. In fact, trust is the inherent quality that binds together all involved entities and provides the underlying confidence that allows them to interact in an online setting. The concept of Federated Identity Management (FIM) has been introduced with the aim of allowing users to access online services in a secure and privacy-friendly way and has gained considerable popularities in recent years. Being a technology targeted for online services, FIM is also bound by a set of trust requirements. Even though there have been numerous studies on the mathematical representation, modelling and analysis of trust issues in online services, a comprehensive study focusing on the mathematical modelling and analysis of trust issues in FIM is still absent. In this paper we aim to address this issue by presenting a mathematical framework to model trust issues in FIM. We show how our framework can help to represent complex trust issues in a convenient way and how it can be used to analyse and calculate trust among different entities qualitatively as well as quantitatively.

Keywords: Trust, Federated Identity Management, Mathematical Modelling.

1 Introduction

Unlike the brick and mortar world, the physical evidence and visual cues that can be used to establish trust and gain confidence are largely absent in online services. Despite this, the popularity of online services has grown exponentially in the last decade or so. The concept of trust played a crucial role in popularising online services. In fact, trust is the inherent quality that binds together all involved entities and provides the underlying confidence that allows them to interact in an online service. The mathematical modelling and analysis of different trust requirements in online services are abound and is a well established research area. Such a model helps to express and to reason with trust issues in a formal way which can ultimately help to create novel ways for determining trust among involved entities.

The concept of Federated Identity Management (FIM) has been introduced to ease the burden of managing different online identities and to allow users to access online services in a secure and privacy-friendly way [1]. FIM offers

an array of advantages to different stakeholders and has gained considerable popularities in recent years. Being a technology targeted for the online setting, FIM is also bound by a set of trust requirements. Surprisingly, the mathematical representation, modelling and analysis of different trust requirements of FIM have received little attention so far. The aim of this paper is to fill this gap.

Here, we present a comprehensive mathematical framework considering different trust aspects targeted for FIM. In doing so, we show how our framework can formally express trust in FIM and how such expressions can be used to analyse and evaluate trust qualitatively and quantitatively. The main contributions of the paper are:

1. Inspired by the notation of trust presented in [14], we present a notation to express trust between different entities in FIM.
2. We use this notation to develop the first mathematical framework to model, analyse and derive trust in different types of identity federations.
3. We explore trust transformations resulting from interactions in FIM.
4. Finally, we present a simple method to evaluate trust quantitatively in FIM.

The paper is structured as follows. Section 2 provides a brief introduction to FIM and the required trust issues in this setting. Section 3 introduces the notation and the interaction model that will be used in our framework. The trust issues in different types of identity federations are modelled in Sections 4 and 5. We show how trust transformations occur within different federations using our framework in Section 6 and how trust can be calculated quantitatively in Section 7. Section 8 discusses the related work and finally Section 9 concludes the paper.

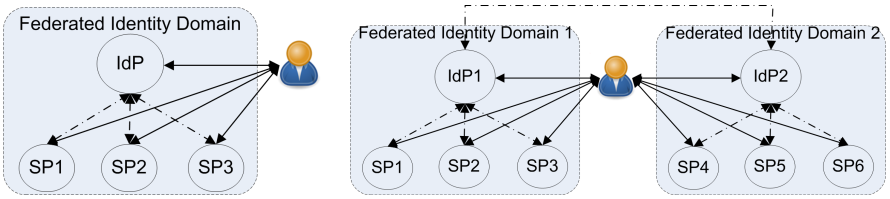
2 Background

In this section, we provide a brief introduction to FIM, to different aspects of trust in general and to trust issues in FIM specifically.

Federated Identity Management. Identity Management consists of technologies and policies for representing and recognising entities using digital identifiers within a specific context [7]. A system that is used for managing the identity of users is called an Identity Management System (IMS). Each IMS includes the following types of parties: **Service Providers (SPs)** or **Relying Parties (RPs)** - entities that provides services to users or other SPs, **Identity Providers (IdPs)** - entities that provides identities to users to enable them to receive services from SPs and **Clients/Users** - entities that receive services from SPs. Among different IMS, the Federated Identity Management (FIM) has gained much attention and popularity.

The Federated Identity Management is based on the concept of Identity Federation. A federation with respect to Identity Management is a business model in which a group of two or more trusted parties legally bind themselves with a business and technical contract [1,17]. It allows a user to access restricted resources seamlessly and securely from other partners residing in different Identity Domains. An identity domain is the virtual boundary, context or environment in which an identity of a user is valid [17]. Single Sign On (SSO) is the capability that allows users to login to one system and then access other related

but autonomous systems without further logins. It alleviates the need to login every time a user needs to access those related systems. A good example is the Google Single Sign On service which allows users to login a Google service, e.g., Gmail, and then allows them to access other Google services such as Calendar, Documents, YouTube, Blogs and so on.



(a) Type 1. (b) Type 2.

Fig. 1. Federated Identity Domain.

