ETSI GS INS 005 V1.1.1 (2011-03)

Group Specification

Identity and access management for Networks and Services; Requirements of an Enforcement Framework in a Distributed Environment

Disclaimer

This document has been produced and approved by the Identity and Access Management for Networks and Services (ETSI INS) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/INS-005

Keywords
authorization, enforcement

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Identity and access management for Networks and Services (INS).

Introduction

Enforcing authorization decisions in a distributed environment is a challenging task compared to traditional services. The entity directly controlling and enforcing, the access to the resources may be organizational or physically separated from the entity providing the decision. In a cloud environment multiple entities might control the authorization for a particular activity. In addition to the enforcement of the pure access decision a set of obligations may have to be enforced. Another approach is to attach the access policy directly to the data and ensure that it is always enforced.

In a distributed environment these approaches require not only a trust relationship between the enforcement and decisions points on the one hand and entities passing data with attached policies on the other hand, it also has to be ensured that decisions and obligations has well as the attached policies are syntactically and semantically understood in the same way at all involved entities.

While the use cases and resulting requirements of distributed access control has been previously addressed [i.1] is focusing more on the decision process, the present document considers the distributed enforcement of these decisions and the related obligations, which are used to protect the data in general, ensure the privacy of the user, or provides flexible auditing of the access requests. If multiple entities are involved in the decision process their obligations have to be enforced as well. The present document will also illustrate that for a distributed environment to location of the enforcement is an important aspect. As different entities are involved the obligations utilized in the authorization process have to be specified in a dynamic manner.

After providing the relevant references and defining the used terminology an overview of the current landscape on distributed enforcement environment is given. The main contribution of the present document is a set of application scenarios illustrating various aspects of distributed enforcement environments which are not yet considered or addressed by other standardization activities. These application scenarios are also used to illustrated requirements related to distributed enforcement environments, which are finally presented in the present document.

1 Scope

The present document will provide the requirements on distributed enforcement environments, taking into account attached policies as well as frameworks with dedicated enforcement and decision points. The requirements of the decision making process has been covered in [i.1].

The present document will not only deal with the requirements of the architecture and the information carried in the decision, but will take into account the requirements regarding specification of the obligations exchanged.

It is assumed that the different entities especially those described as policy enforcement points (PEP) and policy decision points (PDP) have a mutual trust relationship, on which they rely on with respect to decision being made and enforced accordingly. The basis of these trust relationships could be based on legal agreement and/or unforgeable audit trails.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS INS 002 (V1.1.1) "Identity and Access Management for Networks and Services Distributed Access Control for Telecommunications Use Cases and Requirements".

[i.2] OASIS (2.0 edition, 1 February 2005): "eXtensible Access Control Markup Language (XACML)".

[i.3] OASIS (3.0 edition, 10 August 2010): "eXtensible Access Control Markup Language (XACML)", Committee Specification 01.

[i.4] OASIS XACML (v3.0, 28 December 2007): "Obligation Families Version 1.0", Working draft 3.

[i.5] IBM: "Enterprise Privacy Authorization Language (EPAL), Version 1.2", Submission to W3C, 2003.

[i.6] W3C Recommendation W3C PLING (16 April 2002): "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification".

[i.7] Anne H. Anderson: "A comparison of two privacy policy languages: EPAL and XACML" In Proceedings of the 3rd ACM workshop on Secure web services (SWS '06). ACM, New York, NY, USA, 53-60.

[i.8] G. Karjoth, M. Schunter, M. Waidner: "Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data", 2nd Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science, Springer Verlag - 2002G.

[i.9] Marco Casassa Mont, Siani Pearson, Pete Bramhall: "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," Database and Expert Systems Applications, International Workshop on, p. 377, 14th International Workshop on Database and Expert Systems Applications (DEXA'03), 2003.

