SECURING WEB SERVICES USING IDENTITY-BASED ENCRYPTION (IBE)

Kari Anne Haaland

Chunming Rong

Department of electrical and computer engineering, University of Stavanger, Stavanger, Norway

Keywords: Authentication, Authorization, Identity-based Encryption, open standards, and Web Service Security.

Abstract: There is obvious need in cooperation between organizations. A recent trend is cooperation online, which result in the need of facilitating and managing cross-domain access to information and applications. It is important to utilize open standards that leverage existing technologies instead of replacing them. WS-Security, emitted by OASIS, defines standards on how to encode security tokens. In this paper we look at the use of Identity-based Encryption to leverage the exchange of security tokens, and how it can be implemented with WS-Security. Identity-based encryption offers, compared to the more conventional PKI, some additional advantages. For instance: databases maintaining public-key certificates are now longer necessary, this simplify key management, saves space, and eliminate the threat of attacks on these databases. It is also more suitable to grant collective access to groups, and is therefore suited for role based access control. We do not suggest Identity-based encryption as a replacement, but rather a complementary.

1 INTRODUCTION

There is obvious need in cooperation between organizations, e.g. suppliers, distributors, and business partners. The recent trend is cooperation online, which results in the need of facilitating and managing cross-domain access to information and applications

In the early stage, each entity explicitly registered and authenticated all its external users. However, dynamic changing environment demands for more integrated solutions that offer seamless cross-domain access and interaction.

Traditional cryptographic systems show their limitation in terms of flexibility and manageability (Mont et al., 2003) to coop with organizations shift towards more and more complex structures, where peoples roles and permissions changes frequently.

Identity-based Encryption (IBE) (Boneh and Franklin, 2001) is an encryption system that makes an easy way to grant collective access to groups, thus integrates well with frequently change in users roles and permissions. It is based on the more conventional PKI, but with some additional advantages. The public key is an arbitrary string (e.g. role, name, email address etc.) Thus, databases to maintain public key certificates are no longer needed. This simplifies key management, saves space, and eliminates attacks on the certificate databases.

As different organizations already have, more or less, functioning technologies in place, it is preferred to leverage existing technologies instead of replacing them. It's important to utilize the advantages of open standards, and security that works across multiple heterogeneous systems.

WS-Security (Atkinson et al., 2002b), an open standard emitted by OASIS (Organization for the Advancement of Structured Information Standards), describes enhancements to SOAP messages to provide integrity, message confidentiality and single message authentication. It is part of the *web service security road map* (IBM Corporation and Microsoft Corporation, 2002), and defines standards on how to encode security tokens and include opaque encryption keys. It does not specify any specific type of token, but is designed to be extensible to support multiple security tokens. (E.g. X.509 Authentication Certificates and Kerberos tickets).

Anne Haaland K. and Rong C. (2006).
SECURING WEB SERVICES USING IDENTITY-BASED ENCRYPTION (IBE).
In *Proceedings of the International Conference on Security and Cryptography*, pages 413-418
DOI: 10.5220/0002103504130418

Together with other existing standards it forms a building block for other WSS-standards. **Figure 1**.

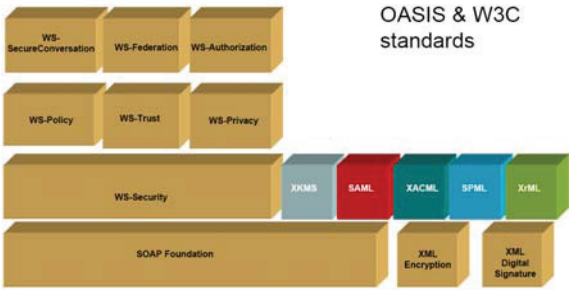

Figure 1: OASIS and W3C Standards.

In this paper we suggest IBE as a complementary technology to leverage cross-organization communication. The rest of the paper is organized as follow: First we give a general description on the use of security tokens before we look at IBE, its advantages, and how it can be used to form security tokens. Then we describe some related, existing technologies and give a discussion on the different methods advantages and disadvantages.