A federated identity domain can be formed by one IdP in an identity domain and a number of SPs with each SP residing in a separate identity domain (Type 1 in Figure 1(a)). Several federated identity domains can be combined to form a larger federated identity domain where each smaller federated domain is of Type 1 (Type 2 in Figure 1(b)). A Type 2 federation allows an IdP of a Type 1 federation to delegate the authentication task to another IdP in a different Type 1 federation. To enable this, both IdPs need to act as both IdPs and SPs. The issue of trust is a fundamental concept in FIM as different autonomous bodies need to trust each other inside the federation. Such parties inside a federation are said to form the so-called Circle of Trust (CoT).

A federation can be of two types depending on how it is created. The traditional federation, also called a *Static Federation*, is where the federation is created at the admin level and is bound with a legal contract using a specified set of administrative procedures. On the other hand, in a *Dynamic Federation* any user, not only administrators, can create the federation in a dynamic fashion without administrative intervention or a legally binding contract [3].

Trust. The concept of trust and trust management in the setting of online services is a widely studied topic and has been defined in numerous ways. For the purpose of this paper, we use the following definition taken from [11] which was originally inspired by [13].

"*Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible.*"

The definition gives a directional relationship between two entities: the first is regarded as the *Trustor* and the second the *Trustee*. The trustor and trustee can be any entity, however, in the scope of this paper, only those involved in FIM will be considered (i.e. users, IdPs and SPs). The pairwise trust relations we consider are user-IdP, user-SP, IdP-SP and IdP-IdP which is inline with current IMS setting and the relationships that occur inside a federation.

Trust can be of two types: Direct Trust (DT) and Indirect Trust (IT) [12]. Direct trust signifies that there exists a trust relationship between the entities based on first hand experience and evidence. On the other hand, indirect trust, also known as Transitive Trust, is a trust relationship between two entities based on referral from one or more intermediate third parties.

Every trust relationship has a scope that signifies the specific purpose or context into which that trust relationship is valid. The trust strength (also known as the trust degree) signifies the level of trust a trustor has over a trustee [14]. The type and value used to define the level of trust will vary depending on the trust scopes as well. Trust can be defined as *Mutual Trust* only if there is a bi-directional trust relationship with the same trust type, scope and strength between the corresponding entities. In such case, both entities can act as the trustor and the trustee. Trust often exhibits the transitivity property [11]: if an entity A trusts another entity B and B trust another entity C, a trust relation can be derived between A and C. To derive such a transitive trust relation, the trust scope must be same. The trust transformation is the process when a trust relationship between two entities changes due to the change of trust strength while the trust type remains the same. Such a transformation occurs normally for two reasons: i) when the trust is derived following the transitivity property and ii) when one entity interacts with another entity to perform a certain action which ultimately triggers the change in the trust strength. The transformation can be positive, meaning the new trust strength is higher than what was before, or can be negative, meaning the new trust strength is lower than what was before.

A trust with a single scope can be defined as atomic trust. Compound trust can be defined as the combined trust of several different atomic trusts where the trustor, trustee and the trust direction and strength between them remain the same. The compound trust will also have the same trust direction and strength.

Trust Issues in Identity Management. The issue of trust is a fundamental concept in FIM as different participating organisations need to trust each other inside the federation at a sufficient level to allow them to exchange and trust user information. We will consider such trust issues using two separate instances.

The first, called *High Level* trust, is the abstract level of trust that is assumed between federated entities (IdPs and SPs) in a federation. This level of trust is common in the existing literature on FIM. For example, it is common to express that two entities trust each other if they belong to the same CoT. In such an expression, the trust is treated at an abstract level and is used mostly to signify their architectural relation inside a federation.

The second, called *Fine-grained* trust, is a detailed expression of trust including the scope between entities (including users) in a federation. The expression may (optionally) include a trust type or strength. Inspired by the requirements outlined in [8,12], the authors in [2] have outlined a set of fine-grained trust requirements in the traditional federation which are applicable for both Type 1 and Type 2 federations. We will use their requirements to represent fine-grained trusts in Section 4.

Trust in a dynamic federation is modelled using three classes of entities [3]: **Fully Trusted** entities are IdPs and SPs in the traditional SAML (Security Assertion Markup Language) federation which have a legal contract between them [18]; **Semi-trusted** entities are SPs in a dynamic federation that have been added dynamically to an IdP inside the federation under **some conditions** without a contract and to whom any user of the IdP has agreed to release a subset of her attributes and **Untrusted** entities are IdPs and SPs in a dynamic federation which have been added dynamically under **some conditions** without a contract. A detailed discussion of these classes can be found in [3].

3 Notation

In this section we will introduce the notation that will be used to build up the model. We use E to denote the set of entities, with U the set of users, SP the set of service providers and IDP the set of identity providers. Since each user, SP and IdP is also an entity, we have $E = U \cup IDP \cup SP$. In addition, $\mathcal{F}$ denotes the set of federations and will use subscript from $\mathcal{F}$ to define the contexts of entities (i.e. the federation in which they belong). For example, E_f will be used to denote the sets of entities in a federation f. We use T to denote the set of trust types. As explained above, we consider two types of trust: direct trust (denoted by DT) and indirect trust (denoted by IT). Therefore, $T = \{DT, IT\}$.

