XML Signature in a real-life banking environment: Room for improvement?

Position Paper for the

W3C Workshop on Next Steps for
XML Signature and XML Encryption
26/26 Sept 07

Marcus Ertel

Marcus Ertel IT Consulting

1. Introduction

The new German money transfer standard (EBICS; Electronic Banking Internet Communication Standard; see [1]) uses XML Signature (XMLDSig; see [2]) as a part of its security features.

Not only because EBICS has the potential to become a European standard, it is essential that all its mechanisms be clearly defined and having no room for interpretation. This applies particularly to standards that are not defined within EBICS itself, but are used as a part of its functionality, such as XMLDSig. Otherwise, different implementations might suffer from incompatibilities between one another.

During the development of an EBICS client which uses third-party XMLDSig libraries, the issues described in this document arose. They led to elaborate and still ongoing discussions of ISV's with each other as well as with their customers.

2. Situation

This paragraph will give an overview of a Use Case of XMLDSig as well as a description of the problems caused by a certain lack of clarity within XMLDSig.

2.1 Use Case of XMLDSig

In EBICS, the XML Signature is calculated over several tags of an EBICS message. These tags bear the attribute „`authenticate=true`". The following code piece can illustrate this:

```
<ebicsRequest>
    <header authenticate="true">
        <static>
            <HostID>BLB</HostID>
            <Nonce>A168FBC6A28CB554606023625FA320CE</Nonce>
            <Timestamp>2007-08-14T05:34:42.236Z</Timestamp>
            (…)
        </static>
```

```
        <mutable>
            <TransactionPhase>Initialisation</TransactionPhase>
        </mutable>
    </header>
    (…)
    <body>
        <DataTransfer>
             <DataEncryptionInfo authenticate="true">
               (…)
             </DataEncryptionInfo>
            <SignatureData authenticate="true">
               (…)
            </SignatureData>
        </DataTransfer>
    </body>
</ebicsRequest>
```

2.2 The role of the XMLDSig Reference in EBICS

The data to be signed are selected by means of the Reference element's URI attribute ("`Reference URI`"). EBICS uses an `xpointer` for this purpose:

```
<SignedInfo>
    <CanonicalizationMethod Algorithm= …>
    <SignatureMethod Algorithm= …/>
    <Reference URI="#xpointer(//*[@authenticate='true'])">
          <Transforms>
                <Transform Algorithm= …/>
          </Transforms>
          <DigestMethod Algorithm= …/>
          <DigestValue> …
          </DigestValue>
    </Reference>
</SignedInfo>
```

It is important to note that the URI is part of the XML Signature itself and thus has to be handled properly before being signed or before validating a signature. As a consequence, if two implementations handle the URI differently, there will be different signatures that cannot be validated by an XML Signature validator with a different implementation.

3. Problem

XMLDSig says that the `Reference URI` – being an URI – has to be RFC 2396 compliant. This is the point where discussions start and different implementations are created.

According to XMLDSig, a `Reference URI` has the format "`anyURI`" which is defined as follows:

`anyURI` `represents a Uniform Resource Identifier Reference (URI). An` **`anyURI`** `value can be absolute or relative, and may have an optional fragment identifier (i.e., it may be a URI Reference). This type should be used to specify the intention that the value fulfills the role of a URI as defined by [RFC 2396], as amended by [RFC 2732].`

The RFC's 2396 and 2732 determine how a URI has to be handled (for details see 5.1), but unfortunately they are somewhat "blurry" because not all legal contents of a URI are completely defined.

The point is that it is not clear whether parts or all of the URI have to be escaped before building the XML Signature (NB: The `xpointer` itself is exchanged as it is; escaping takes place only when the XML Signature is being built.). As of today, there are two opposite positions regarding this issue (with some more opinions in between, leaning more or less to one of these two).

One of them says that the signed URI must remain unchanged:

```
"#xpointer(//*[@authenticate='true'])",
```

while the other one demands escaping which makes the URI look like this:

```
"#xpointer(%2F%2F*%5B%40authenticate%3D%27true%27%5D)"
```

The complete contents of XMLDSig can be found in [2] through [7].

