On the Usage of SAML Delegate Assertions in an Healthcare Scenario with Federated Communities*

Massimiliano Masi[1,2] and Roland Maurer[1]

[1] Tiani "Spirit" GmbH, Guglgasse 6, Gasometer A - 1110 Wien, Austria
http://www.tiani-spirit.com
[2] Università degli Studi di Firenze, Viale Morgagni, 65 - 50134 Firenze, Italy
{massimiliano.masi,roland.maurer}@tiani-spirit.com

Abstract. The importance of the Electronic Health Record (EHR) has been addressed in recent years by governments and institutions. Many large scale projects have been funded with the aim to allow healthcare professionals to consult patients data in different organizations. Concepts like interoperability, security and confidentiality are the key for the success for these projects. The Integrating the Healthcare Enterprise (IHE) initiative promotes the coordinated use of established standards for authenticated and secure EHR exchange amongst clinics and hospitals or even regions. For these scenarios, the problem of having authenticated transactions is crucial, in order to provide a form of authorization while accessing patient healthcare information. The IHE initiative addresses the problem by mean of SAML assertions, i.e. XML documents containing authentication statements. In this paper, we focus on the problem of propagating the authentication information of healthcare professionals amongst hospitals or regions (in the IHE jargon, *communities*) by relying on the delegation mechanism introduced by SAML.

Keywords: Healthcare Professionals Authentication, Direct Brokered Trust, Security.

1 Introduction

The secure exchange of patient healthcare information amongst clinics and hospitals is becoming a crucial task due to the numerous initiatives introduced by governments and institutions in recent years [2,3,4,5,6].

The Integrating the Healthcare Enterprise (IHE) [7] is a worldwide initiative founded for promoting the coordinated use of established standards (see e.g. [8,9]) to improve information sharing in an healthcare scenario. In particular, the IHE profiles named XUA, ATNA and BPPC are voted to address the problem of security, authentication and authorization, by exploiting a Service

* A full version which provides a larger explanation and details of the research conducted is available online [1].

M. Szomszor and P. Kostkova (Eds.): E-Health 2010, LNICST 69, pp. 212–220, 2011.

Oriented Computing (SOC) approach and adopting OASIS standards, such as SAML [10], ebXML [11] and WS-Trust [12].

The IHE initiative introduces the concept of *communities*, a set of healthcare facilities such as hospitals and clinics that cooperate together for exchanging healthcare data. Examples of communities are regions, federated hospitals or even countries. A community is uniquely identified by a *gateway*, a software entity responsible for the exchange of data with other communities, as described in the IHE XCA [13] profile.

The authentication of healthcare professionals is one of the basic requirements for the access of person related health data. The IHE profile XUA makes use of SAML authentication assertions for propagating the identity of the user. A SAML assertion is a signed XML document issued by the *identity provider*, a service able to attest the identity of an user and to create authentication statements by relying on an underlying mechanism (i.e. Kerberos).

The application of XUA in a cross community scenario introduces issues that a security architect needs to address for providing optimum patient care, i.e. for applying access control policies.

In order to perform a transaction that crosses the border of a community, the SAML assertion obtained by the local identity provider has to pass through the gateway that "forwards" the authentication claims to the remote services.

However, impersonation and forwarding must be avoided especially in service oriented computing because only stateless end to end messages are permitted. In fact, before performing any cross community transaction, the gateway needs to act *on behalf* of the real user. The information about the user must be forwarded to the remote community by the gateway. This is covered also by OASIS as *direct brokered trust* [12,14].

The main contribution of this work is to provide a solution for the problem of using IHE XUA in a cross community scenario (also called *federated* scenario). Our solution is based on the use of SAML *delegate* authentication assertions [15]. We show that our solution does not affect any existing standard and we demonstrate our experience in a pilot project running in an Austrian region.

This work is structured as follows: in Section 2 we first briefly revise the details of the healthcare security standards, XCA, XUA and SAML. In Section 3 we describe our solution to the problems introduced by the usage of delegate assertions in the federated healthcare scenario and in Section 4 we touch upon the future and related work and we conclude.

2 Communities

The basic IHE patient healthcare data exchange pattern is based on an ebXML [11] model, called Cross Enterprise Document Sharing (XDS) [7]. This specification consists of four actors, a document *source* that creates documents for the patient (e.g. using Clinical Document Architecture (CDA) [8]), a document *consumer*, i.e. a workstation that displays healthcare documents to the professional, a document *repository* that provides storage for the binary documents and finally a document *registry*, using the ebXML catalogue for indexing documents metadata.

