XML WORLD EURO EDITION

# XML Security: Security Designed for the Web


## Ed Simon
## Entrust Technologies


Entrust Technologies
We Bring Trust to e-Business™

# Outline

- What is XML Security?
- XML Signature and its applications
- XML Encryption and its applications
- Security service languages:
  XKMS, SAML, and XACL
- Summary

# DISCLAIMER!


This presentation contains forward-looking statements.

In fact, almost the entire presentation is “forward-looking” because it discusses incomplete, pre-version 1 specifications.

This presentation does NOT describe
“How do I do this today?”;
it describes
“**How might XML Security look tomorrow?”**

Entrust Technologies
We Bring Trust to e-Business™

# What is XML Security?


**XML Security** is the application of XML-aware security technologies

**XML Cryptography** will be used to refer specifically to “XML Signature” and “XML Encryption”.

These specifications design security protocols around XML and the way XML is, and is expected to be, used.

A design goal is to make adding security to XML-based applications as seamless as possible.

# What is XML Security?

## The "XML Signature" specification


**XML Signature** is a specification for creating and verifying XML-encoded digital signatures

A **digital signature** protects the integrity and authenticity of data; prevents the data from being changed and binds an entity (eg. a user) to the data

# What is XML Security?

## The "XML Encryption" specification


**XML Encryption** is a specification for encrypting and decrypting data, particularly XML-encoded data

**Encryption** protects the privacy of data; only specified users have access to data that has been encrypted

# Why develop new security technologies for XML?
## (Pre-XML security protocols)


Pre-XML security protocols view the data being secured solely as an opaque stream of bits

**...10110111001001010110101010011101100110110110 1...**

Adequate for binary and text* where every bit counts

*ignoring character encoding issues for the moment

# Why develop new security technologies for XML?

## (Pre-XML security protocols…)

Pre-XML security technologies CAN be used to secure XML data just as they can any other data.

XML Security technologies are designed
with XML,
and what people want to do with XML,
in mind.

Entrust Technologies
We Bring Trust to e-Business™

# Why develop new security technologies for XML?..

## (Top three reasons)

And so,

the **top 3 reasons** in reverse order for developing new security technologies for XML are...

Entrust Technologies
We Bring Trust to e-Business™

# Why develop new security technologies for XML?..

## (Top three reasons…)

**Reason #3:**

**Proliferation of XML-based protocols**

- XML is being widely adopted because it is both powerful and easy to work with
- XML makes it easy for single XML instance to include data from multiple namespaces and schemas; makes it easy to secure data according to its object class
- Expressing security protocols in XML helps overcome the development barriers (both technical and human) to integrating security into XML-based protocols

Entrust Technologies
We Bring Trust to e-Business™

# Why develop new security technologies for XML?..

## (Top three reasons…)

**Reason #2:**

**The Web environment**

On the Web, secure apps

- should be able to do as much as possible with commonly available Web tools
  (eg. XML parsers,
  HTTP, XSLT, etc.)
- should be able to use existing/upcoming Web technologies (eg. Context-specific queries)

Entrust Technologies
We Bring Trust to e-Business™

# Why develop new security technologies for XML?..

## (Top three reasons…)

**Reason #1:**

**XML's structure and semantics**

XML's structure and semantics make it possible to **secure specific parts** of an XML instance **according to what those parts are**

- semantics -- describes the meaning of the data
- structure -- shows the relationships among data

Entrust Technologies
We Bring Trust to e-Business™

# Quick example

**Suppose you have this:**

```
<Customers>
…
<Customer>
<Name>Jake Kidd</Name>
<CreditCard Type="VISA"
   Number="4500 0123 4567 8901"/>
</Customer>
...
</Customers>
```

and you want to sign just the **<Customer>** elements and encrypt just the **<Creditcard>** element's Number attribute

# Quick example

**With pre-XML-aware security technologies, the secured version looks like this**

```
MIIKfQYJKoZIhvcNAQcCoIIKbjCCCmoCAQExCzAJBgUrDgMCGgUAMIAGCDQEHAQAAoI
   IJBTCCAx8wggKIoAMCAQICBDJIZggwDQYJKoZIhvcNAQEFBQAwMTELMAkGA1UEBh
   MCQ...0ExEDAOBgNVBAoTB0VudHJ1c3QxEDAOBgNVBAsTB1IgYW5kIEQwHhcNMDA
   wODA3MTUyNDMxWhcNMDEwMjA3MTU1NDMxWjBWMQswCQYDVQQGEwJDQTEQ
```

None of the XML instance is usable directly by the application in its protected form.

Note: detached signatures do preserve the original plaintext but exclude any encryption, and the signature must be managed separately.

