Critical issues in the practical use of digital signatures

Frederick Hirsch, Chair W3C XML Security WG

Nokia

OASIS Open Standards Forum 2008

1 October 2008

These slides reflect my opinions,
not the position of Nokia or W3C.

Security viewed as a Cost

Security

ROI?

hard to quantify financially even though many case studies?

do not want a "science project"

As secure as the weakest link, makes for a wide technical cost

"Security does not make more sales..."

However: risk management is justified in financial industries, for example...

Functional requirements

With a →

Technology Focus

Mix of legal, business,
social and technical

The myth of non-repudiation

Forgetting trust with focus on technology

Leading to ⟶

Complexity

The inherent insecurity of complex systems

Performance

The spectacular failure of large initiatives
versus
the success of “interim solutions”

Is it possible to layer security later?

Scary crypto

XML is not simple

Combining complicated
applications, XML and Security!

Namespaces, Schema,
Parsing, whitespace,
QNames, XSL etc

XML Signature WG did a **great** job in 2002!

This limits ⟶

Continuity and Usability

Key Management

backward compatibility, versioning

Revocation, roll-over

what you see is what you sign, or is it?

Evolving technologies

Whatever happened to secure Signed/Encrypted eMail??

PKI

Integration and Interoperability

More capable adversaries

Unfixed bugs, old algorithms, short key lengths etc

yet ⟶

Those little bugs

Work Continues

http://www.oasis-pki.org/resources/whitepapers/

ROI: http://www.oasis-pki.org/whitepaper/roi.pdf

Risk management

http://en.wikipedia.org/wiki/Risk_management

Next Steps Workshop: http://www.w3.org/2007/xmlsec/ws/agenda.html

http://idtrust.xml.org/

Identity federation

XAdES: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21353

DSS-X: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss-x

Bugs: http://www.schneier.com/blog/archives/2005/11/howard_schmidt.html

XKMS: http://www.w3.org/2001/XKMS/

XML Security, including XML Signature: http://www.w3.org/2008/xmlsec/

Trust: http://www.rh.edu/~rhb/cs_seminar_2005/SessionA1/stifel.pdf

Thank you !

Patent expirations...

http://www.rsa.com/press_release.aspx?id=261