[i.10] M. Y. Becker, C. Fournet and A. D. Gordon: "Design and semantics of a decentralized authorization language". In IEEE Computer Security Foundations Symposium, pages 3-15, 2007.

[i.11] M. Y. Becker, A. Malkis and L. Bussard: "A framework for privacy preferences and data-handling policies". Technical Report MSR-TR-2009-128, Microsoft Research, 2009.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

obligation: operation specified in conjunction with a policy, either by the data owner or other relevant entities, and should be enforced as part of a policy decision

NOTE: Obligations may be triggered by timing constraints, by policy violations, or by event notifications from other entities.

associated/sticky policies: policies associated with obfuscated user data and sent around with this data, determining the relevant disclosure constraints

NOTE: Sticky policies are usually specified as the results of an automated matching between user's wishes and service provider's promises with regard to data handling. They contain the authorization rules and obligations that the PEP is obliged to enforce.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

EPAL	Enterprise Privacy Authorization Language
IdM	Identity Management
IdP	Identity Provider
LBS	Location Based Service
MNO	Mobile Network Operator
MSNS	Mobile Social Network Site
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SaaS	Software as a Service
SecPAL	Security Policy Assertion Language
TA	Tracing Authority
XACML	eXtensible Access Control Markup Language

4 Current Landscape

4.1 eXtensible Access Control Markup Language (XACML)

During the recent years OASIS XACML 2.0 [i.2] has become the recognized standard for the specification of access control policies as well as a generic framework for access control. The policy enforcement point (PEP) sends access requests, which are evaluated at a policy decision point (PDP). In addition to the results which indicate whether the access should be granted or denied, a list of obligations, which have been specified in conjunction with the evaluated policies and policy sets, may be sent back to the PEP. The PEP is responsible for decoding and enforcing these obligations. While for access privileges the policy language is flexible, the handling of obligations is quite limited.

From a language point of view a general syntax is specified encoding the name of an obligation and its arbitrary list of attributes, which are fixed values or as of 3.0 [i.3] variables.

The OASIS XACML standard [i.2] assumes that the PEP recognizes the obligations returned by the PDP upon on access request and knows how to implement them correctly. If the PEP does not recognize the obligation, the request is denied according to the specification. In XACML 3.0 [i.3] different types of PEPs are specified, but the general assumption is that the PEP understands the obligations and is able to enforce them. In addition to obligations a new element called *advice* has been introduced in version XACML 3.0 [i.3], these advices are like obligations specified in conjunction with policies or policy sets and provided by the PDP to the PEP as part of the decision. In contrast to obligations advices may be safely ignored by the PEP.

There has been work [i.4] regarding the timing constraints on enforcing the obligation and fall-backs in case of errors during the obligation execution.

4.2 Enterprise Privacy Authorization Language (EPAL)

The Enterprise Privacy Authorization Language (EPAL) is a formal language to express fine-grained enterprise privacy policies, submitted to the W3C consortium [i.5]. The key aspect of EPAL is to provide a detailed description of high-level privacy policies such as W3C P3P [i.6].

EPAL defines policy which contains a general information element describing the policy, a set of vocabulary which may be used inside the policy and conditions on their usage acting as a global pre-condition, together which rules which define the actual authorization of the policy. Parameterized obligations could be associated to rules specifying actions which should be executed to ensure the privacy of the user data. The actual syntax or semantic of obligations is not specified.

It has shown has been shown in [i.7] that EPAL policy and rules provides a subset of the functionality that can be provided by XACML [i.2].

4.3 Sticky Policies

In [i.8], sticky policies are defined as a paradigm that allows users to strictly associate policies to identity data, to drive access control decisions and privacy enforcement. When using sticky policies, data is sent obfuscated from the user to the data consumer (usually a service or an identity provider). This obfuscated data is sent along with a set of sticky policies that determine the relevant disclosure constrains. Only in the case that the data consumer fulfils with all the requirements, it will be provided with a decryption key to be able to read the data.

