Critical issues in the practical use of digital signatures

Frederick Hirsch, Chair W3C XML Security WG

These slides reflect my opinions, not the position of Nokia or W3C.
Security viewed as a Cost

ROI?
do not want a "science project"

hard to quantify financially even though many case studies?

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

Combining complicated applications, XML and Security!

XML is not simple

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

XML Signature WG did a great job in 2002!

This limits
Continuity and Usability

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

backward compatibility, versioning

Key Management

Revocation, roll-over

yet →

Those little bugs
Work Continues

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

Thank you!

Patent expirations…

Risk management

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

http://idtrust.xml.org/


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

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

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

Identity federation


Patent expirations…