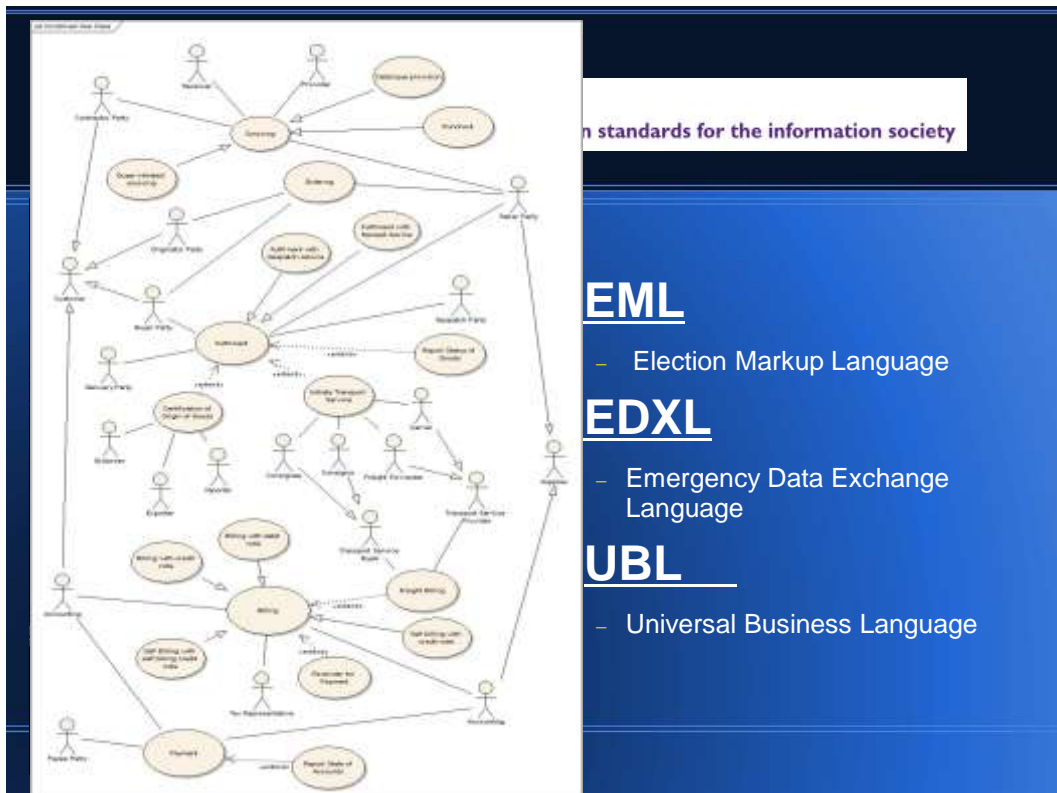
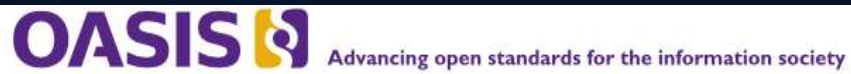


- A not-for-profit organization
- Heads development, convergence, and adoption of open standards
- Produces standards for security, e-business, and leads standardization efforts in both public sector and application-specific markets.
- Over 5,000 participants throughout 600+ organizations and 100 countries.





- Allows the interoperability of web-related components
- Better visibility in searches
- Allows both client and server side software to work better
- Compliant pages are converted to other formats easier (Handheld's, Phones, ect.)
- Allows code to be edited easier by others

Why is Standardization Important?



- Business's
 - Restricts Access
 - Profit Margins
- People
 - Disabled
 - Poor Regions
- Stability
 - Ease of Use

Web Services Security (WSS)

- Originally thought to be over-hyped technology
 - IBM & Microsoft release “Security in a Web Services World”
 - First security framework for Web Services
- July, 2002 – OASIS takes over WSS Standardization

Three Essential Security Requirements

- “The communication between our customer and his business partner should not be able to be viewed by a third party as it travels on the Internet.”
- “Our customer needed to be able to determine from whom the message was coming and be able to verify that the sender was who the sender claimed to be.”
- “Our customer needed to be able to ensure that the data being transmitted was not tampered with.”
 - Thompson, Sam. "Implementing WS-Security."

Web Services Security 1.0

- Released March 2004
- First platform designed to be flexible so it can operate on multiple platforms.
- Not expected to provide a full security solution for WSS, but is a good start.
- Security tokens, digital signatures, and encryption are all used to authenticate and protect SOAP messages

Web Services Security 1.0 (SOAP)

In order to create encrypted SOAP messages in compliance with OASIS's specifications, it's recommended that the steps below be followed in this specific order....

Web Services Security 1.0 (SOAP)

Create a new SOAP envelope.

Create a Security header

When an Encrypted Key is used, create an element that should contain a data reference to each data element encrypted using the key.

Locate data items to be encrypted, (i.e., XML elements, element contents in the SOAP envelope).

For each XML element or element content within the target SOAP envelope, encrypt it according to the processing rules of the XML

Original Elements or content are removed and replaced with encrypted versions

Web Services Security 1.1

- November 2006 OASIS announced a set of “errata”
- By February, 1.1 was ratified and released
- Security Additions were result of feedback from users

Business Identity Credential

- Security models between the two business's rely on a shared business identity credential
- For every WS request, the body of the SOAP message contains the WS operation and message parts that are digitally signed by the sender using X.509 certificates
- Service Provider uses the credentials given to authorize in order to control access to back-end business functions

Individual Credential

- Each user that would like to access the data has their own individual credentials, user ID and password, for the LDAP registry.
- Users are authenticated by the “consuming application” and their identity is passed to WS request using *UsernameToken*
- Security tokens along with the body of the SOAP message are digitally signed using X.509

Federated Identity

- Employees need to access applications from their separate locations.
- Primary goal is to allow each business to provide their employees with a set of services that allow them to take advantage of the business functions of other partners.
- Jumping between Web sites of business partners and suppliers can create a number of security issues.

Federated Identity

- One of the primary goals was to not expose user security credentials.
- To do this, they must agree on a pseudonym mapped to each of their users.
- Service Provider maps the pseudonym to a local user within its security domain
- User id is passed as HTTP header parameter within Service Provider's environment when invoking the Web services implementations

Conclusion

- Automation of SOAP allows for less and less human interaction.
- Allows messages to be transmitted regardless of framework