We use S for the set of trust scopes. Different trust scopes can be defined depending on the trust requirements. We consider the following trust scopes for FIM based on the fine-grained trust requirements of [2]:

- REG is trust in the implementation of the registration process;
- STO is trust in secure attribute storage;
- $AUTHN$ is trust in the implementation of the authentication mechanism;
- AP is trust in allowing the use of anonymous or pseudonymous identifiers;
- $CONSENT$ is trust in the release of only those attributes consented to;
- ABU is the trust that an entity will not abuse attributes released to it;
- $CARE$ is the trust an entity handles her attributes with adequate care;
- HON is the trust that an entity provides attribute values honestly;
- $ACDA$ is the trust that an entity adheres to the agreed policies and procedures during access control and delegated access;
- SRV is the trust in service provisioning;
- $MIN\text{-}ATT$ is the trust that an entity requests only minimal attributes;
- REL is the trust in an entity correctly releasing attributes;
- ND is the trust in an entity adhering to the non-disclosure of attributes;
- FED is trust between federated entities.

We consider the following types of trust strengths in FIM.

Subjective Trust. This defines the subjective trust a user may have in IdPs and SPs in a federation and will be denoted with $conf$. It can have different levels, however, we have opted for three levels: *LOW (L), MED (M), HIGH (H).*

Level of Assurance (LoA). This defines the trust strength between federated IdPs and SPs and is used during service provisioning. It is based on the NIST

LoA guidance of 1 to 4 where Level 1 can be used to model the lowest trust and Level 4 the highest [15]. It will be denoted as *loa* with values from 1 to 4.

Federation Trust. The last type concerns the trust strength between federated IdPs and SPs with respect to their architectural relations. It is denoted with *fed-trust* and can take four different values: *UNTRUSTED (UT)*, *SEMI-TRUSTED (ST)*, *RESTRICTED-TRUSTED (RT)* and *FULLY-TRUSTED (FT)*. The lowest trust strength UT means a trustor does not trust a trustee at all and is associated between entities federated in a dynamic fashion or between entities in a transitive trust in static federations (see below). The strength ST means a trustor trusts a trustee upto a certain level. An example is the trust strength between a dynamically federated IdP and an SP and the fact that the IdP may not want release sensitive attributes to the SP as there are no formal agreement between them. The strength RT is higher than ST, but lower than FT. Such a strength is exhibited when the trust relationship between a trustor and trustee is derived using transitivity and the trustor may not fully trust the trustee as there are no formal agreements between them. The strength FT signifies the highest strength and is exhibited when the trustor and trustee are part of a traditional federation. The federation trust strengths are ranked:

$$UT < ST < RT < FT\,.$$

To indicate an entity $e_1 \in E_f$ (the trustor) has $t \in T$ trust over an entity $e_2 \in E_f$ (the trustee) in a federation $f \in \mathcal{F}$ with a trust scope of $s \in S$ and the trust strength of v, we will use the following notation, inspired by [14]:

$$e_1 \xrightarrow[v]{t\,:\,s} e_2$$

where v represents the trust strength (either *conf*, *loa* or *fed-trust*). To express the same trust t between two entities e_1 and e_2 with same trust strength v in a number of different scopes, $s_1, \ldots, s_n$, we extend the notation to:

$$e_1 \xrightarrow[v]{t\,:\,\{s_1,\ldots,s_n\}} e_2$$

If there exists a mutual trust (t) between two entities in the same trust scope(s) with the same trust strength (v), we use the notation:

$$e_1 \xleftrightarrow[v]{t\,:\,s} e_2$$

3.1 Interaction Model

To enable a protocol flow in a federation, each entity interacts with another entity in order to perform an action at another entity. A user interacting with an IdP to authenticate herself by providing an identifier (e.g. username) and a credential (e.g. password) is example of an interaction. Interaction between entities to perform an action can cause the trust between the involved entities to transform. The interaction model consists of the actions that an entity can perform at another entity in a federation. Such interactions must be carried out

using a communication channel. We will use the notation *CHANNEL* to define the set of channels. Two types of channels will be considered: secure channels, denoted SC, model secure HTTPS connections whereas unsecured channels, denoted UC, model unsecured HTTP connections.

To denote an interaction that represents an entity e_1 performs action a at entity e_2 using communication channel c, we will use the following notation: $c(e_1 \overset{a}{\rightsquigarrow} e_2)$. There could be many interactions in a federation, however, to the scope of this paper, we restrict attention to the following interactions:

- $c(u \overset{RG}{\rightsquigarrow} idp)$ representing user u registering at IdP idp through channel c;
- $c(u \overset{A}{\rightsquigarrow} idp)$ representing user u authenticating herself at IdP idp through channel c;
- $c(idp \overset{AP}{\rightsquigarrow} u)$ representing IdP idp allowing user u to use anonymous or pseudonymous identifiers through channel c;
- $c(idp \overset{C}{\rightsquigarrow} u)$ representing IdP idp providing user u with the opportunity to provide consent for releasing selected attributes through channel c;
- $c(idp \overset{RL}{\rightsquigarrow} sp)$ representing IdP idp releasing user u's selected attributes to the SP sp through channel c.

