W3C Workshop on Next Steps for
XML Signature and XML Encryption

Position Paper

Abstract:
This paper is being submitted to further the practical and business applications of XML signature and encryption. Most development has occurred on the application and use of this syntax as a solution for authenticity, data integrity and non-repudiation of data between customers (B2B) and within a company's internal network. However our implementation and integration experience in developing an end-to-end solution (from a customer's back-end system to our systems) has shown gaps in the process; one of these implementation gaps exists when one of the parties is new to XML and, by extension, the XML security space. A second gap is an ever-evolving challenge within global and regulated industries like the financial sector. These industries face increasingly complex and regionally-focused legal, audit and compliance requirements. These requirements are also being mandated through a larger part of the financial payments and reporting supply chain. This paper will provide some background regarding these challenges and introduce some topics for further discussion.

Scope:

The challenges outlined above have been observed as part of an ongoing internal initiative by a large, multi-national financial institution to implement XML messaging and security. One of the many business-level banking solutions offered to customers is the ability to extend its payments supply chain to send payment with no customer intervention directly involving the bank (with one exception to be discussed later in this paper). A high-level architecture of customers using this functionality typically fall into three categories:

1. Customers that interact using the SWIFT network
2. Customers that utilize the bank's internally created and developed solution
3. Customers that develop their own solution referencing the financial institution's published requirements.

The scope of this discussion is limited to the category three customers, who have decided to develop a solution internally and are looking for the industry's best practices for guidance in this development.

Background

In order for a customer to send payments using their internal resources for development the "simplest" solution would be a common file format and a communication method. In this solution the bank would allows its customers the ability to transmit over the Internet the groups of domestic or international payments directly from the customer's ERP/AP system to the bank. The bank then routes the payment instructions to the appropriate countries for execution. However, the solution as described has inherent risks associated with it; namely, criminal activity including the ability for a user to execute payments (i.e. withdraw company funds) using the company's identity. To avoid this problem a third component of the solution was introduced; message security. The ability to provide authenticity, data integrity and support non-repudiation is critical for this third component. The bank currently utilizes the EDIFACT PAYMUL (D96A) and the EDIFACT AUTACK security message to meet these requirements[1]. Further development outside of this solution was extremely limiting until the development and acceptance of the XML signature syntax, which provided for a second "full service" solution.

B2B Customer Concerns:

The existence of a solution, though, is not enough for customers looking to develop the solution internally or by utilizing third-party software packages. The project manager and sponsor of integration projects involving a customer and a financial institution are typically from the business side (typically the Cash Manager or Assistant Treasurer) with technical resources a member of the project. Any proper project analysis will have a "buy vs. build" component to it very early in the project timeline. While communication and XML mapping/transforming tools exist in the marketplace currently our research has found no commercially available software available to customers to benchmark against during the "buy vs. build" phase of the project.

Compliance Concerns (Extensibility):

As mentioned above global financial institutions must meet complex and extensive auditing and reporting requirements in the countries payments are sent for execution, in the case of the referenced financial institution over 50 countries and growing annually. These requirements can be broken down into two broad categories; payment-related requirements and file-related requirements. Payment related requirements can include central bank reporting of payment instructions and information requirements for tax purposes. File-related requirements include audit trail of people/persons that have "signed" the file (i.e. responsible for generating the XML signature. This does not necessarily have to be a physical person, i.e. can be generated as part of an automated process. However flexibility in the standard should be present to include authorized signer information to be included in the syntax).

In addition companies are becoming increasingly global with different departments and subsidiaries existing in different regions of the world. For centralized payment factories and control this does not present a problem. An entirely feasible and popular solution is the automated insertion of the XML signature on an outbound payment file which is subsequently sent off to the financial institution for validation and execution. However another possible landscape requested by a customer could include the manual intervention and approval of a set of payment instructions. This manual intervention introduces the concern of authority of approval, i.e. only people/persons explicitly designated and authorized by the company should be allowed access to this approval process. The number of signers required to send a file to the financial institution along with the number of people authorized to sign a file must not only be carefully documented and but should also be recorded in the signature syntax. Thus an auditor or regulator is performing analysis on a XML file that has a signature should be able to determine the number of signers as well as which authorized signers actually signed the file.

Discussion Recommendations (Compliance and Syntax):

Further discussion is recommended to determine if the current XML syntax is flexible enough to handle various workflow scenarios around security and message authorization. One such scenario would be the creation of a XML signature as a response to a device (for example a SMART card and reader) authorizing the payment. The XML signature would then contain pre-determined characters identifying the person who authorized the payment. This logic can be extended to X number of users depending on the authorization workflow of the customer, creating X XML signature instances. From the decryption and verification side all XML signatures would need to be decrypted and verified successfully before processing of file can continue. Discussion of these scenarios and how the current syntax can handle them should be considered.

Discussion Recommendations (B2B Customers):

There is very little in the way of assistance for customers looking for rapid deployment of a XML and/or automated payment solution. A second recommendation is to discuss ways to ensure industry compliance with the XML security schema as well as interoperability of commercial software that will help customers solve their XML security needs. One possible model to follow is the interoperability requirements of software vendors implementing AS2[2]. AS2 was developed and accepted by the IEFT and business community; an independent, privately held company called the Drummond Group is "responsible for conduction interoperability and conformance testing and publishing related strategic research"[3]. While this paper (nor the author) does not take a position on the benefits or detriments to using a private or third-party for interoperability testing of standards, the recommendation is for further discussions regarding methods for ensuring a smooth and timely integration of not only XML security standards but of interoperability between any third party vendors that develop commercial software for the rapid adoption of XML security.

Submitters:

This paper was submitted by Chris Techter (chris.techter@abnamro.com) on behalf of ABN AMRO, a multi-national bank based in the Netherlands with US headquarters in Chicago.

References

1. These two messages are derived from the UNECE (United Nations Economic Commission for Europe) http://www.unece.org/trade/untdid/welcome.htm

2. RFC4130, http://www.ietf.org/rfc/rfc4130.txt

3. http://www.drummondgroup.com/html-v2/about.html