In the IHE model all services sharing the same registry instance are logically classified as an *affinity domain.* A set of affinity domains cooperating together to exchange documents is identified as a *community.* Communities are uniquely identified by a service, called *gateway*, that acts as a proxy (i.e. it intercepts all the messages that are travelling amongst communities). It is worth noticing that from a functional point of view a community can be established not only by federating affinity domains but also any kind of healthcare related software that uses a gateway for accessing data can be abstracted as a community itself, if the gateway observes the behavior defined by [7]. An example of a community built upon a Computing GRID is shown in [16].

When a client service (a document consumer or a source) needs to perform a *cross gateway query* (i.e. to query for document metadata in a foreign community) it contacts the local gateway (that is called *initiating* gateway) that creates a message which is sent to all known foreign gateways (named *responding* gateways) where patient health information has been discovered using a patient identification service [7]. The reason for that is that it could be unknown in which community the document related to the searched patient is stored.

In order to be able to perform a successful query, the patient identifier is obtained by the initiating gateway using the IHE XCPD mechanism [17]. The Cross Community Patient Discovery (XCPD) profile supports the ability to locate communities which hold a patient's relevant health data and the translation of patient identifiers across communities holding the same patient's data. The XCPD service can be hierarchical: each community can have its own XCPD service consulting the local patient index or it can exist a topmost service able to contact the community's patient indexes. For the sake of simplicity in this work we consider the last option, where a centralized XCPD service contacts the local patient indexes.

3 Applying Security

The IHE security model is driven by the Audit Trail and Node Specification profile. Each machine containing and transmitting healthcare data must possess an X.509 certificate and a private key attesting the identity. Access to data must be permitted only to clients using audited XDS transactions secured by means of TLS communication channels.

The Security Assertion Markup Language (SAML) [10] used by XUA, is an OASIS standard that defines the exchange of security statements using signed XML documents called *assertions*, playing the role of security tokens. SAML introduces a new actor, called *identity provider*, responsible to attest the identity of an user based on an authentication procedure performed by an underlying authentication mechanism (such as Kerberos) for a *Subject.* The SAML assertion contains an element called `AudienceRestriction` where the list of services where the token can be used is specified. Notably, this element should

Table 1. The delegate assertion usage protocol

$A \rightarrow I$	:	$A, \mathit{msgId1}, I, \{[RST(\mathit{user}, \mathit{role}, \mathit{org}, B, C)]\}_{K_A^-}$	(1)
$I \rightarrow A$	:	$I, \mathit{msgId2}, \mathit{msgId1}, A, RSTR(\{[I, \mathit{role}, \mathit{org}, \{u_{id}\}_{K_B^+}, \{u_{id}\}_{K_C^+}]\}_{K_I^-})$	(2)
$A \rightarrow B$	:	$A, \mathit{msgId3}, B, \{[I, \mathit{role}, \mathit{org}, \{u_{id}\}_{K_B^+}, \{u_{id}\}_{K_C^+}]\}_{K_I^-}, \mathit{XDSData}$	(3)
$A \rightarrow C$	:	$A, \mathit{msgId4}, C, \{[I, \mathit{role}, \mathit{org}, \{u_{id}\}_{K_B^+}, \{u_{id}\}_{K_C^+}]\}_{K_I^-}, \mathit{XCAData}$	(4)
$C \rightarrow I$	:	$C, \mathit{msgId4}, I, \{[I, \mathit{role}, \mathit{org}, \{u_{id}\}_{K_B^+}, \{u_{id}\}_{K_C^+}]\}_{K_I^-}, RST(\mathit{remgw})$	(5)
$I \rightarrow C$	:	$I, \mathit{msgId4}, \mathit{msgId5}, C, RSTR(\{[I, \mathit{role}, \mathit{org}, \{u_{id}\}_{K_{remgw}^+}]\}_{K_I^-})$	(6)

be always included in the assertion. In [18] a security flaw is shown because of the lack of the audience restriction element. The interaction is made by using WS-Security [19] for embedding the token into each IHE transaction managing health data. The contacted *service provider* uses the assertion for authenticating the requester. SAML subjects can be confirmed with the method listed in the `SubjectConfirmation` element. It is worth noticing that IHE does not define a structure of the token neither a method for obtaining it which could result in potential weak and insecure implementations. We assume a secure token issuance process as in [20].