4 Trust Modelling in Traditional (Static) Federations

In this section, we model trust between different entities in traditional federations. We will consider first high level trust and then fine-grained trust.

4.1 High Level Trust Modelling

We can express the high level trust in a Type 1 federation $f \in \mathcal{F}$ between an IdP $idp \in IDP_f$ and an SP $sp \in SP_f$ by:

$$idp \xleftarrow{\frac{DT:FED}{FT}} sp$$

This signifies that idp and sp have a mutual direct trust in the scope of the federation. Since it is a Type 1 federation, the entities trust each other fully, hence the trust strength is fully trusted (FT).

Let us now consider a Type 2 Federation consisting of two Type 1 federations, say $f_1, f_2 \in \mathcal{F}$. Since f_1 and f_2 are Type 1 federations, we have for $i \in \{1, 2\}$, $idp_i \in IDP_{f_i}$ and $sp_i \in SP_{f_i}$:

$$idp_i \xleftarrow{\frac{DT:FED}{FT}} sp_i$$

Trust between an IdP $idp_1 \in f_1$ and an IdP $idp_2 \in f_2$ deserves further attention. Since they are in a Type 2 federation, these IdPs will act as both IdPs and SPs depending on the use-cases. Without specifying which entity acts as what, we can model the underlying trust relations between these IdPs as follows:

$$idp_1 \xleftarrow{\frac{DT:FED}{FT}} idp_2$$

Next we model the trust transitivity property of [11] by introducing the following rules to derive a transitive trust between entities in a Type 2 Federation.

Rule 1 (Trust Type in a Transitive Trust.) *A derived transitive trust between entities in a traditional Type 2 Federation must be of indirect trust type.*

Rule 2 (Trust Strength in a Transitive Trust.) *The strength of the derived trust is that immediately below the lowest value of the intermediate trusts except when no such value exists, in which case the strength will be the lowest value.*

The trust type between the entities changes in a transitive trust since they are not directly connected with each other. Changes in the trust strength between entities in a transitive trust is because there need not exist a formal agreement between the entities, and hence the rule ensures that the derived level of trust is the lowest among (or lower than) any intermediate trust levels in the transitive path. The rule also includes a limiting condition to ensure that the trust strength does not reduce to an undetermined value as it is reduced along a transitive path of trust.

Next, let us consider a Type 2 Federation consisting of two Type 1 federations $f_1, f_2 \in \mathcal{F}$. For $sp_1 \in SP_{f_1}$, $idp_1 \in IDP_{f_1}$ and $idp_2 \in IDP_{f_2}$ the transitive trust between sp_1 and idp_2 can be derived using Rule 1 and Rule 2 as follows:

$$\frac{\left[sp_1 \xleftarrow[FT]{DT:FED} idp_1\right] \qquad \left[idp_1 \xleftarrow[FT]{DT\ :\ FED} idp_2\right]}{\left[sp_1 \xleftarrow[RT]{IT\ :\ FED} idp_2\right]}$$

We can use these rules to derive trust between any number of entities in a Type 2 federation. For example, consider three federations $f_1, f_2, f_3 \in \mathcal{F}$ with three different IdPs $idp_1 \in IDP_{f_1}$, $idp_2 \in IDP_{f_2}$ and $idp_3 \in IDP_{f_1}$. Furthermore, suppose there is a Type 2 federation between f_1 and f_2 and another between f_2 and f_3, and hence both idp_1 and idp_2, and idp_2 and idp_3 are directly connected. For an SP sp_1 in federation f_1 we can derive the trust relations between sp_1 and idp_3 using Rule 1 and Rule 2 and the following proof tree:

$$\frac{\dfrac{\left[sp_1 \xleftarrow[FT]{DT:FED} idp_1\right] \qquad \left[idp_1 \xleftarrow[FT]{DT:FED} idp_2\right]}{\left[sp_1 \xleftarrow[RT]{IT:FED} idp_2\right]} \qquad \left[idp_2 \xleftarrow[FT]{DT:FED} idp_3\right]}{\left[sp_1 \xleftarrow[ST]{IT:FED} idp_3\right]}$$

4.2 Fine-grained Trust Modelling

Now, we model fine-grained trust for a Type-1 Federation as outlined in [2]. In the following scenarios, each trust will include a strength *conf* or level of assurance *loa* in a Type 1 federation $f \in \mathcal{F}$ between a user $u \in U_f$, IdP $idp \in IDP_f$ or SP $sp \in SP_f$. The trust strength *conf* is assumed when one of the entities is a user and *loa* when the trust is between an IdP and SP.

User Trust in the IdP.