# Quick example

## But with XML-aware security, you get

```
<Customers>
...
<Signature xmlns="http://www.w3.org/Signature">
...
<Customer>
<Name>Jake Kidd</Name>
<CreditCard Type="VISA"/>
<EncryptedData xmlns="http://…/Encryption"
   Type="../@Number">Rg8I9…</EncryptedData>
</Customer>
...
</Signature>
...
</Customers>
```

- only the data that really needs to be secured is secured
- signed-only data stays intact whether signature is detached or not

# With XML-aware security protocols

Applications can:

- **conveniently** secure textual data with different character encodings
- use ubiquitous Web tools for secured data
- secure just the data that needs to be secured
- continue to take advantage of data's *unencrypted* structure and semantics

Entrust Technologies
We Bring Trust to e-Business™

# XML Cryptography

Taking a closer look at

- XML Signature
- XML Encryption

We Bring Trust to e-Business™

# XML Signature

- XML-based protocols began to include disparate ways of representing a digital signature in XML
- Standardization work began in early 1999. Approaching W3C Candidate Recommendation status
- Makes it easy for applications to sign one or more resources located on the Web
- Usable with standard Web technologies. eg. Search engines don't need to do anything special in order to index XML Signatures

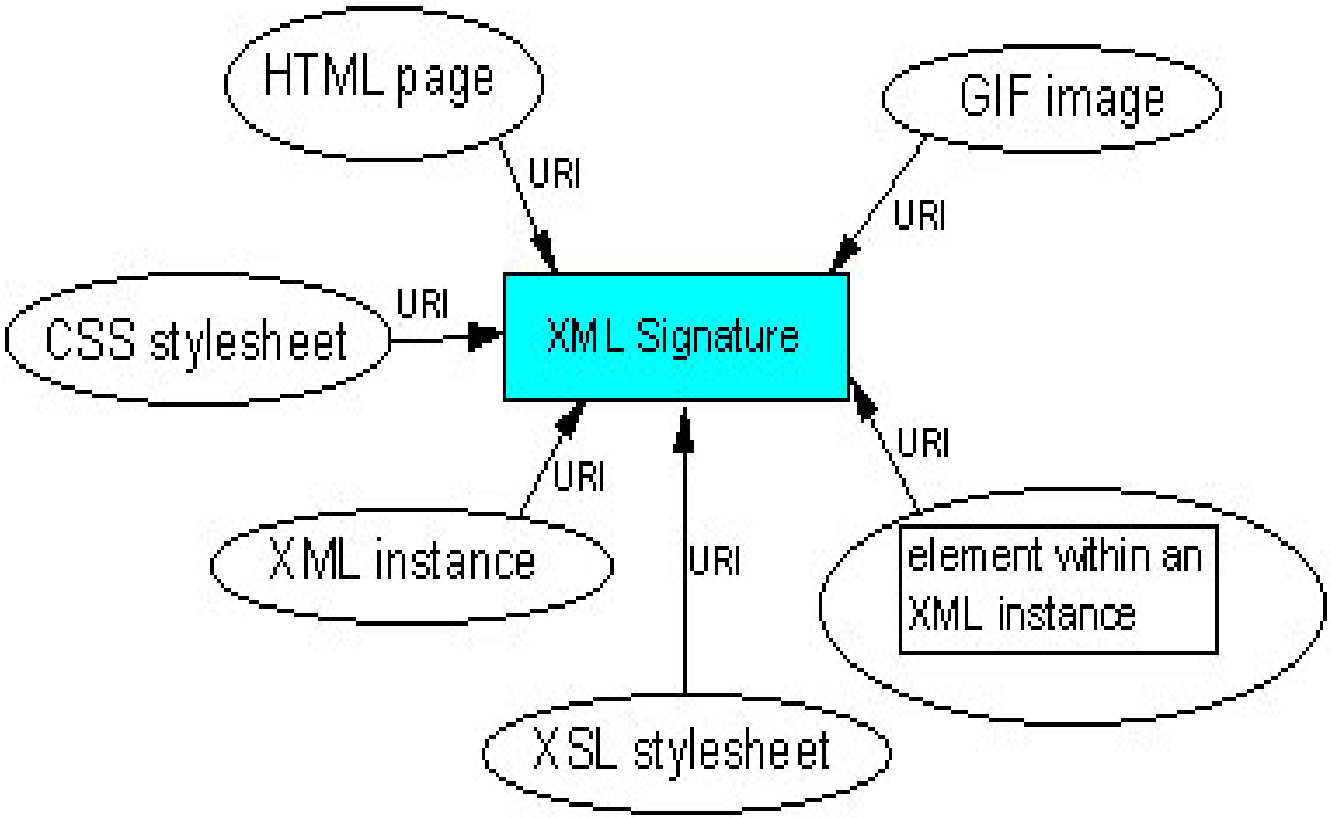
# XML Signature:
## Canonicalization/serialization