In [i.9] it is provided an extended model that refines the initial proposal of [i.8]. This model describes a trusted third party called Tracing Authority (TA). Any consumer has to demonstrate to the TA that it understands the involved terms and conditions, and that it fulfils with the requirements established in the sticky policies. Once this is demonstrated, is the TA who provides the consumer with a key that can be used to decrypt the obfuscated data. All the disclosures of confidential data are logged and audited by the TA. In order to minimize the risk of having only one trusted entity, multiple TAs are allowed. Sticky policies created by the user should specify which TA must be consulted by the consumer in order to obtain a valid decryption key.

4.4 Microsoft Security Policy Assertion Language

The Security Policy Assertion Language (SecPal) [i.10] is a declarative, logic-based authorization language designed to meet access control requirements in large-scale distributed computing environments such as such as those for on-demand utility computing. As a constrained natural-like language with limited set of deduction rules, the SecPal appears simple and comprehensive. SecPal syntax and semantic aim for a balance between simplicity and expressiveness of security policies. SecPal also provides functions for expressing trust relationships at a fine-grained level, delegation policies, identity and attribute assertions, capability assertions, revocations, and allowing auditing. Moreover it can be easily integrated within existing identity management mechanisms and protocols. By supporting an automatic translation of any security rule into a simple and very flexible XML syntax, SecPal suppress, or at least minimizes, the necessity for semantic or syntax translation and reconciliation between different trust and security protocols. With SecPal, authorization policies and security tokens are specified assertions logics whereby an assertion contains one or more claims and variables. A claim contains a fact which is essentially a statement about a subject and a target. On the other hand, variables included in SecPAL assertions allow generic policies to be authored. They are substituted for concrete values at evaluation-time. In its specification SecPal defines five main kinds of predicates which could be used to make almost any statements about principals. Those are:

1) *Action Verbs:* which describe a right a subject may have to perform an action (read, write, delete, etc.) on a resource.

2) *Possess:* that allows attributes, common name, group names, roles etc to be assigned to a subject.

3) *Can Say:* is used to express trust relationships and constrained delegation of right.

4) *Can Act As:* allows the specification of unconstrained mapping between a new subject and an old one e.g. after dynamic (re-) provisioning.

5) *Revoke*: to express the revocation of previously issued claims.

However, SecPal does not allow the specification and enforcement of obligations in a flexible-enough way. With "SecPal for privacy" [i.11], Microsoft proposes an extension of the original SecPal in order to allow both the user to specify its preferences on how its private data should be handled by a service, and the service' promise on handling users' private data. Those preferences and policies are specified in terms of access control rules to be granted and application (in-) dependent obligations to be enforced. They can be expressed as assertions/ statements and queries in an instance of the original SecPAL.

5 Application Scenarios

The following application scenarios are illustrating the different aspects related to an enforcement framework in a distributed environment. Some aspects are shared between several scenarios as a kind of general assumption.

5.1 support for the specification and enforcement of privacy obligation in clouds

In cloud environment various services are interacting to provide a service to the user. These services could be applications which are collaborating in a so called mash-up to provide a service to the user. Another example is one service storing the data of a user, ranging from single attributes to media collection, while another service is actually working on this data. As an example we assume on service storing the photos of a user, while another one is offering an editing and printing service.

How the data at another service is actually accessed or methods are called is out of the scope. What could be observed is that the obligations tied to the access or the usage of a service could not only be enforced at the hosting side. Such obligations are not only related to the privacy like "deletion after usage" or "not used outside country x". They could also be related to the general confidentiality of the data "encrypted interim storage" or even ensure that the rights of owner could be proved by enforcing an obligation like "attach digital watermark". These obligations have to be enforced at the side requesting the access or composing an existing service into a larger one. In existing systems the obligations have to be added to the reply related to the actual access or method request or they are contained in the policies which are coupled with the actual data. The requesting service has to evaluate the obligations and enforce them accordingly. This could be seen as a kind of second level PEP.