In our federated scenario, the application of the IHE security model is not straightforward. The user first authenticates using the local identity provider (located in the healthcare facility, affinity domain or community) for enabling authentication in transactions performed within the community (i.e. an XDS transaction from a document consumer to the registry). When the authentication process begins, the client service needs to specify the list of recipients to be placed in the `AudienceRestriction` element. Notably, the list of possible responding gateways could be unknown by the client.

At this stage the identity provider is allowed to encrypt data (e.g. the user identifier [10], or as in [20] the WS-Trust issuing context identifier). Under these assumptions, the SAML assertion issued by the local identity provider for the usage with the local services cannot be used for performing any cross gateway transaction. A high level overview of the motivating scenario is shown in the Table 1[1]. The notation, commonly used to describe security protocols is as follows. $\{M\}_{K_A^+}$ stands for the encryption of message M using the public key of A and $\{[M]\}_{K_A^-}$ for the signature of M using As private key (where $[M]$ is the hash code of M). $\mathit{ts}, \mathit{ts}, \mathit{ts1}$ and $\mathit{ts2}$ are timestamps.

In step 1, the consumer named A requests a SAML assertion with the local username *user* to the identity provider I by passing its name, A, a message

[1] In order to ease the readability of the article, at this stage we assume that every message is travelling along secure and authenticated channels. We do not introduce here additional signatures checks that are out of the scope of this work.

identifier $msgId_1$ and the address I, that represents the WS-Addressing elements `From`, `MessageID` and `To` respectively. The SOAP Body of the message contains a signed request security token (RST) where the client application sends the requested user, role and organization. The last two values, B and C are the endpoints of the registry and the initiating gateway where the assertion will be used. The identity provider validates the message and issues the SAML assertion. In a scenario with federated identity providers the subject of the assertion is a newly created pseudonym, as defined in [10]. This new SAML subject, u_{id}, is encrypted for the endpoints requested. The response message (step 2) has a new message identifier ($msgId_2$) and the old message identifier, as `RelatesTo` WS-Addressing element. At this stage (step 3) the consumer A uses the obtained SAML assertion for contacting the registry (B) and the initiating gateway (C) (step 4). Both services are able to decrypt the value of the username. The representation of the assertion is the signed tuple $\{[I, role, org, \{u_{id}\}_{K_B^+}, \{u_{id}\}_{K_C^+}]\}_{K_I^-}$.

3.1 The Delegate Assertion

In our model, the layout of the identity assertion is given by [21,6]. The assertion contains the *role*, the *institution*, the *username* and the *purpose of use* of the requester (i.e. the doctor). In order to send audit trails with the correct subject and to use attributes to enforce access control policies, it is important for the remote site to attest the digital identity including the attributes of the user that is requesting health data.

As we can derive from the counterexample shown in Table 1, the responding gateway of the foreign community does not share the public keys (K_B, K_C). Thus it can't decrypt the `EncryptedID` value of the SAML assertion that is forwarded by the initiating gateway. This is a common problem when an entity needs to perform brokering of security tokens. There are several trust models [14] covering this case. The model that we use is the *direct brokered trust*: the responding gateway of the foreign community trusts the initiating gateway of the local community that vouches for the document consumer of the local affinity domain.

When the document consumer needs to perform a cross gateway query, it contacts the initiating gateway with the SAML assertion containing the local subject. In order to establish the direct brokered trust in cross community transactions, the initiating gateway needs to vouch for the document consumer with the responding gateway in the foreign community.

Since the attributes as defined in [21] for attesting the digital identity of the requesting subject (i.e. the doctor sitting at the document consumer) are defined in the local authentication assertion, the initiating gateway requests a new assertion, using the local SAML authentication assertion as authentication statements against the identity provider. In this way, the identity provider validates the local SAML assertion and issues a new token containing the original attributes such as role and organization. The subject of the assertion becomes the endpoint of the initiating gateway.

This behavior is shown in steps 5 and 6 of Table 1. The initiating gateway C sends a request security token to the identity provider using the assertion as authentication statement and the address of the remote gateway as list of service where it intends to use the assertion. The identity provider validates the request, validates the assertion and issues a new one used by C for any cross community transaction (step 6), by also contacting the pseudonym service, if needed.