T1. The user trusts that the IdP has correctly implemented user registration procedures and authentication mechanisms (denoted *T2* in [8]):

$$u \xrightarrow[conf]{DT\ :\ \{REG,AUTHN\}} idp$$

Note the direction between the said entities. Since it is not a mutual trust, the direction of trust is from the user to the IdP. Also, as there are two trust scopes (registration and authentication).

T2. The user trusts that the IdP allows the user to utilise anonymous or pseudonymous identifiers (denoted *T1* in [8]):

$$u \xrightarrow[conf]{DT\ :\ AP} idp$$

T3. The user trusts that the IdP will release only those attributes to the SP that the user has consented to:

$$u \xrightarrow[conf]{DT\ :\ CONSENT} idp$$

T2 and **T3** can be combined to denote the user trusting the IdP to protect the privacy of the user through the following rule for compound trust of privacy.

Rule 3 (Compound Trust of Privacy.) *A compound trust of Privacy (PRIV) is a user's trust in the IdP to preserve its privacy to an SP using anonymous or pseudonymous identifiers (**T2**) and trust in allowing the user to choose and provide consent regarding the attributes that it wants to release to the SP (**T3**). Formally we have:*

$$\frac{\left[u \xrightarrow[conf]{DT\ :\ AP} idp\right] \qquad \left[u \xrightarrow[conf]{DT\ :\ CONSENT} idp\right]}{\left[u \xrightarrow[conf]{DT\ :\ PRIV} idp\right]}$$

As mentioned earlier, the trust direction and strength must be same in **T2** and **T3** and the compound trust will inherit these values.

T4. The user trusts that the IdP has satisfactory mechanisms to store user attributes safely and securely:

$$u \xrightarrow[conf]{DT\ :\ STO} idp$$

User Trust in the SP.

T5. The user trusts that the SP will ask only for the minimum number of user attributes that are required to access any of its services:

$$u \xrightarrow[conf]{DT\ :\ MIN\text{-}ATT} sp$$

T6. The user trusts that the SP will not abuse the released user attributes and will use them only for the stated purpose(s):

$$u \xrightarrow[conf]{DT\ :\ ABU} sp$$

IdP and SP Trust in the User.

T7. The IdP trusts that the user handles their authentication credentials with adequate care (denoted as *T3* in [8]):

$$idp \xrightarrow[conf]{DT\ :\ CARE} u$$

T8. The SP trusts that the user is honest while providing attributes to an IdP:

$$sp \xrightarrow[conf]{DT\ :\ HON} u$$

IdP Trust in the SP:

T9. The IdP trusts that the SP adheres to the agreed privacy policies regarding non-disclosure of user data (denoted as *IdP-T.1* in [12]):

$$idp \xrightarrow[conf]{DT\ :\ \{ND,ABU\}} sp$$

In other words, the SP will not abuse the released user attributes and will use them only for the stated purpose(s). The policy might include that the SP will not cache any user-attributes other than those which are absolutely necessary. This is to ensure that the IdP can always provide the updated attributes regarding the user. In cases where the SP needs to cache any attributes (e.g. IdP-supplied identifiers), the SP must inform the IdP.

T10. The IdP trusts that the SP adheres to the agreed policies and procedures, if they are available regarding access control and delegated access:

$$idp \xrightarrow[conf]{DT\ :\ ACDA} sp$$

If there are no such policies or procedures, this requirement is ignored.

Like Rule 3, we can combine **T9** and **T10** to define a compound trust through the following rule.

Rule 4 (Compound Trust of Policy.) *A compound trust of Policy, denoted as POL, is an IdP trust in a SP adhering to the non-disclosure of attributes and not abusing the released attributes (**T9**) and maintaining the agreed policies and procedures regarding access control and delegated access (**T10**). Formally:*

$$\frac{\left[idp \xrightarrow[conf]{DT\ :\ \{ND,ABU\}} sp\right] \qquad \left[idp \xrightarrow[conf]{DT\ :\ ACDA} sp\right]}{\left[idp \xrightarrow[conf]{DT\ :\ POL} sp\right]}$$

As before, the trust direction and strength must be same in **T9** and **T10** and the compound trust also will have that same trust direction and trust strength.

SP Trust in the IdP.

T11. The SP trusts that the IdP has implemented adequate procedures for registering users and for issuing credentials (denoted as $T7$ in [8]):

$$sp \xrightarrow[loa]{DT\ :\ REG} idp$$

This captures the realistic scenarios where a LoA value, determined and released by the IdP, is used by the SP to evaluate the level of trust it can have on the IdP in a specific trust scope. A lower LoA value may influence the SP to place a lower trust and similarly a higher LoA value may influence the SP to have a higher trust on the IdP for a particular scope.

T12. The SP trusts that the IdP will authenticate the user appropriately as per the requirement and will release user attributes securely:

$$sp \xrightarrow[loa]{DT\ :\ AUTHN} idp$$

We combine **T11** and **T12** to define a compound trust using the following rule.