As presented in [i.1] the decision of whether the access to the data is granted or not may be distributed and several remote decisions are combined to the final one. In a cloud scenario the service providing a mash-up for an employee of a company checks back with the company what underlying services are in line with their corporate policy and also checks in a kind of advance manner whether the underlying service actually provide access to the service for the particular user.

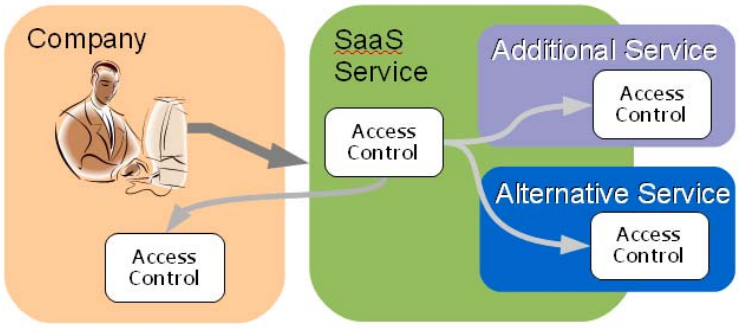

Figure 1: SaaS

As the decision of each access control entity may contain obligations these obligations have to be combined and enforced at the PEP handling the original request. Each of the access control engines might have a different list of obligation it is requesting. In order to successfully provide the service it has to be ensured that these obligations are understood at the PEP.

5.2 Location Based Service in Enterprise Environment

5.2.1 Description

Consider a company that authorizes its employees to use mobile communication devices (e.g. smartphones, tablet computers) to access, within the context of their job responsibilities, a Location Based Service (LBS) to which it has subscribed. The company uses the LBS provided as SaaS by a Telco Operator to improve the coordination between mobile employees and to enhance its customer relationship management processes. Hence the LBS may not only indicate the actual geographic location, or the proximity, of a mobile employee to other relevant players (colleagues and customers) but also her/his general availability. This way meetings between colleagues could be easily set up, company's customers can indicate need for consultancy and the company can smoothly deploy personal resources to respond to such kind of needs, etc. However, since an automated collection, processing and exchange of employees' location and the availability information clearly pose a threat to both the security and business interests of the company and the Telco Operator, and the privacy interest of each mobile employee, mechanisms to prohibit information leakage and manage privacy level are required.

As an example, let us assume that an employee -Alice- is visiting a customer in a particular country/town. While this customer may be allowed to get detailed location information to see that Alice has arrived on schedule at the airport etc., other customers in the same country/town who would not be visited the same day do not have access to any detailed information on Alice's location/availability at all. Instead the LBS is just indicating that Alice is travelling or in a meeting. Alice, being the data owner, might rely on her company policy framework to specify privacy preferences and obligations (e.g. commitment to obfuscate her location information) which alongside other security policies would be enforced by the LBS Provider. According to her corporate policy, Alice may also want to deactivate (or not) her visibility for certain designated user groups at all.

The policies and obligations related to this use case may need to be well specified, evaluated and enforced in a distributed fashion.

5.2.2 Actors

- Mobile employee (Alice): the mobile employee of a Company, using a LBS while carrying out her job responsibilities.
- Bob: is either a colleague of Alice's or one of her external business partner. Bob has subscribed to Alice's location and availability information.
- Telco Operator providing LBS to Companies (i.e. its customers) as a SaaS, through a subscription model.
- LBS a service that provides Alice's information to subscribers (i.e. colleague and external business partner) with different level of detail.
- Company signing up for a paid-subscription to a LBS provided by the Telco Operator.

5.2.2.1 Actors specific Issues

- Mobile employee (Alice): agrees with having her presence and availability information published.
- Bob: Alice's colleague or Business partner subscribes to location and availability information on Alice.
- Telco Operator provides LBS as additional service.
- LBS collects, processes and transfers location and availability information according to the policies of the related company and employees respectively.
- Company manages policies and obligation related to the handling of its employee's presence and availability information.