In order to establish the brokered trust, we adopt the SAML delegation mechanism [15]. The `Conditions` element of the new delegate assertion is enriched with the `DelegateRestrictionType`, containing two values: the instant when the identity provider delegated the initiating gateway to act on behalf of the user and the subject of the assertion. The SAML condition element becomes

```
<saml:Condition
  xmlns:del="urn:oasis:names:tc:SAML:2.0:conditions:delegation"
  xsi:type="del:DelegationRestrictionType">
  <del:Delegate
  ConfirmationMethod="urn:oasis:names:tc:SAML:1.0:cm:sender-vouches"
  DelegationInstant="2010-05-13T12:50:30.846Z">
    <saml:NameID>drmasi@hospital.at</saml:NameID>
  </del:Delegate>
</saml:Condition>
```

When C requests the assertion all the endpoints are known and thus it can also request new encryptions for a new list of audience restrictions. The UML sequence diagram of the new scenario is depicted in Figure 1. The `AudienceRestriction` element of the delegate assertion now contains the list

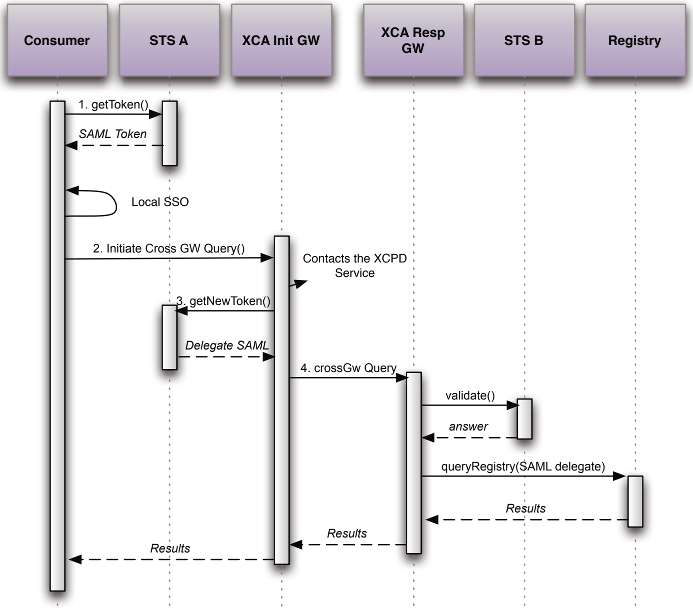

Fig. 1. The cross community query with delegation. Communities are named A, B.

of the web service endpoints of the known gateways of the other communities and the topmost XCPD service. The patient identifier discovery transaction is also authenticated using the delegate assertion. Notably if there is no topmost XCPD service, the `AudienceRestriction` list shall contain all the web services endpoints of all the XCPD services in all communities.

We used our solution in the e-Care pilot project in an Austrian region (presented at the IHE Connectathon 2008 [22]). In this pilot three hospitals need to cooperate together to exchange the EHR of the patients. Hospitals are identified as communities. A requirement of the project is to enforce a patient consent at the remote site (i.e. a policy) which the patient has given at the hospital where she is receiving treatment. For this reason when the initiating gateway performs a cross hospital transaction, it obtains the SAML delegate assertion and another treatment-related assertion that contains the encrypted local policy. Initiating gateway uses the delegated assertion to perform the patient discovery transaction. When the patient is found (and the community containing data is found) initiating gateway sends the delegate assertion and the treatment assertion containing the policy encrypted for the responding gateway. The access control methodology is XACML-based and the access request is built upon the attributes of the delegated assertion and on the document metadata (the *resource*). The responding gateway grabs the policy from the encrypted assertion and performs a XACML flow, by importing also local policies.

4 Conclusions

We presented our experience on the application of SAML delegate assertions in an healthcare scenario as defined by the IHE standards. Specifically we considered a scenario including a number of communities, a set of healthcare facilities cooperating together exchanging data over gateways. We proposed the usage of the OASIS brokered trust model where the initiating gateway obtains a new authentication assertion on behalf of the real user operating in the local community. We provided a methodology for the exchange of the user attributes over cross community transactions in order to give to the remote gateway the possibility to authenticate and to enforce local or remote access control policies.

Our proposal fits well whenever the access control methodology is based on XACML [23] and the access request's subject is obtained from the attributes of the authentication assertion sent along the transaction.

We implemented our proposal using web service technologies such as WS-Security [19], WS-Trust [12], SAML profile for XACML [24]. A prototypal version of our software is running in a pilot project connecting three hospitals (communities) in an Austrian region and it will be extended to a governmental level in Austria. An STS capable of issuing the assertion with the proposed layout is available at `http://office.tiani-spirit.com:41081/SpiritIdentityProvider/listServices`. We provided a full version of this work that includes the layout of the delegated assertion and a formalization of the motivating example. More information can be found in [1]. Our solution is under discussion at the time of writing as default methodology for propagating security claims on the eHR project in South Africa [4].