Rule 5 (Compound Trust of Registration-Authentication.) *A compound trust of Registration-Authentication, denoted as RAUTH, outlines the SP trust that the IdP registers users securely (**T11**) and authenticates users and releases attributes as per the requirement (**T12**). Formally, we have:*

$$\frac{\left[sp \xrightarrow[loa]{DT\ :\ REG} idp\right] \qquad \left[sp \xrightarrow[loa]{DT\ :\ AUTHN} idp\right]}{\left[sp \xrightarrow[loa]{DT\ :\ RAUTH} idp\right]}$$

5 Trust Modelling in Dynamic Federations

In this section, we model trust between different entities in traditional federations. We only consider high level trust as the fine-grained trust for this federation is similar to traditional federations.

Type 1 Federation. Here, we have two different types of trust. To an SP, each dynamically added IdP will be treated as *untrusted*. Formally, in a Type 1 federation $f \in \mathcal{F}$ for $sp \in SP_f$ and dynamically added $idp \in IDP_f$:

$$sp \xrightarrow[UT]{DT\ :\ FED} idp$$

However, to the IdP, the SP can be *untrusted* or *semi-trusted* depending to conditions discussed previously:

$$idp \xrightarrow[\{UT,ST\}]{DT\ :\ FED} sp$$

Type 2 Federation. This is similar to the traditional Type 2 federation as discussed previously, except there is no mutual trust between dynamically added entities and static entities, hence we consider each trust direction separately.

Using Rule 1 and Rule 2 we can derive a transitive trust between any two entities in a dynamic federation as follows. For $f_1, f_2 \in \mathcal{F}$, $sp_1 \in SP_{f_1}$, $sp_2 \in IDP_{f_2}$, $idp_1 \in IDP_{f_1}$, $idp_2 \in IDP_{f_2}$ and where idp_2 has been added dynamically into federation f_1 and sp_2 has been added dynamically into federation f_2:

$$\frac{\left[sp_1 \xleftarrow[FT]{DT\ :\ FED} idp_1\right] \qquad \left[idp_1 \xrightarrow[UT]{DT\ :\ FED} idp_2\right]}{\left[sp_1 \xrightarrow[UT]{IT\ :\ FED} idp_2\right]}$$

Since, idp_1 acts as the SP to idp_2 and a dynamically added IdP is always treated as an *untrusted* entity to a SP, the trust from idp_1 to the idp_2 is regarded as untrusted. A few more derivation are given below:

$$\frac{\left[idp_2 \xrightarrow[UT]{DT\ :\ FED} idp_1\right] \qquad \left[idp_1 \xleftarrow[FT]{DT\ :\ FED} sp_1\right]}{\left[idp_2 \xrightarrow[UT]{IT\ :\ FED} sp_1\right]}$$

This derives the transitive trust between idp_2 and sp_1.

$$\frac{\left[sp_2 \xrightarrow[UT]{DT\ :\ FED} idp_2\right] \qquad \left[idp_2 \xrightarrow[UT]{DT\ :\ FED} idp_1\right]}{\left[sp_2 \xrightarrow[UT]{IT\ :\ FED} idp_1\right]}$$

This derives the transitive trust between sp_2 and idp_1 and below we derive the transitive trust between idp_1 and sp_2.

$$\frac{\left[idp_1 \xrightarrow[UT]{DT\ :\ FED} idp_2\right] \qquad \left[idp_2 \xrightarrow[\{UT,ST\}]{DT\ :\ FED} sp_2\right]}{\left[idp_1 \xrightarrow[UT]{IT\ :\ FED} sp_2\right]}$$

6 Trust Transformation with Interactions

We have seen how trust is transformed due to transitivity. Next, we explore how it is transformed due to interactions. We use the following notation to denote a change of trust from T_1 to T_2 for an interaction A: $T_1 \overset{A}{\Rightarrow} T_2$. Sometimes, we logically join (using the "$\wedge$" operator) more than one interaction to signify the fact that more than one interaction is required to trigger a trust transformation.

Trust transformation in Static Federations. Our first example explores how the trust can be transformed between a user (the trustor) and an IdP (the trustee). At the initial stage, the confidence (trust strength) of the user could be low. Once the user is registered and authenticated using a secure communication channel (e.g. HTTPS), the trust strength could increase to medium since it reflects that the IdP is careful to maintain the confidentiality and integrity of her data. For a federation $f \in \mathcal{F}$, $u \in U_f$ and $idp \in IDP_f$, this is modelled by:

$$\left[u \xrightarrow[L]{DT:\ RAuth} idp\right] \xRightarrow{\{SC(u \overset{RG}{\rightsquigarrow} idp)\} \wedge \{SC(u \overset{A}{\rightsquigarrow} idp)\}} \left[u \xrightarrow[M]{DT\ :\ RAuth} idp\right]$$

The user may have another boost in trust when she has a positive interaction with the IdP for a period. One example is the use of a consent form that allows the user to select the attributes that she wants to release to an SP, and thus allows her the option to provide consent to release data to the SP. Formally:

$$\left[u \xrightarrow[M]{DT:\ SRV} idp\right] \xRightarrow{\{SC(idp \overset{C}{\rightsquigarrow} u)\}} \left[u \xrightarrow[H]{DT\ :\ SRV} idp\right]$$