5.2.2.2 Actors specific Benefits

- Mobile employee (Alice): relies on LBS to easily carry out her job responsibilities (e.g. better coordination with colleagues and effective customer relationship management) while being able to manage her level of privacy. This way she can set a coarse granularity of disclosure for presence and availability information requested outside the working hours.
- Bob (Alice's colleague or Business partner): colleagues enjoy smother collaboration among each other; Business partner enjoy the improved interaction and coordination with Alice's company.
- Telco Operator/ LBS:
  - diversifies its business and consequently enjoys business advantages through an new activity that would have been deemed as non-core activity only a few years ago;
  - benefits from being able to deliver such services to multiple large customers;
  - addresses its customers privacy concerns by collecting, processing and transferring location data according to the privacy policies and obligations of each related company/mobile employee (one step towards legal compliance).
- Company:
  - relies on LBS to assist its mobile employees in carrying out their job responsibilities;
  - addresses growing employees' privacy concerns by making sure that the interaction with the LBS as well as the disclosure of employees' location data complies with the privacy preferences and obligations of each employees involved (one step towards legal compliance).

5.2.3 Pre-Conditions

- The Telco Operator acting as SaaS provider has licensed the location based application to this particular company.

5.2.4 Post-Conditions

- Each authorized mobile employee has specified privacy preferences and obligations which both the company and the SaaS provider enforced.
- Mobile employees (and remote business partners) have utilized the LBS according to the policies and obligations which expressed the matched interest of all involved actors.

5.3 Online Social Network Site

5.3.1 Description

Consider a mobile User -Alice- using her Smartphone to surf on the Net and subscribes for premium services offered by a Mobile Social Network Site (MSNS). The services booked involve a Location Based Service (LBS) that make use of Alice's current geographic location to actualize her online profile available on the MSNS. Alice's location is captured by the Mobile Network Operator's (MNO) with help of triangulation techniques. The MSNS Operator has an alliance with Alice's MNO. Hence it can accept the services usage charges to Alice mobile phone bill. The MNO subsequently acts both as IdP and Payment Provider. It leverages previously registered user's identity attributes, e.g. credit card number, for delivering payment services and return collected location data to the MSNS.

Let us imagine Alice asking the MSNS for the position of a person belonging to her electronic "Circle of Friends", i.e. best client, current project colleagues or other persons with similar interests, or just request for peoples in her geographical proximity. Such location information are managed (i.e. collected, processed and disclosed) according to the privacy preferences of all users involved. The MNO acting as Location Information Provider, from the MSNS point of view, ensures that location information are collected and processed according to Alice's privacy preferences. However, once posted online other types of policies may apply to the information contained in the post i.e. the MSNS may enforce additional privacy policies and obligations, depending on the context and the degree of trust in the person requesting access to location data in Alice's profile. Such privacy obligations would for instance stipulate to log this particular process or to use reliable data masking techniques to de-identify location data before disclosure. In a default setup which might assumes that the MSNS is not to be considered trustworthy, the MNO provides functions that allow an automatic management of all mobile users' privacy preferences and their enforcement every time a request for location data is made, without sharing any kind of sensitive information with the MSNS.

All related privacy policies and privacy obligations typically result from an automated matching of the data owner's (i.e. mobile User) privacy preferences and the data requestor's (e.g. the MSNS) privacy promises.

5.3.2 Actors

1) Mobile User (Alice): uses her Smartphone to access a mobile social network platform.
2) Mobile Network Operator: besides being a network operator, the MNO also acts as provider of e-payment services.
3) Mobile Social Network Site (MSNS) provides a mobile social network platform in which LBS are integrated.