In XML, data is abstracted to a higher level and the way XML encodes data means data with the **same structure and semantics** can **have different binary representations**

Require a digital signature to **reliably** sign the structure and semantics of XML instances to prevent false negatives

# XML Signature Example 1

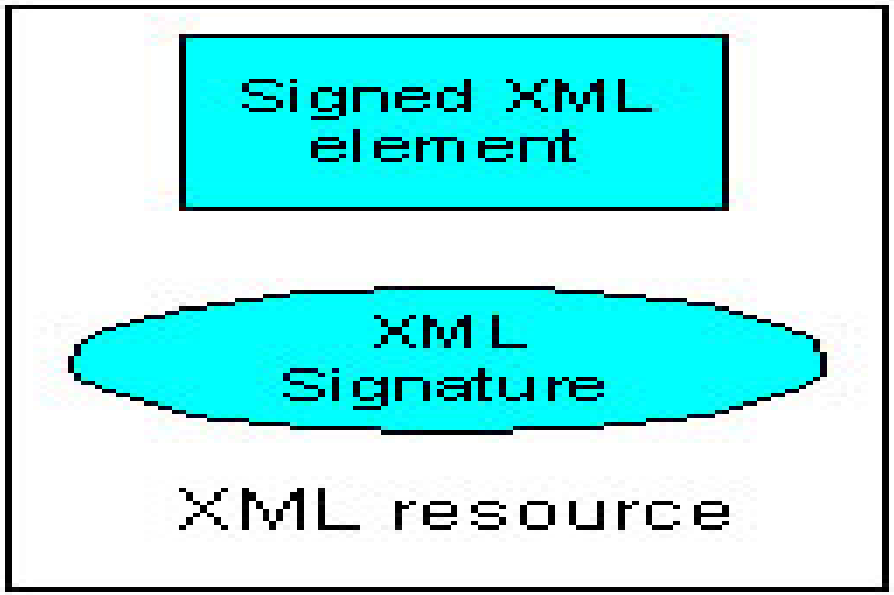
An XML Signature can point to one or more Web resources through Uniform Resource Identifiers (URIs).




We Bring Trust to e-Business™

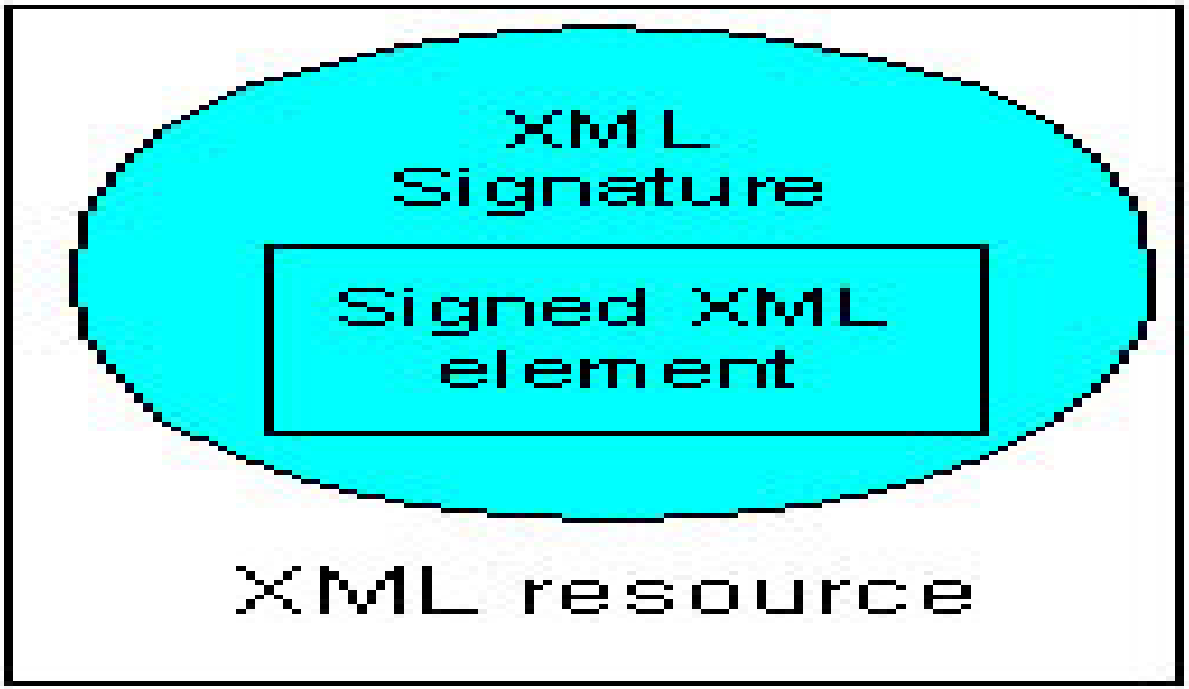
# XML Signature Example 2

An XML Signature can reside in the same resource as the signed XML object(s) but be separate from them.