Related and Future works: To the best of our knowledge, there are no known relevant works related to the usage of SAML delegate assertions. In the european project epSOS [3], the information about the local subject is propagated by placing it in an attribute as in [21] which does not follow the emerging SAML standard [15]. The Liberty Alliance Project [25] proposes a set of specifications that covers the problem of brokering trust. However these specifications have not been selected by IHE. The access control methodologies are defined by the IHE White Paper on Access Control [26]. The usage of XACML in conjunction with attributes [21] is recommended, as in our case.

To simply adopt WS-Security, WS-Trust and SAML does not guarantee absence of security flaws. Hence, due to the complexity of the healthcare applications we plan to provide a formal methods-based analysis in the near future in order to investigate on the absence of flaws such as rewrite or protocol attacks.

References

1. Masi, M., Maurer, R.: On the usage of SAML delegate assertions in an healthcare scenario with federated communities (full version). Technical report, DSI, Univ. Firenze - Tiani Spirit, Wien (2010), `http://rap.dsi.unifi.it/cows`
2. ARGE-ELGA: Die Österreich Elektronische Gesundheitsakte (2008), `http://www.arge-elga.at`
3. The epSOS project: a European eHealth Project (2010), `http://www.epsos.eu`
4. The South African Department of Health: the EHR project in South Africa (2009), `http://southafrica.usembassy.gov/root/pdfs/pepfar-hmis-docs/ndoh-e-hr-for-south-africa.pdf`
5. GIP DMP: Dossier Médical Personnel (2009), `http://www.d-m-p.org`
6. The Nationwide Health Information Network (NHIN): an American eHealth Project (2009), `http://healthit.hhs.gov/portal/server.pt`
7. The IHE Initiative: IT IT Technical Framework (2009), `http://www.ihe.net`
8. Health Level Seven organization: Hl7 standards (2009), `http://www.hl7.org`
9. ACR-NEMA: Digital Imaging and Communications in Medicine (DICOM) (1995)
10. OASIS Security Services TC: Assertions and protocols for the OASIS security assertion markup language (SAML) v2.02 (2005), `http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf`
11. OASIS/ebXML Registry TC: ebXML business process specification schema technical specification v2.0.4. (2006), `http://www.ebxml.org`
12. OASIS Web Services Security TC: WS-Trust 1.3 (2007), `http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf`
13. Witting, K.: Cross Community Access profile (2008), `http://wiki.ihe.net`
14. OASIS Web Services Security TC: Trust Models Guidelines (2004)
15. OASIS Web Services Security TC: SAML V2.0 Condition for Delegation Restriction Version 1.0 (2009), `http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-delegation.html`
16. Masi, M., Meoni, M.: Using Integrating the Healthcare Enterprise (IHE) profiles for an healthcare DataGRID based on AliEn. In: Emmit, AITIM (2008)
17. IHE Technical Committee: XCPD (2009), `http://www.ihe.net`

18. Armando, A., et al.: Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps. In: FMSE. ACM, New York
19. OASIS Web Services Security TC: Ws-security: SOAP message security (2006), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
20. Masi, M., Pugliese, R., Tiezzi, F.: On Secure Implementation of an IHE XUA-Based Protocol for Authenticating Healthcare Professionals. In: Prakash, A., Sen Gupta, I. (eds.) ICISS 2009. LNCS, vol. 5905, pp. 55–70. Springer, Heidelberg (2009)
21. OASIS eXtensible Access Control Markup Language TC: Cross Enterprise Security and Privacy Authorization Profile for XACML for healthcare (2009), http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-os.html
22. Aichinger, B.: e-Care project presentation (2008), http://www.ihe-austria.at/fileadmin/user_upload/CAT2009/documents/IHE_CAT09_WSProgram_englisch.pdf
23. eXtensible Access Control Markup Language TC v2.0 (XACML): Extensible access control markup language (XACML) version 2.0 (2005), http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-NORMATIVE.zip
24. eXtensible Access Control Markup Language TC v2.0 (XACML): SAML 2.0 profile of XACML v2.0 (2005)
25. The Liberty Alliance: Project Liberty (2010), http://www.projectliberty.org/
26. The IHE Initiative: IHE Access Control White Paper (2009), http://www.ihe.net