5.3.3 Actors specific Issues

1) Mobile User (Alice):
   a) subscribes for, and uses, LBS offered by a MSNS.
   b) specifies privacy policies and obligations related to the handle of and the access to her private data.

2) Mobile Network Operator:

   a) acts as broker that provides IdM services as well as payment services and thus is able to collect, process and transfer user's current position and other private data to the MSNS Operator;

   b) collects, process and transfers location data according to Alice's privacy preferences;

   c) enforces or make sure that all related security and privacy obligations are enforced either prior to, during or after each user's data collection, processing or transfer.

3) Mobile Social Network Site (MSNS):

   a) provides its mobile customers with a online platform involving location based features;

   b) grants Alice the access to the service based on identity credential and assertions received from the MNO;

   c) grants access to location information displayed on Alice's profile page according to privacy settings which would obviously be specific to certain user groups;

   d) enforces or make sure that all related security and privacy obligations are enforced either prior to, during or after each user's data collection, processing or transfer.

5.3.4 Actors specific Benefits

1) Mobile User (Alice):

   a) uses credentials she received from the MNO to seamlessly access, and pay for a transaction with an external service provider (i.e. MSNS);

   b) specifies privacy preferences , or in some settings, negotiates privacy obligations that on one hand police her interaction with both the MNO and the MSNS, and on the other hand govern the handling of her sensitive information by the MNO and MSNS.

2) Mobile Network Operator:

   a) leverages two of its most important assets, i.e. its reach and its infrastructure, in order to diversify its business and deal with margin pressures and an increasingly competitive environment;

   b) addresses growing user's privacy concerns by collecting and transferring location data according to the privacy policies/obligations of each related user.

3) Mobile Social Network Site (MSNS):

   a) enjoys business advantages by integrating location data in location based features in their social network services;

   b) addresses growing user's privacy concerns by supporting access control, according to the user's privacy preferences.

5.3.5 Pre-Conditions

- The MSNS has set up Alice's online profile.

5.3.6 Post-Conditions

- Mobile User (Alice) has specified and subsequently exchanged or negotiated privacy obligations with, the MNO and the MSNS respectively.
- MNO has delivered Alice's location information to the MSNS according to her privacy preferences and related obligations.
- Privacy policies and obligations are reliably enforced whenever location information posted on Alice's profile is accessed.

5.4 Specification of enforcement location

A user wants to ensure the privacy of his data which is handled by a SaaS environment. Enforcing obligation at the PEP of the entity does not help to control the later usage of the data. In a distributed environment like SaaS various entities are actually handling the data or at least have indirect access. In addition to the entity storing the data, the user wants to enforce obligation at those processing entities processing his data and finally the entities displaying it to himself or other users.

At each entity some obligations might need to be enforced in order to achieve privacy (e.g. no persistence storage at the processing or displaying entities) or more general data confidentiality as other obligations may be related to the communication between different entities (e.g. encryption of the channel or authentication of the end-points). In addition to this obligations might require that at some involved sites logs are created for audit purpose.

As when editing a policy the user describes these entities either in an abstract way based on the functionality (e.g. the displaying site), or in order to get a reliable audit track specifies the sites explicitly, which e.g. should store the log.

5.5 Dynamic obligation specification

The application scenarios in which Identity and Access Control Management could be used are wide spread, therefore the obligations which have to be enforced when accessing the user's data might differ between organizations. Some example categories and the included obligations could be:

- Data Storage
  - Location of storage (e.g. Jurisdiction)
  - Securing the stored data (e.g. Encryption)
- Data TraDnsportation
  - Securing during transportation
  - Routing enforcement (e.g. not passing a specific jurisdiction)
- ExpiratiDon
  - Deletion of data at a certain time
  - Deletion after usage
- Access Notification
  - Logging of access requests to the data
  - Notification about access requests

This list of obligation is not exhaustive and one can claim that creating a list which covers all obligations required by the potential applications seems to be impossible and not extensible.