2 BASIC CONCEPTS

To utilise the advantage of cooperating, organizations need to inter-connect services. Our working case is a web-portal acting as a framework for gathering information and applications. E.g. a doctor at the hospital has, in his portal, a link to all cooperating public health centres, which give him access to all relevant information at the different health centres, without the need to re-authenticate. Authentication can either be *direct*; client and service are in a trust relationship, or by a *broker*; client and service do not share a direct trust relationship (Hogg et al., 2005) (Figure 2). Authentication is done by the Authentication Broker, which is trusted by both parts. A ”token”, containing information about the user (e.g. identity, role, privileges), is communicated to the Service.

When all parts are in the same trust-domain it is easy to establish trust between the Authentication Broker and the different services. However, entities situated in different domains may rely on different security mechanisms and policies to communicate tokens and establish trust relationships, and might not interpret each other’s tokens directly. Open standards, like WS-Security, aim to form an independent framework that describes how to securely communicate information across heterogeneous and distinct security domains boundaries.

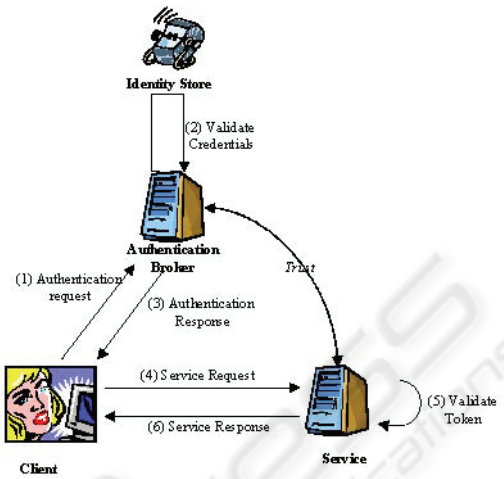

Figure 2: Broker authentication.

2.1 Evaluation Criteria

Cross-realm authentication is a decisive property. Establishing and revocation of access rights must be simple and easy to administrate.

Security: No unauthorized users should gain access to resources, or be able to impersonate a user, neither in its home domain nor in any remote domains. An adversary should not be able to delete, modify, or read any communicated information. Another important security issue is trust management, the willingness to rely on other entities to execute a set of actions or to make a set of assertions about a set of subjects (Anderson et al., 2005), e.g. trust authentication done by others.

Scalability: It should be easy to add new users to the system, and to integrate new cooperating organizations.

Transparency: When first authenticated in its home domain the user should not be aware of further cross-domain authentication.

Simplicity: It should be easy to use (we reckon that transparency implies simplicity for the user), and in addition easy to maintain and control. This we considered first and foremost a matter of implementation.

Applicability: Different authentication mechanisms focus on different targets and the applicability will depend on several factors, like size, number of cooperating companies, requirements to flexibility etc. Other properties may also come into account when considering best

solution. E.g. a mechanism that, in addition, offers secure communication and/or non-repudiation eliminates the need to consider other mechanisms and infrastructures to accommodate these facilities.

In the next section we demonstrate the use of IBE for broker authentication, and show how it can be integrated with WS-security to facilitate cross-domain authentication.

3 IBE FOR CROSS-DOMAIN ACCESS

In 1984 Shamir proposed the idea of Identity-based encryption (IBE), and in 2001 Boneh and Franklin presented on of the first practical IBE schemes (Boneh and Franklin, 2001). With IBE the public key can be any arbitrary string, e.g. the user's ID, the role name, the name of a group of users etc. Thus, IBE eliminates the need for large databases maintaining the correspondence between an identity and the related public key, which is needed in many PKI-based solutions, like X.509 Authentication Service. This simplifies key management, saves space, and eliminates threats related to attacks on the certificate-database.

As rolenames can represent the public key it also makes a good basis to collectively grant access to groups, and is suitable for RBAC. In (Mont et al., 2003) IBE is used for secure messaging in private health care, where messages are encrypted on a role-based level.

3.1 Basic Concepts of IBE

The public key of a user is an arbitrary string that uniquely identifies him. A Private Key Generator generates the corresponding private key, on demand. The scheme consists of four algorithms: (1) *setup* selects a master key and generates a public parameter, based on the master key; (2) *extract* uses the master key to generate the private key corresponding to the arbitrary public key ID and public parameter; (3) *encrypt* encrypts messages using the pubic key ID; and (4) *decrypt* decrypts messages using the corresponding private key.