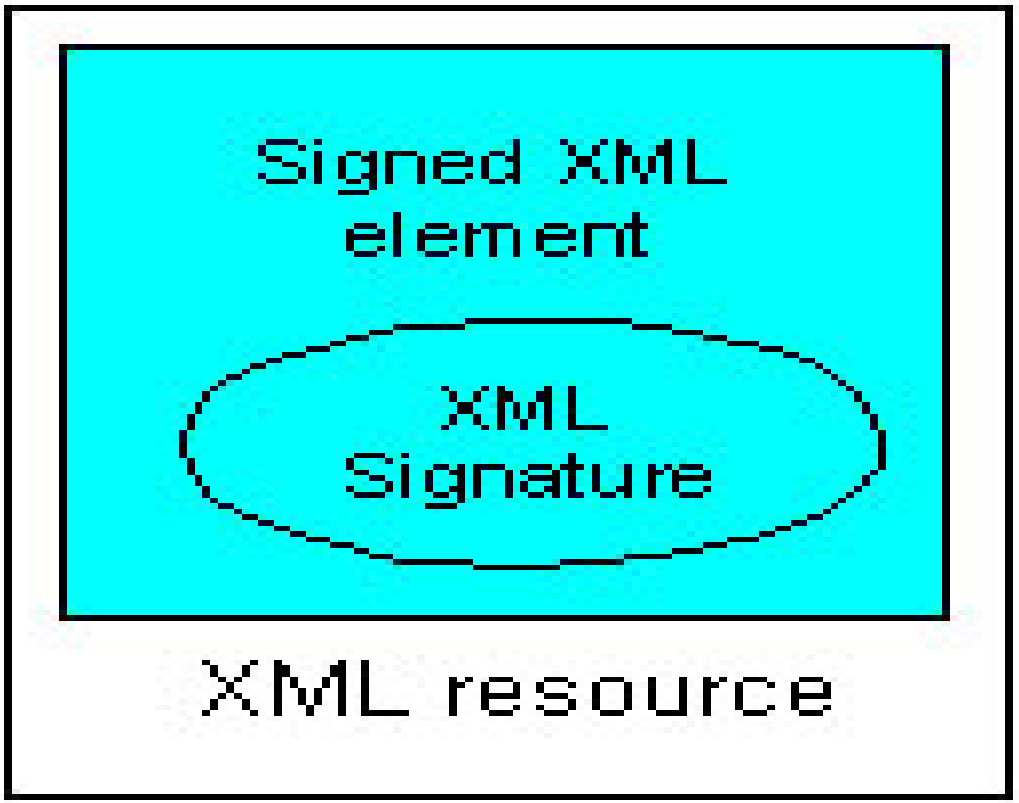
# XML Signature Example 3

The XML resource(s) being signed is/are embedded within an XML Signature.
(The signature encapsulates the data being signed.)



# XML Signature Example 4

The XML resource has its XML Signature embedded within itself.