In order to illustrate how dynamic obligation specification can support to enforce the required obligations we consider the following scenario:

A user wants to use a new service, which requires access to some identity information or other user's attributes. The new service has to make sure that it is able to enforce the obligations associated to this information.

As there is most likely no general list of all possible obligations, the new service and the entities responsible for the identity management of the user synchronize their list of obligations. The new service provides the list of obligation, it is able to enforce. The identity management provides the list of obligations which are used in the policies. The goal final goal of this exchange is to agree on a common list of obligations which may be used and are guaranteed to be understood. As an initial step this understanding is on a syntactical level, describing the semantic of an obligation in a generic way, moves the problem of finding a comprehensive list of obligations just to a meta-level.

If the original lists do not match, it might be possible to negotiate some substitutes for these non-matching obligations. In an advanced negotiate the PEP might not be able to delete some data at a certain point of time, but the obligation that no data is persistently stored covers the actual privacy needs of the policy administrator.

Especially the later list of obligation might change over the time, as the user would like to enforce additional obligations based on the experiences he made on the usage of his identity information through the services.

6 Requirements

This clause aims to explore the requirements of an Enforcement Framework in a Distributed Environment, which are either presented in the above use cases or are derived from general assumptions made in the present document.

6.1 General Distributed Enforcement Framework Requirements

1. All entities interacting in an enforcement environment should have a trust relationship, regarding how related obligations are enforced. *from general assumption*

In the introduction of the present document it has been stated has a general assumption that a trust relationship is required, as the different entities might not be under the control of one organization. The trust relationship could be established by technical means like direct observation of the enforcement, trust establishment and validation between obligation issuer and subject, or by non-technical such as legal contracts. The result of the trustworthiness evaluation of both obligation issuer and subject should be considered as input for the obligation enforcement. This trustworthiness evaluation could be achieved by relying on different trust models/ technologies.

2. Authentication, Integrity and non-repudiation should be enabled for all transactions. *from general assumption*

While this requirement has been already stated for an Distributed Authorization framework [i.1], it has to be emphasized that all additional transactions share this requirement as a general assumption necessary for this framework.

3. All entities support a general language describing the syntax of an obligation including its parameters.
from use case 1 & 5

This general language obligation description language is utilized in several of the following requirements to exchange information on the obligations.

4. Obligations should be available in an unambiguous formalization and thereby their respective contents should be both machine interpretable and easily comprehensible, in particular for users.
from use cases 1 to 5

5. A negotiation protocol exchanging the supported and utilized obligation and providing a mechanism to resolve non-matching obligations. *from use cases 1, 2, 3 & 5*

This negotiation protocol could be done between a PEP and PDP or between different entities of a distributed decision framework. An authorization decision containing unsupported obligations may result into an unintended behaviour of the PEP (e.g. denying an access which based on the decision should be permitted).

6. The enforcement framework should support mechanisms to enforce obligations in conjunction with an access requests.
from use cases 1 to 5

This requirement ensures that an obligation has to be enforced although the actual access request was denied. The actual point of time when the obligation is enforced may be specified in addition.

7. An obligation may specify when in relation to the access to the data it has to be enforced, i.e. **before**, or **after** the access (either immediately or with a well specified delay), or **during** which is either before or immediately after the access.

The last case that the obligation is enforced during the access may be equivalent to the case that no point of time is actually specified.

8. An obligation may specify the physical or logical entity at which it should be enforced.
from use case 4

This entity might be one which could not be modified and is used for audit purposes.

9. The enforcement framework should *support cross-domain* enforcement of obligations
from use cases 2 & 5

This cross-domain enforcement is not only required in case of distributed decision points, but already if the PEP and PDP are under different organizational control.

10. The enforcement framework should support the enforcement of obligation independently from the underlying policy language.
from use cases 2, 3 & 5

Different sets/types of obligations with regard to the time of enforcement (i.e. before, during or after user's access to protected resource) and the independence from the underlying language model (e.g. XACML, P3P or Sticky-policy).