3.2 IBE Broker Authentication

IBE has generally been used for encryption purposes, where the public key is used to encrypt the message. Her IBE facilitates authentication, i.e. instead of using the public key to encrypt messages the private key is used to sign requests.

A client wants to access a service. **Figure 3**. The client contacts the PKG and request a private key corresponding to his public key string ID <*e*>. If the client is authenticated and approved as the rightful 'user' of <*e*>, the PKG generates a private key and returns it to the client. Next the client sends a request for service, signed with the private key. (To assure confidentiality the request can be encrypted with the services public key string ID). The service uses the public key string ID of the use and the public parameter to validate the signature.

A valid signature confirms the clients ID, because he could not have signed the request without the proper private key.

The same token/private key can be used for all services within a security domain.

In IBE any string can serve as the decryption key. This has great beneficial when access permissions are based on other parameters than identity, e.g. role or group belonging. Some services allow anonymous access as long as the client can prove certain group belonging. E.g. academically institute that have access to different information databases. Client authenticates to the PKG, and request a private key corresponding to the public key string ID <AcademiaA>. Any request signed with this key proves his belonging to the given group.

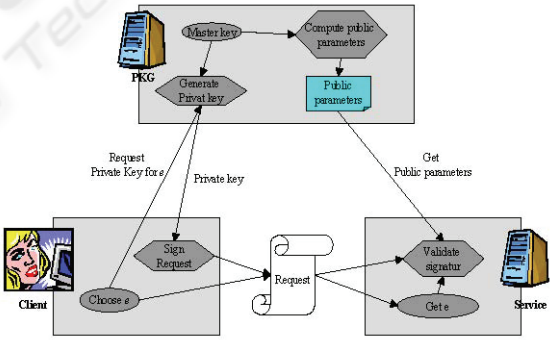

Figure 3: IBE Broker Authentication.

3.3 Cross-domain Cooperation

WS-Security defines a standard on how to exchange security tokens, and support multiple security token formats. As seen, IBE has its advantages and should be implemented with WS-security to facilitate cross-domain cooperation. Illustrated in **Figure 4**. A doctor, situated in a X.509 AS based domain (domain A), requests the Security Token Service (STS) in his home domain for a security token to access the STS in the target domain (domain B) (the

security token will typically be a public key certificate issued by the home domain STS). The target STS interprets and trusts certificates issued by the home domain, and responds with a private key corresponding to the public key string ID <doctor>. Access control at the public health centre is role based. A valid request assures that the requester is a doctor, thus he will get access to information based on this role.

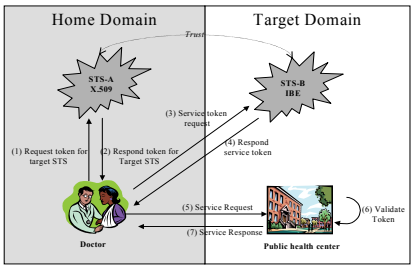

Figure 4: Cross-domain cooperation.

3.4 Requirements and Challenges

As the public key can be constructed of any arbitrary string, there needs to be a mutual agreement on how to construct and interpret uniquely identifying public string ID. E.g. the string < JohnSmith@orgA > does not hold if there exists two John Smith's in Org A.

A client may own several private keys (e.g. for different domains, or if the keys are based on other parameters then users ID). Thus, issues concerning key management and lifetime need to be taken into consideration. E.g., how long should a key be valid? A short lifetime means that the client often need to request a new key, while a long lifetime means that the client needs to keep track of all keys in his possession, and the keys need to be stored in a secure manner, to avoid theft.

The lifetime of the private key will also affect the need for revocation mechanisms. A short lifetime result in the key being invalid before there is a need to withdraw the key, while a long lifetime will need good revocation mechanisms.

If IBE is to be used for collective access to groups it is needed to determine whether it should be possible, and necessary to trace a group-members actions. This is a matter of different domains security policy.

The PKG has access to all private keys, and need to be *unconditionally trusted* (Menezes et al., 1996). To coop with this Al-Riyami and Paterson (Al-Riyami and Paterson, 2003) introduces Certificateless Public Key Cryptography (CL-PKC), where the private key is only partly generated by the PKG, but this solution have some security flaws(Zhang and Feng, 2005).

