Sécurité en ingénierie du Logiciel

Le cadre des Web Services
Partie 8 : Sécurité des messages

Alexandre Dulaunoy

adulau@foo.be

Agenda

- Introduction
- OpenPGP
- OpenSST
- XML Signature
- XML Encryption

Introduction

- Confidentialité,
- Authentification,
- Intégrité,
- Non-repudiation (non désaveu),

Dans le cadre des Web Services, une sécurité de bout en bout est requise.

OpenPGP

Crytosystème hybride réalisé par P. Zimmermann en 1991 (PGP). RFC en 1996 (John Callas).

- Format binaire (<=> XML),
- Format de message,
- Format pour les clés,
- Format et description des signatures,

Utilisé pour le courrier électronique mais aussi le "batch-processing".

OpenSST

Cryptosystème hybride pour créer une alternative simple à XML Enc - XML Sig.

- Format XML,
- Format de message et type de message,
- Format pour les clés (indirect),
- Format et description des signatures sur le message,

http://www.opensst.org/protocol/message-format/opensst.xsd

XML Signature

Eviter la modification d'un message XML ou le désaveu du message lui-même.

- Signatures sur des portions possibles,
- Plusieurs signatures par plusieurs entités,
- Signature dans le document (p.ex. dans SOAP),
- Signature de documents détachés (p.ex. document PDF attaché à un XML),

!Canonisation http://www.w3.org/Signature/

XML Encryption

Garantir la confidentialité d'un message (ou d'une partie) XML,

- Chiffrement sur des portions possibles,
- Plusieurs clés possibles (KeyInfo),
- Compatible avec une XML Signature,

Q&R

- adulau@foo.be
- http://www.foo.be/cours/securite-webservices/
- 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD