

# INTERNET SECURITY & THE BR DOMAIN

## LONG TERM STORAGE

**John Murray**

Enterprise Registry Solutions Limited  
([www.erst.eu](http://www.erst.eu))

# Quick Run Through

- ❖ Digital Signature
- ❖ PKI
- ❖ Archival
- ❖ Long term storage
- ❖ Legal aspects

# Internet Security & BRs

- ❖ Internet security is particularly en vogue
- ❖ BRs world wide embarking on e-filing initiatives
- ❖ Use of various technologies to 'provide' security
- ❖ BRs by their nature of function demand longevity of storage
- ❖ Dubious whether 'digital certificates' can provide 'longterm storage'

# Digital Security 101

Client  
Certificates

Server  
Certificates

Certificate  
Authority  
(CA)

Trusted  
Third Party  
(TTP)

Public key  
Infrastructure  
(PKI)

# 'Digital signatures'

“Digital signature is a metaphor that illustrates a particular use of public key cryptography by referral to the well-known concept of a signature.”

# Definition of Electronic Signature

- ❖ Use of the term 'signature' removes the 'mystic' of the technology
- ❖ Obscures the differences in a hand-written signature and a digital one
- ❖ Political persuasion world-wide is pushing the acceptance of electronic communication
- ❖ Paper signatures fulfil important functions – grounded in law and regulation
- ❖ Paper communication sets certain legal requirements for electronic signatures
- ❖ Establishment of a sufficient level of security for communication, and sufficiently trustworthy procedures for electronic documents

# Electronic versus Digital

- ❖ Electronic is technology neutral
- ❖ Used by the EU Directive on electronic signatures
- ❖ Digital signature refers to a particular technology for electronic signatures
- ❖ Open electronic signature mechanism

# With or Without?

## OPTION

1

**Store the document with signature.**

Ensure enough information to validate the signatures when required

## OPTION

2

**Store the document without signature.**

Store the validation process details before archival took place

# Closer Look at Option 1

- ❖ Long term archival of digital signatures create problems in:
  - ❖ Limited life time of data formats
  - ❖ Expired keys and certificates (reconstruction)
  - ❖ Security of the cryptographic algorithms over time
  - ❖ Complexity of the technology
  - ❖ < 10 years not regarded as reliable

# Closer Look at Option 2

- ❖ Archival of documents without the signature:
  - ❖ Not sufficient for legal scrutiny in certain cases
  - ❖ Trust security of the archive against modifications
  - ❖ Process of conversion of the format

# Authentication and Trust

- ❖ A lot of questions raised about the viability of digital signatures and the supporting technology
- ❖ Public Key Cryptography here for 20 years or more
- ❖ No real break through in that time
- ❖ PKI services are marketed as 'trust services'
- ❖ PKI provides authentication not trust
- ❖ Identification of a party does not provide trust

# Authentication and Trust (Ctd.)

- ❖ Brokers are required to mediate between unknown parties and provide 'trust'
- ❖ A receiver can make use of the information to determine whether there is sufficient 'trust' for the particular purpose
- ❖ Infrastructure for authentication is very useful and is evidenced by the greater electronic communication between the private and public sector

# Why do we sign?

- ❖ No single answer – dependent on the culture, practice and legal system of a country
- ❖ Purpose of a signature:
  - ❖ Identification – link document to name of signer
  - ❖ Authorisation – signer consents to what is contained in the document
  - ❖ Symbolic – signing as part of a ceremony
  - ❖ Fulfilment – denoting end of negotiation
- ❖ Real question is whether digital signatures can fulfil these functions over time

# Electronic versus Paper

- ❖ Paper actants: signer, contents, paper, ink, signature, receiver and law
- ❖ Electronic actants: document format, editing application, operating system, hardware and storage media
  - ❖ Digital signature: signature format, cryptographic algorithm and keys
  - ❖ Validation: access to public keys, network components and access to online certificate information

# Digital Signature

2 properties required for signature:

- ❖ **Document must be finite or closed**
  - ❖ Hash created from static value => in turn must be able to recomputable for validation
- ❖ **WYSIWYS – What You See Is What You Sign**
  - ❖ Signer must have a true version of the document on screen
  - ❖ hidden text, revision traces and local configurations
  - ❖ WYSIWYS not evident for most documents

# Quick Recap...

- ❖ Digital and Handwritten are fundamentally different!
- ❖ Technologies can be used for the same functions
- ❖ Paper based on stable technology
- ❖ Electronic based on quickly evolving and changing technologies

# Long term storage

## ❖ 5 real difficulties

- ❖ Lifetime of the storage medium
- ❖ Lifetime of the keys and certificates used
- ❖ Lifetime of the signing method, related to key sizes and other aspects of the cryptographic algorithms
- ❖ Lifetime of the document, signature, and certificate formats
- ❖ Lifetime and service offer of (trusted and other) actors involved

# Storage Media

- ❖ All storage media are vulnerable to time
- ❖ Time renders older media unreadable
- ❖ Routine copying to new media
- ❖ Avoid undesired changes to documents and invalidation of signatures
- ❖ Logistically complex and time-consuming but practically possible

# Certificate and Keys

- ❖ Digital signature must be unique
- ❖ Signature binds to the name in the certificate
- ❖ Name can be person, organisation or affiliation
- ❖ After expiry or revocation – the validation of the link from signature to name is difficult
- ❖ Time-stamp for the signature must be reliable  
=> know exactly when it was valid
- ❖ Time-stamp must be included in the comms protocol

# Life-time of Signing Method

- ❖ Key sizes are based on estimate of processing power to prevent a brute force attack on the key pair
- ❖ Number of possible key pairs must be large enough to make it unfeasible to try
- ❖ Strength of a signature is based on the above!
- ❖ Quantum processing? Bioinformatics?
- ❖ Development in maths will undermine PKI
- ❖ Protection of existing signed documents by using another counter-signature
- ❖ Counter-signature is possible but very complicated

# Lifetime of Formats & Technology

- ❖ Individual vendor document formats have less longevity than standards (SGML, XML, etc)
- ❖ Most certificates today are based on the ASN.1 X.509

# Lifetime of Trusted Actors

- ❖ Processing that requires an external party is always risky
- ❖ Having all the information stored in house runs its own risks
- ❖ Users maintaining their own client certificate stores

# Alternatives to Signed Archival

- ◆ Do not use digital signatures at all
- ◆ Use other means to achieve non-repudiation
- ◆ Remove signatures and store only a trace of the validation process
- ◆ Only applicable in certain cases
- ◆ If Digital signatures are required – is there a real need to archive them?

# Non-archival

- ❖ Evidence for archival is not there!
- ❖ Norway Archival Law allows removal as long as the signature verification process is recorded
- ❖ Documents had to be converted into storage formats anyway
- ❖ What is stored in message/document log?
  - ❖ State document signed by named parties
  - ❖ Identify certificates from named issuers
  - ❖ State certificates were neither expired or revoked
  - ❖ State the version of the process/system that performed the validation
- ❖ No signed document – witness statement!

# Non-archival

- ❖ Storage of the log has to be secure
- ❖ Must protect against manipulation
- ❖ Archival in trusted third party rather than in-house

# Legal Requirements

- ◆ 'Electronic signature' is technology independent
- ◆ Some definitions include pins, ids etc.
- ◆ Pins and others only really used with additional authentication mechanisms