4 RELATED METHODS

(Atkinson et al., 2002a, Thurston et al., 2004) describe the integration of X.509 authentication certificates and Kerberos tickets with WS-security, but the standard is extensible to support other types of tokens as well. We suggest the integration of IBE, and in this section we give an overview of other central mechanisms, their advantages and disadvantages.

4.1 Kerberos

Kerberos (Fabrice, 2003) is based on symmetric key encryption, and authentication is done in three phases. (1) User authenticates to an Authentication Service (AS), with the use of a password, and obtains a credential (token) to be used to request access to other services. (2) User request authentication for a specific service. (3) The user presents the credential to the end server.

For a service to be able to validate a token it needs to exchange a secret key with the AS at prior. Thus, different entities need to know of each other in advance. Cross-domain access can be accomplished by having AS's in different domains trust tokens issued by each other, but negotiating cross-realm agreements can often be a lengthy and complex process and Kerberos is mostly used within a single administrative domain (Thompson et al., 2003).

4.2 X.509 Authentication Service

The X.509 Authentication Service (AS) (Stallings, 2003) is based on public key cryptography (PKC). Each user is assigned a private key that uniquely identifies the user. The corresponding public-key certificates are signed with the private key of a trusted certificate authority (CA) and associated with each user. The certificates are placed in a directory, for users to easy obtain certificates of other users.

X.509 suggests that CA's are arranged in a hierarchy, and in order to verify a certificate one needs to verify the whole certificate-chain. It is considered well suited for cross-organizations

operations, but establishing trusted CA relationships can be a lengthy process (Thompson et al., 2003)

4.3 PGP

PGP (Stallings, 2003) is, like X.509 Authentication Service, based on PKC. The main difference lies in the distribution of certificates. PGP is based on a *Web of trust*, rather than a certificate authority, for distribution of public keys and each user need to maintain it's own database of all communication partners. Thus, anyone can "certify" a key, and the different parts maintain their own key-list.

PGP originally evolved as a system for secure mail exchange between personal users. A main problem with this solution is that two parties need to know of each other (exchange certificates) before they can communicate, contrary to X.509 AS where users can "look up" each other's public key certificate in the dictionary.

4.4 X.509 Attribute Certificate

A X.509 attribute certificate (AC) (Chadwick et al., 2003) binds a set of attributes to its holder. It is based on X.509 authentication certificates, and has therefore many similar concepts. The certificates are organized in the same manner as X.509 Authentication Certificates, a trusted certificate authority issues attribute certificates.

Instead of binding an identity to a key, it binds a set of attributes (claims, roles etc.) to an identity. As AS's don't offer authentication they are generally used in combination with authentication certificates, or other mechanisms to identify the holder of the certificate. Validation of AC's chains can be complex and time-consumption (Knight and Grandy, 2002).

4.5 SPKI

SPKI (Liimatainen, 2005) is an authorization certificate system similar to AC. But, unlike AC, it does not have any centralized CA to whom all must trust. Instead the resource owner issues certificates holding permission-information to the resource. The certificate identifies who is allowed to access the resource, and further delegate permissions. Thus, permissions can be passed on to other uses. When requesting access to a resource the user sends all certificates to the owner of the resource. If they form a complete chain from owner to user, all certificates are valid, and give the required permissions, access is granted.

SPKI use a certification revocation list, which is checked every time a certificate is used, to manage expired certificates.

5 DISCUSSION AND CONCLUDING REMARKS

Open standard are decisive in cooperation between organizations, and should leverage on, rather then replace existing technologies.

OASIS has developed a standard framework on how to exchange, inter alias, security tokens. The standard does not require a specific type of token, but supports different tokens, like Kerberos tickets, X.509 certificates etc.

In this paper we have investigated the user of IBE for the exchange of security tokens, and in addition we have described, in short, other technologies of current interest. The different technologies have their advantages and disadvantages, which makes them more or less suited in different situations.

Kerberos, X.509 AS, and IBE all offer authentication facilities, in contrary to AC and SPKI that depend on the existent of a separate authentication mechanism.

Authentication in Kerberos is password-based, therefore vulnerable to dictionary attacks. The AS's list of passwords and symmetric keys is also an attractive point of attack, and needs to be stored securely.

PKI based solutions are generally considered as more secure. Certificates only need to be secured against modification while password-files need to be secured against both read and writes operations. However, the private key needs to be stored securely (e.g. on a smartcard or in the computer), and is less portable than a password.