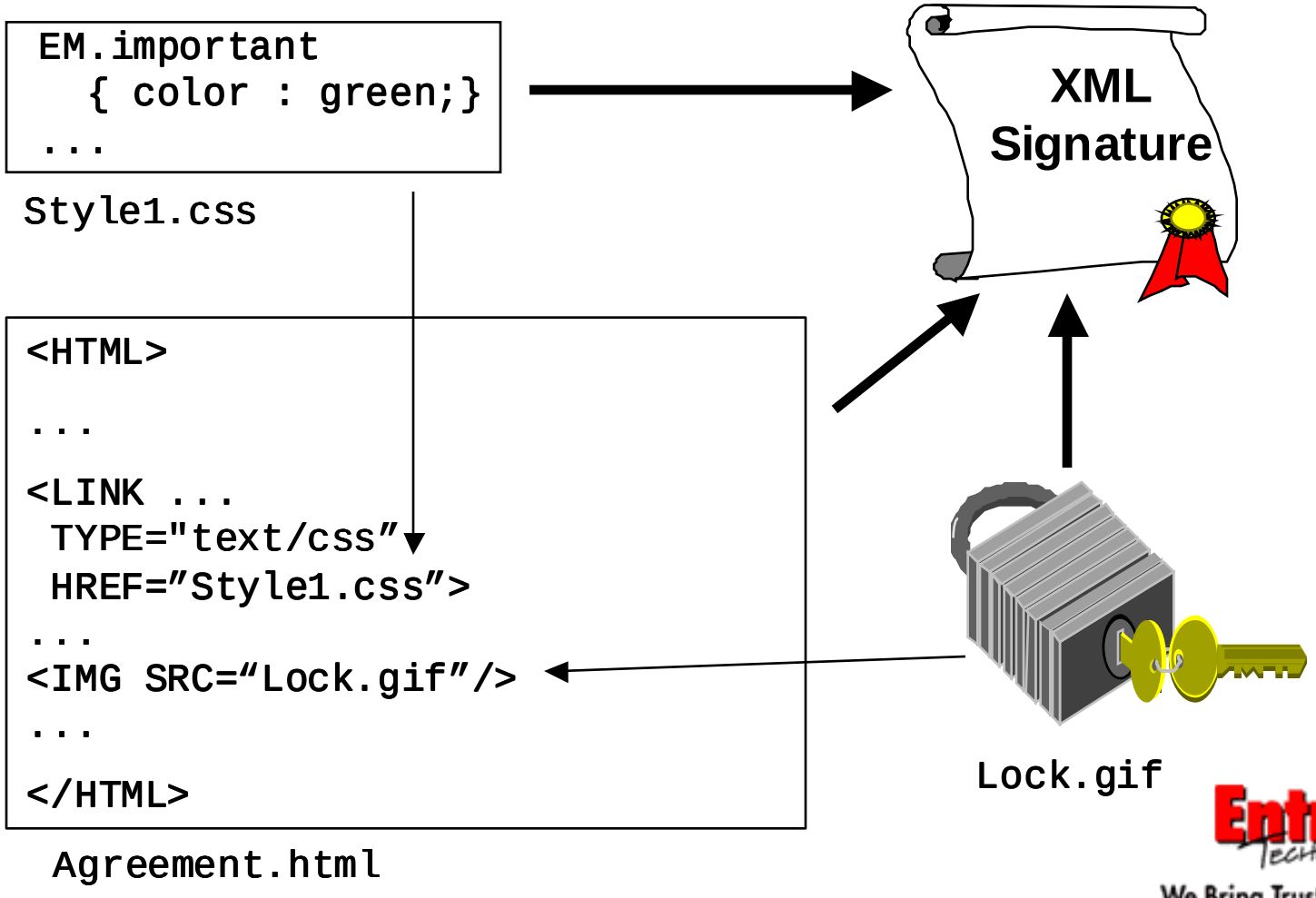


# XML Signature: Capabilities

- Supports transformations including XSLT and XPath
- Useful for signing just specific parts of an XML instance

# XML Signature App:
## Signing an agreement over the Web

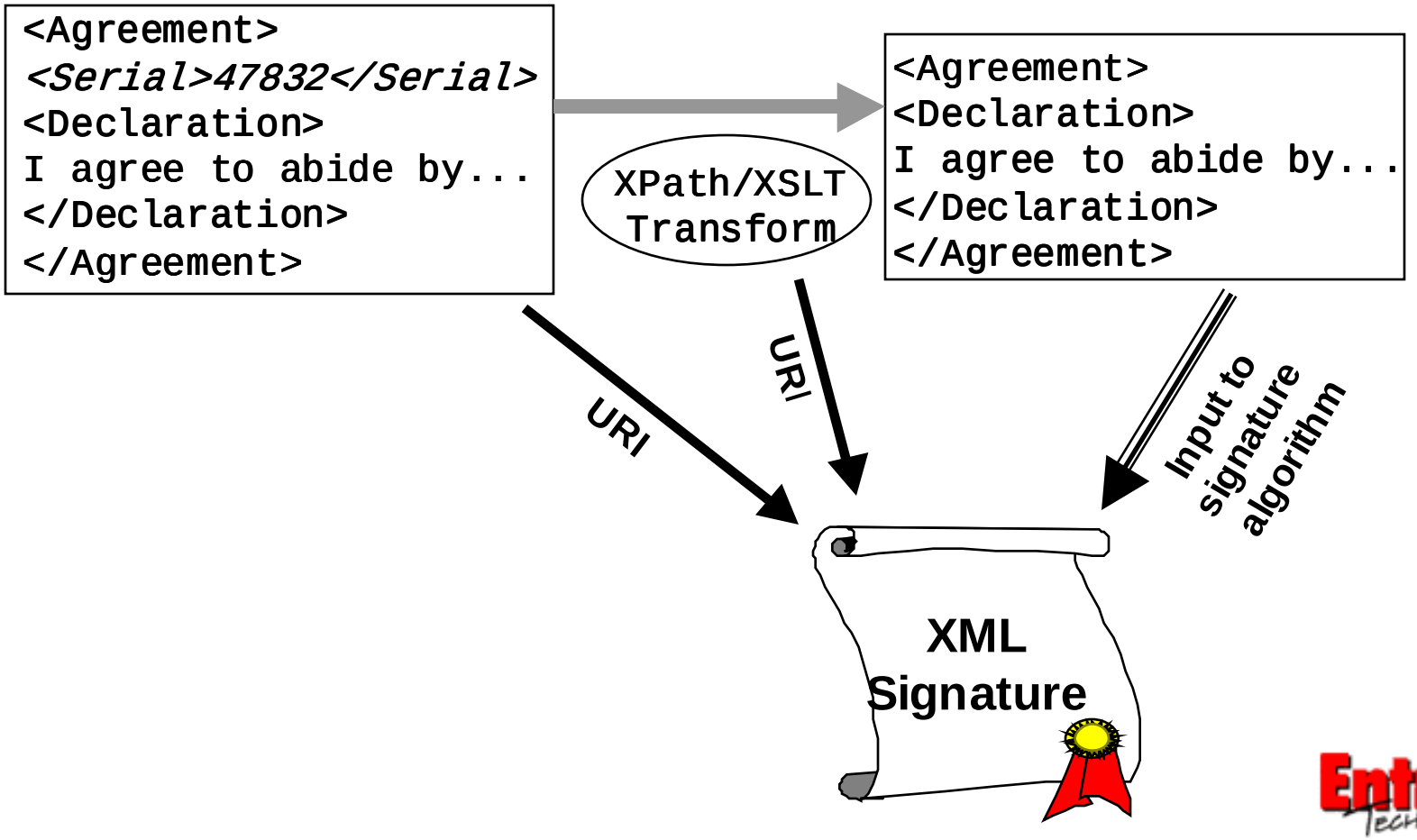
Need to sign all info that affects what the signer sees