Our second example involves transforming privacy trust with interactions. The involved interactions are the IdP allowing the user to use anonymous or pseudonymous identifiers and offering the opportunity to provide consent regarding attributes. The trust strength will initially be low and will transform to either medium or high depending on different factors. Example factors are a user-friendly interface that makes it easier for the user to choose anonymous or pseudonymous identifiers or allows the user to choose attributes and provide consent. The trust transformation is modelled by:

$$\left[u \xrightarrow[L]{DT\ :\ PRIV} idp\right] \xRightarrow{\{SC(idp \overset{AP}{\rightsquigarrow} u)\} \wedge \{SC(idp \overset{C}{\rightsquigarrow} u)\}} \left[u \xrightarrow[\{M,H\}]{DT\ :\ PRIV} idp\right]$$

Trust transformation in Dynamic Federations. For federation $f \in \mathcal{F}$, $u \in U_f$, $idp \in IDP_f$ dynamically added by u and $sp \in SP_f$, the trust transformation occurs only if u has agreed to release her attributes from idp to sp:

$$\left[idp \xrightarrow[UT]{DT\ :\ FED} sp\right] \xRightarrow{\{SC(u \overset{C}{\rightsquigarrow} idp)\} \wedge \{SC(idp \overset{RL}{\rightsquigarrow} sp)\}} \left[idp \xrightarrow[ST]{DT\ :\ FED} sp\right]$$

7 Quantifying Trust

In real life, trust is an analogue property, and hence it is difficult to represent with discrete values. However, it might be useful to compute the trust between involved entities using discrete values when the entities belong to a computational system and require a discrete value to represent the trust in that system. Among three pieces of information used to represent trust (type, scope and strength), we only use type and strength to compute a trust value. This is because scope only represents a context, a qualitative attribute, in which trust holds, while both type and strength can be represented numerically. For example, direct trust represents a higher confidence as it is based on first-hand experience, unlike indirect

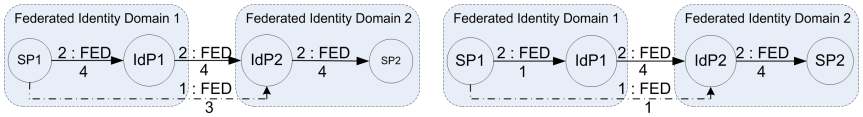
trust. We introduce the following formula to quantify trust in a federation $f \in \mathcal{F}$ between entities $e_1, e_2 \in E_f$ for trust scope s where e_1 is the trustor and e_2 is the trustee:

$$QT_{e_1}^{e_2}(s) = t_{e_1}^{e_2}(s) \cdot v_{e_1}^{e_2}(s)$$

where $QT_{e_1}^{e_2}(s)$, $t_{e_1}^{e_2}(s)$ and $v_{e_1}^{e_2}(s)$ represent the quantified trust, trust type and strength of e_1 over e_2 in the scope s for federation f.

In the formula the trust strength quantifies how much trust one entity may have over another entity and the trust type signifies the confidence on that quantification. Trust type can be thought as the weight of the trust strength. Note that, this is one way of quantifying a trust and there are other possibilities.

We now consider a few examples. As stated above to quantify trust we need to give values to trust types and strengths. Regarding types, we assign 1 and 2 to indirect and direct trust respectively, and for strength, we assign 1, 2 and 3 to *conf* and 1, 2, 3 and 4 to *fed-trust*.



(a) Static Federation. (b) Dynamic Federation.

Fig. 2. Quantifying trust example.

We can now quantify trust in the federations illustrated in Figure 2. The left box of Figure 2(a) illustrates a Type 1 static federation while Figure 2(a) and Figure 2(b) illustrate a Type 2 static and dynamic federations respectively. The direct trust between sp_1 and idp_1 for the Type 1 static federation is given by:

$$QT_{sp_1}^{idp_1}(FED) = 2 \cdot 4 = 8$$

since the entities have direct trust between them ($t_{sp_1}^{idp_1}(FED) = 2$) and they fully trust each other ($v_{sp_1}^{idp_1}(FED) = 4$).

For the static Type 2 federation in Figure 2(a), the indirect trust between sp_1 and the idp_2 is given by:

$$QT_{sp_1}^{idp_2}(FED) \ = \ 1 \cdot 3 \ = \ 3$$

This is because the entities have indirect trust between them ($t_{sp_1}^{idp_2}(FED) = 1$) and according to 2, the trust strength between them ($v_{sp_1}^{idp_2}(FED) = 3$).

Similarly, for the dynamic Type 2 federation in Figure 2(b) and calculating the indirect trust between sp_1 (the trustor) and the idp_2 (the trustee), where the trust strength between the transitive entities are not same, we have:

$$QT_{sp_1}^{idp_2}(FED) \ = \ 1 \cdot 1 = \ 1$$

8 Related Work

A few major papers on the general topic of trust and trust management can be found in [5,9,10,11,16]. These works mainly concentrated on the discussion and analysis of trust and trust management and the discussion of trust regarding identity management was mainly absent.