X.509 Authentication Service and IBE also have better scalability capabilities then Kerberos. Different entities need not know of each other prior to communication, as long as they can form a valid chain of certificates back to a trusted root authority. However, asymmetric encryption is computationally intensive, and validation of certificate-chains can be complex and time-consuming if the certification chain grows long.

IBE offers some additional advantages compared to more conventional PKI, like X.509 AS. The public key can be any arbitrary sting and need not be distributed in a certification database. This saves space, simplifies key management, and eliminates

attacks on the certificate-database. It is only needed to verify the signature, in comparison with X.509 AS where both the certificate and the signature need to be validated.

Another benefit compared to X.509 AS is that there is no need to "look up" and validate the public key certificate of the receiving parts, as long as the public string ID is known. The public parameters are the same for all entities related to the same PKG, and only need to be fetched once.

On the other hand, the PKG has access to all private keys. It need to be unconditionally trusted, like the AS in Kerberos, and is suited for attack. The master key needs to be securely stored.

X.509 AS is based on users identity, and is well suited when access is based on identity. But in many cases, particularly in cross-domain cooperation, access permissions are based on roles and privileges rather than the users actual identity.

Attribute certificates and SPKI make an easy way to grant collective access for groups, and is therefore suited for RBAC. The main difference between the two technologies is the assigning of certificates, where AC relies on a certification authority while SPKI leave the issuing of certificates to the source-owner. IBE also makes a good basis for collective access to groups, as public key can be any arbitrary string (e.g. role-name), and is suited for RBAC. In addition, it offers authentication, thus need not rely on a separate authentication mechanism.

Although there have been some work on the security of IBE it is still in an early stage, and has not been 'attacked' to the same degree as more familiar technologies. Thus it is not as accepted as 'older' technologies, which have proven their security throughout several attempts of attack.

REFERENCES

Al-Riyami, S. & Paterson, K. (2003) Certificateless public key cryptography. Advances in Cryptology - Asiacrypt'03. Springer-Verlag.

Anderson, S., Bohren, J., Boubez, T., Chanliau, M., Della-Libera, G. & et al. (2005) Web Service Trust Language (WS-Trust). IBM.

Atkinson, B., Della-Libera, G., Hada, S., Hallam-Baker, P., Hondo, M. & et al. (2002a) Web Service Security Kerberos Token Profile OASIS.

Atkinson, B., Della-Libera, G., Hada, S., Hondo, M., Hallam-Baker, P. & et al. (2002b) Spesification: Web Service Security (WS-Security). IN KALER, C. (Ed.), IMB

Boneh, D. & Franklin, M. (2001) Identity-Based Encryption from the Weil Pairing. Lecture Notes in Computer Science, 2139, 213-240.

Chadwick, D., Otenko, A. & Ball, E. (2003) Role-based access control with X.509 attribute certificates. Internet Computing, IEEE, 7, 62-69.

Fabrice, K. A. H. (2003) Understanding Kerberos v5 authentication protocol. SANS institute.

Hogg, J., Smith, D., Chong, F., Taylor, D., Wall, L. & SLATER, P. (2005) Web Service Security Microsoft.

Knight, S. & Grandy, C. (2002) Scalability Issues in PMI Delegation. 1st Annual PKI Research Workshop.

Liimatainen, S. (2005) Usability of Decentralized Authorization Systems - A Comperative Study. System Sciences, 2005, HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on.

Menezes, A. J., Van Oorschot, P. C. & Vanstone, S. A. (1996) Trusted third parties and public-key certificates. Handbook of Applied Cryptography. CRC.

Mont, M. C., Bramhall, P. & Harrison, K. (2003) A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care. HP.

Stallings, W. (2003) Cryptography and Network Security, Prentice Hall.

Thompson, M. R., Essiari, A. & Mudumbai, S. (2003) Certificate-based authorization policy in a pki environment. ACM Transactions on Information and System Security, 6, 566-588.

Thurston, G., Siebenlist, F., Hughes, M., Reid, I. & et al. (2004) Web Service Security X.509 Certificate Token Profile. OASIS.

Zhang, Z. & Feng, D. (2005) On the Security of a Certificateless Public-Key Encryption. Cryptology ePrint Archive.