We Bring Trust to e-Business™

# XML Signature App:
## Signing a form with non-binding fields

Need to exclude some form fields from signing




We Bring Trust to e-Business™

# XML Signatures and e-Signatures Law


- Legislation regarding electronic/digital signatures in various jurisdictions now
- Goal is that XML Signature spec provides an excellent mechanism for creating legally-effective electronic/digital signatures
- XML's human readability is considered to be particularly valuable for long-term archiving
- Discussion on http://www.legalxml.org

# XML Encryption

- Work on specification just started in early August 2000 by W3C
- Following description is based on very early work and is likely to change significantly in the next weeks

# XML Encryption: Capabilities

Can encrypt:

- all of an XML element
- the content of an XML element
- ~~an attribute (name and value)~~
- an attribute value (currently being hotly debated)
- ~~other node types~~
- arbitrary data (eg. GIFs, MPEGs, etc.)

# XML Encryption: Capabilities...

Bi-directional association of keying material and encrypted data:

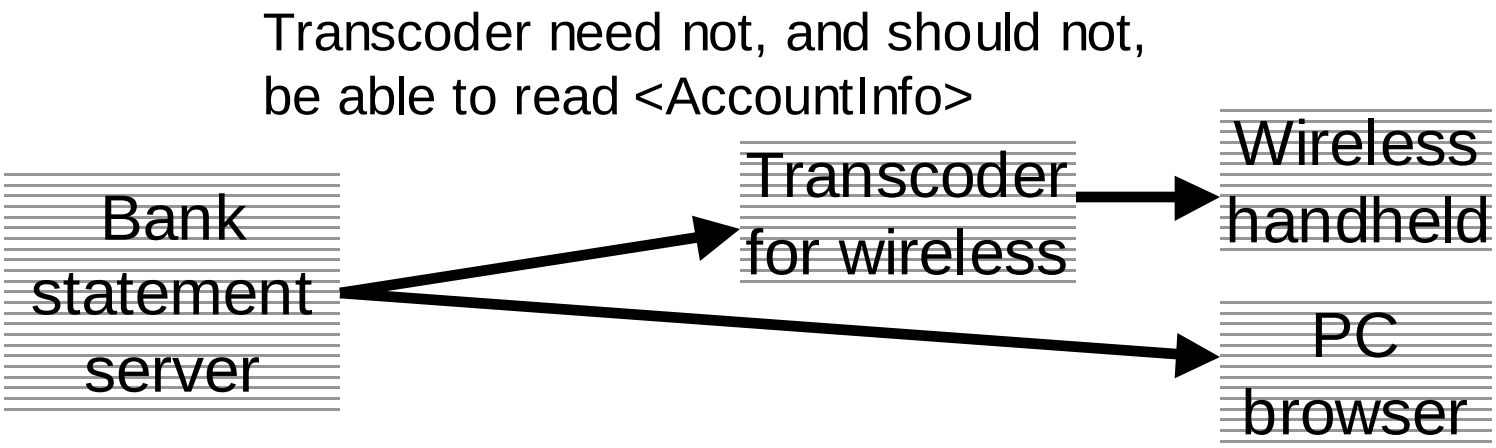
- <EncryptedData> can point to <EncryptedKey> elements
- Encrypted nodes can be stored separately from original data; an <EncryptedKey> element can point to one or more <EncryptedData> or <EncryptedKey> elements

# XML Encryption Application: Wireless online banking


Brokerage wants to provide access to stock trading through handheld device and uses a transcoder to strip out images.