A comprehensive taxonomy of trust requirements for the FIM can be found in [2]. Unfortunately, the requirements have been outlined in textual formats and none of requirements has been modelled and analysed mathematically. The authors in [14] have presented an integrated trust management model with respect to context-aware services. The model is based on different trust relationships which have been analysed using mathematical notations. The paper did not consider the underlying trust requirements that hold together the involved entities in that trust relationship. In this paper we have adopted their notation to illustrate the trust relationship. Huang et al. [6] have presented a trust calculus targeted for the PKI (Public Key Infrastructure) and have shown how the calculus can be used to derive trust between entities in a certification chain. The focus of their work is quite different than ours in the sense that they did not deal with any underlying trust requirements in the FIM. The authors in [4] have presented a formalisation of authentication trust for the FIM. The authors did not consider any other trust requirements, and hence their formal representation is not comprehensive in nature.

9 Conclusions

Trust in the traditional Type 1 Federation is a complex issue with the involvement of several different autonomous parties and their disparate security domains. The complexity increases with the introduction of a Type 2 Federation. The advent of the dynamic federation adds up another layer of complexity. Even though there exist numerous works on the mathematical modelling of trust in the online setting, there is a gap on the mathematical modelling and analysis of trust in the setting of FIM. In this paper we have introduced a mathematical framework to represent and analyse complex trust issues in FIM. We have used our model to represent trust in different settings. We have introduced a model of interactions for FIM and have shown how interactions and the trust transitivity can transform trust. Finally, we have proposed a simple formula to quantify trust. Our model can be used in a wide range of applications. It can be used to express and derive trust between any number of entities in any type of federations. A larger federation where there are many IdPs and SPs that exhibit a highly dynamic nature where changes are common. Trust transformation using interactions can be the ideal way to represent trust in such a dynamic environment. Finally, the way we have evaluated trust can be used to assess trust between any entities in a federation or to assess the quality of service provided by an IdP or an SP. Next, we plan to use our model to analyse other aspects of identity management such as attribute aggregation and mobile identity management.

References

1. David W Chadwick. Federated Identity Management. In *FOSAD 2008/2009*, number 5705 in LNCS, page 96-120. Springer, 2009.
2. Md. Sadek Ferdous and Ron Poet. Analysing Attribute Aggregation Models in Federated Identity Management. In *SIN '13*, page 181-188. ACM, 2013.
3. Md. Sadek Ferdous and Ron Poet. Dynamic Identity Federation Using Security Assertion Markup Language (SAML). In *IFIP IDMAN '13: Policies and Research in Identity Management*, volume 396 of *IFIP Advances in Information and Communication Technology*, page 131-146. Springer, 2013.
4. Hidehito Gomi. An Authentication Trust Metric for Federated Identity Management Systems. In *Security and Trust Management*, volume 6710 of *LNCS*, page 116-131. Springer, 2011.
5. Tyrone Grandison and Morris Sloman. In *Trust Management*, page 91-107. Springer, 2003.
6. Jingwei Huang and David Nicol. A Calculus of Trust and Its Application to PKI and Identity Management. In *IDtrust '09*, page 23-37. ACM, 2009.
7. Audun Jøsang, Muhammed Al, and Zomai Suriadi Suriadi. Usability and privacy in identity management architectures. In *ACSW '07*, page 143-152. 2007.
8. Audun Jøsang, John Fabre, Brian Hay, James Dalziel, and Simon Pope. Trust requirements in identity management. In *ACSW Frontiers '05*, page 99-108. Australian Computer Society, Inc., 2005.
9. Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618-644, 2007.
10. Audun Jøsang, Claudia Keser, and Theo Dimitrakos. Can We Manage Trust? In *Trust Management*, volume 3477 of *LNCS*, page 93-107. Springer, 2005.
11. Audun Jøsang, Elizabeth Gray and Michael Kinateder. Simplification and Analysis of Transitive Trust Networks. *Web Intelli. and Agent Sys.*, 4(2):139-161, April 2006.
12. U. Kylau, I. Thomas, M. Menzel, and C. Meinel. Trust Requirements in Identity Federation Topologies. In *AINA '09*, page 137-145, 2009.
13. D Harrison McKnight and Norman L Chervany. The meanings of trust. 1996.
14. Ricardo Neisse, Maarten Wegdam, Marten Van Sinderen, and Gabriele Lenzini. Trust Management Model and Architecture for Context-aware Service Platforms. In *OTM'07*, page 1803-1820. Springer-Verlag, 2007.
15. NISTWP. Electronic Authentication Guideline: INFORMATION SECURITY, April 2006. `http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf`.
16. Sini Ruohomaa and Lea Kutvonen. Trust Management Survey. In *Trust Management*, volume 3477 of *LNCS*, page 77-92. Springer, 2005.
17. Md. Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Md. Moniruzzaman, and Farida Chowdhury. Identity federations: A new perspective for Bangladesh. In *ICIEV '12*, page 219-224. IEEE, 2012.
18. OASIS Standard. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. 15 March, 2005. `http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf`.