For details of this ongoing discussion, please see the W3C mailing list [8].

A very good analysis of the situation can be found in [9].

As a result, the calculation of an XML Signature depends on the interpretation of RFC's and XMLDSig. The worst aspect of this situation is that it's not a question of right or wrong – which could be resolved rather easily – but both implementations are correct in terms of XMLDSig compliance. This applies particularly to developers of XMLDSig libraries; quite prominent examples of the a.m. contrary opinions are Apache XML Signature and IAIK XSECT prior to V1.11.

3.1 Repercussions

The result of this situation are software changes by "majority vote" or market pressure, but not by acceptance of the definitions of XMLDSig. This approach enables the interoperability of certain client-server pairs, but due to the lack of clearness there is no *commonly accepted* way to handle a `Reference URI`.

In a concrete case this means an "either-or" situation in terms of client products accessing the same server. With the advent of more and more EBICS based products, this situation will probably get worse.

4. Summary and Conclusion

EBICS is the first non-proprietary and publicly available Internet-based money transfer standard in Germany. Furthermore, it might become the transport standard for the upcoming SEPA system (Single Euro Payments Area; see [10]). This will yield a lot of implementations of client and server products which claim to support EBICS. While this might be true, the vendors of these products (could) have different opinions on the underlying XML Signature standard, hence being EBICS compliant while still doing things differently (and incompatibly).

Thus, with respect to EBICS and its role as a means of multi-bank money transfer standard, it is mandatory to clarify the background of XMLDSig in all its aspects. If this is not possible, the parts concerned by some vague or mistakable definitions should be officially replaced by newer standards and the old ones declared obsolete or, even better, forbidden.

If this fails, the process of using a worldwide accepted standard might fail, because in this case there is not one single standard, but multiple ones that claim to be the same. This might have a heavy impact on the European banking software industry, its customers and the banking clients willing to operate Europe-wide.

5. Appendix

5.1 Excerpts from RFC's

The following paragraphs contain what the RFC's say concerning URI handling:

RFC 2396

```
Reserved Characters
Many URI include components consisting of or delimited by, certain
special characters.These characters are called "reserved", since
their usage within the URI component is limited to their reserved
purpose.If the data for a URI component would conflict with the
reserved purpose, then the conflicting data must be escaped before
forming the URI.

reserved=  ";" | "/" | "?" | ":" | "@" | "&" | "=" | "+" |
           "$" | ","

The "reserved" syntax class above refers to those characters that
are allowed within a URI, but which may not be allowed within a
particular component of the generic URI syntax; they are used as
delimiters of the components described in Section 3.
```

RFC 2732:

```
This document updates the generic syntax for Uniform Resource
Identifiers defined in RFC 2396 [URL].It defines a syntax for IPv6
addresses and allows the use of "[" and "]" within a URI explicitly
for this reserved purpose.
The following changes to the syntax in RFC 2396 are made:
(...)
(3) Add "[" and "]" to the set of 'reserved' characters:

reserved= ";" | "/" | "?" | ":" | "@" | "&" | "=" | "+" |
          "$" | "," | "[" | "]"
```

5.2 References

[1] http://www.ebics-zka.de/english/document/pdf/Appendix%201-Spezification%20EBICS%20Version%202.2_04052007_EN.pdf

[2] http://www.w3.org/2000/09/xmldsig#

[3] http://www.w3.org/TR/xmldsig-core/#sec-URI

[4] http://tools.ietf.org/html/rfc2396

[5] http://tools.ietf.org/html/rfc2732

[6] http://www.w3.org/TR/xmlschema-2/#anyURI

[7] http://www.w3.org/TR/2001/WD-charmod-20010126/#sec-URIs

[8] http://lists.w3.org/Archives/Public/w3c-ietf-xmldsig/2007JulSep/

[9] http://lists.w3.org/Archives/Public/w3c-ietf-xmldsig/2007JulSep/0005.html

[10] http://www.ecb.int/paym/sepa/html/index.en.html