Transcoder needs to be able to parse and filter the XML but should not have access to sensitive data.

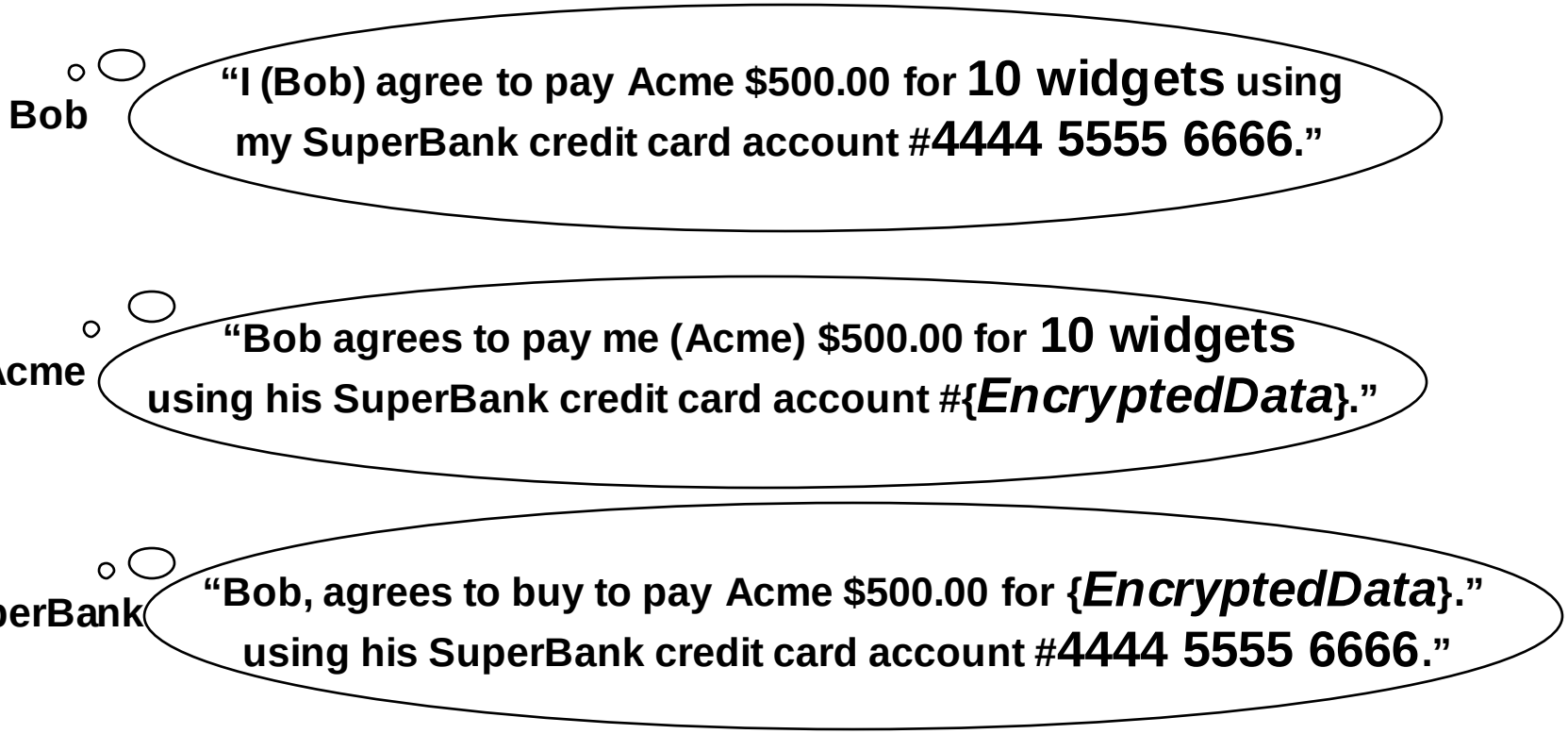
# XML Encryption Application: Wireless online banking...




```
<BankStatement>
  <!-- Logo removed for wireless devices -->
<Logo>…</Logo>
<AccountInfo>
<EncryptedData xmlns="Encryption">…
</EncryptedData>
</AccountInfo>
</BankStatement>
```

We Bring Trust to e-Business™

# XML Encryption Application:
## Buyer-vendor-bank transaction




1. Bob needs to know what he is buying and his card #.
2. Acme needs to know what Bob bought but NOT his card #.
3. SuperBank needs to know Bob's card # but NOT what he bought.