11. The obligation enforcement framework should provide mechanisms to integrate various trust mechanisms and utilize them in an abstract way.
from use cases 1 to 5

The result of the trustworthiness evaluation of both SP and user should be considered as input for the obligation enforcement. Thereby the trustworthiness evaluation may be achieved by relying on different trust models/ technologies. But the actual interface to retrieve this information should be independent of the underlying mechanism.

12. The enforcement framework should define mechanisms that improved the transparency of data processing, e.g., privacy-aware logging of data-handling processes.
from use cases 2 & 3

While obligations are not limited to these obligations, privacy aware logging is an important issue.

13. It must be ensured that specified/negotiated and subsequently exchanged obligations cannot be manipulated (and if required not accessed) by non authorized entities.
from use cases 1 to 5

6.2 Enforcement Point requirements

14. A PEP should be able to provide the list of obligations it is able to enforce (based on a general description language)
from use case 1, 2, 3 & 5

This list of obligations could be compared with those used in the policies, enabling an early detection of unsupported obligations. Thus unintended default behaviours of the PEP like those specified in [i.2] and [i.3] could be avoided.

15. A method to attach obligation to responses on attribute requests or to response of a method call.

These attached obligations could be send in conjunction with the responses of attribute requests, and have to be enforced by the receiver.

6.3 Management Requirements

16. A PAP should be able to provide the list of obligations which may be contained in the stored policies (based on a general description language)
from use case 1 & 5

With this list the decision point could create a global list of all obligations which may show up in the responses it is providing.

6.4 Obligation Requirements

17. A PDP should be able to provide the list of obligations which may be contained in the responses to an access request (based on a general description language)
from use case 1 & 5

This list of obligation could be compared with those supported by the PEP enabling an early detection of unsupported obligations.

18. The type of data which are covered by an obligation should be explicitly known by or visible to the entity that is subject to it.
from use cases 2 & 3

19. The enforcement framework must support mechanisms to determine the entity requiring an obligation to be enforced, as well as the entity bound to fulfil the obligation if this is requested by either the managing or the enforcing entity.
from use cases 2 & 3

6.5 Distributed Decision Point requirements

20. A distributed access control entity sending access request should provide the list of obligations which itself or underlying layer are able to enforce (based on a general description language)
from use case 1, 2, 3 & 5

21. A distributed access control entity receiving access request should provide the list of obligations which may be contained in the responses to an access request originating from its own policies or requests its sending out itself (based on a general description language)
from use case 1 & 5

A distributed access control entity has to provide the supported obligations of the PEP to all peers and provide a complete list of the used obligations of the "underlying" peers.

7 Conclusion

The present document has presented a set of user cases of a distributed enforcement framework covering important aspects like privacy in a cloud environment, location based services for enterprises, and social network services. In addition the importance of specifying the location where an enforcement should take place and the need for a dynamic obligation specification has been illustrated by use cases.

Based on these use cases the necessary requirements especially for a distributed environment have been identified, grouped into different categories. These requirements could be fulfilled by existing frameworks, except perhaps for some single requirements. A framework which should provide a solution for a distributed enforcement framework has to fulfil all or at least most of the given requirements.

In working item 2 [i.1] the requirements of a distributed access control framework have been identified which are in general complementary to those given in the present document. Nevertheless, based on these two set of requirements reference architecture has to be develop which provides a potential solution for a distributed access control and enforcement framework for networks and services.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteur:

Dr. Mario Lischka, NEC Europe Ltd.

Other contributors:

Dr. Kpatcha Bayarou, Fraunhofer SIT.

Dr. Antonio F. Gómez-Skarmeta, University of Murcia.

Alejandro Pérez, University of Murcia.

Hervais Simo Fhom, Fraunhofer SIT.

History

Document history		
V1.1.1	March 2011	Publication