We Bring Trust to e-Business™

# XML Encryption Application:

## Buyer-vendor-bank transaction...

**Invoice's encrypted nodes encrypted for different organizations.**

```
<Invoice>
<Buyer>Bob</Buyer>
<Goods>
<EncryptedData xmlns="Encryption">
   <DecryptionInfo>
      {Bob's & Acme's decryption info}
   </DecryptionInfo>
</EncryptedData>
</Goods>
<CreditCard Type="SuperBank">
<EncryptedData xmlns="Encryption">
   <DecryptionInfo>
      {Bob's & SuperBank's decryption info}
   </DecryptionInfo>
</EncryptedData>
</CreditCard >
</Invoice>
```

XML WORLD EURO EDITION

Entrust Technologies

We Bring Trust to e-Business™

# XKMS:
# XML Key Management Specification


Provides an XML interface to Public Key Infrastructure (PKI) services; lessens or removes need for direct use of a programming API.

Status milestones:

- First public draft published at the end of November
- Initial (but unofficial) discussion meeting at the beginning of March

Quick examples:

- Obtain the key necessary for verifying a signature or decrypting
- Determine if a Certification Authority's signature on an imbedded certificate is valid
- Determine if an imbedded certificate has been revoked

Entrust Technologies
We Bring Trust to e-Business™

# SAML:
# Security Assertion Markup Language


Enables sharing of security services among different organizations.

Status milestones:

- First public draft released in mid-November
- OASIS Technical Committee started in mid-January

Quick example:

- Company A lets registered, authenticated users access its parts catalog. Company B does a similar service for its own parts catalog but with a different set of users. Now Company A and Company B want all the users to be able to access both companies' catalogs. SAML lets them exchange the authentication and authorization data necessary to make it so.

Entrust Technologies
We Bring Trust to e-Business™

# XACL:
# XML Access Control Language


Defines access control rules to specific nodes within an XML instance (fine-grained access control).

Status milestones:

- Has been discussed in academic circles and research labs for over a year
- Critical mass necessary for forming a standardization body appears to have been reached in mid-February; may be done loosely in conjunction with SAML

Quick example:

- Alice is always allowed to read <Account>/<Balance> elements but can only modify them if she signs and logs the changes.

Entrust Technologies
We Bring Trust to e-Business™

# Security designed for the Web: Queries


Because XML Signatures, XML Encryption, XKMS, SAML, and XACL are XML themselves, they can be indexed by search engines making queries like these possible:

- What has A signed?
- Who has signed X?
- Which <email> elements have been encrypted with my public encryption key?
- What are the access control policies associated with element Z when it has parent element Y?

Entrust Technologies

We Bring Trust to e-Business™

# XML Security: Further reading

XML Signature

- W3C/IETF Home Page
- http://www.w3.org/Signature

XML Encryption

- W3C Home Page
- http://www.w3.org/Encryption

XML in Legal Documents

- http://www.legalxml.org

# XML Security: Further reading...

SAML: Security Assertion Markup Language
OASIS
http://www.oasis-open.org/committees/security/index.shtml

XACL: XML access control
University of Milan
http://www9.org/w9cdrom/419/419.html

IBM Tokyo Research Lab
http://www.trl.ibm.co.jp/projects/xml/doccont/index_e.htm

Entrust Technologies
We Bring Trust to e-Business™

# XML Security: Summary


Non-XML-aware security protocols can be used to secure XML data just like it was any other type of data.

But to us XML zealots, XML isn't just like any other data;

- we want security designed with XML in mind, security that doesn't diminish XML's advantages, security that takes advantage of XML's benefits;

- we want security designed for the Web; security that works in concert with the Web's emerging technologies.

Entrust Technologies
We Bring Trust to e-Business™

# XML Security: Summary...


- The W3C is developing the XML Signature specification and may soon begin work on XML Encryption
- XML Signatures protect the authenticity and integrity of one or more objects. Can selectively sign specific nodes of XML instances
- XML Encryption protects the privacy of data. Specific nodes of XML instances can be encrypted for different key holders

Entrust Technologies
We Bring Trust to e-Business™

# XML Security: Summary...


- XML Signatures and XML Encryption are valuable not just for what they can secure but also for what they can leave unsecured
- XML Signatures and XML Encryption are designed to work hand in hand with XML technologies (eg. XPath, XSLT) in a Web environment
- XML Signature is close to Candidate Recommendation status.

  Moves to charter an XML Encryption WG have just started

Entrust Technologies
We Bring Trust to e-Business™

# XML Security: Contact info


**Ed Simon**

**Entrust Technologies**

**ph: (613) 270-2583**

**email:**

***ed.simon@entrust.com***

**or**

***ejs19630722@hotmail.com***


We Bring Trust to e-Business™