Long Term Storage For Electronically Signed Documents

Georg.Lindsberger@XiCrypt.com

ACSAC 2002
Agenda

- Legal Framework
- Difficulties when preserving digitally signed Documents
- Secure METS
- System MailTresor
- Business Case - Electronic Billing
Legal Framework

- digitally signed documents may have equal value to traditionally signed paper-documents

- legislation obligate businesses and citizens to store documents over many years, often even decades
  - Future use for control and account purposes
  - Evidential reasons
  - Protects interests of third persons

-> you have to preserve your digital documents by providing:
  - Authenticity
  - Integrity
  - Verifiability and Validity of the digital signature
  - Readability
Difficulties when preserving digitally signed documents

Problem - Electronic Signatures
- revoked certificates
- revocation information is no longer available
- algorithm used has been broken
- key-length is too small
Difficulties when preserving digitally signed Documents

The Document itself:

- The document format itself is no longer readable by the current software
METS - Metadata Encoding & Transmission Standard

Encodes different types of metadata of digital objects

- descriptive meta data
- administrative meta data
- structural meta data
- ...
S/METS – Secure METS

ETSI TS 101.903
XadES

+ 

METS

= 

S/METS

[DMD (EMAIL) -> Header, Sender, Recipient, Type.. ]
[AMD (EMAIL) -> File size, Rights..]

[FILE -> EMAIL
  -> ]

[DIV -> S/METS -> EMAIL
  -> Header
  -> Body ...>Signature]
System MailTresor

Long term preservation of digitally signed emails
- most used document type
- digital signature already “integrated”

Delivery/Notification System
- TicketMail
- ProveMail
1. Advanced Signature Generator

Advanced Signature Generator

Doc → XadES

CA ↔ TSA

XadES

ES Certificate Revocation Data

Time Stamp
2. Metadata Generator

- a set of descriptive, administrative and structural metadata is generated
- Metadata, Document, XadES form a submission information package (SIP)
3. Storage Module

- Responsible of storing the SIP in a digital preservation system
Business Case – Electronic Billing

Advantages:
- Lower cost
- Higher efficiency
- Faster transactions
- Process takes place in the same medium

Legal Requirements:
Invoices with deductible value added tax have the status of an official document:
- Integrity
- Authenticity
- Preservation (ex. Austria 7 Years)
eBilling – System Overview

1. Generate your invoices -> SMTP
2. S/Mime Enhancement Server signs your invoices
eBilling – System Overview

3. MailTresor preserves the signed document (email)
4. MailTresor takes care that the documents are delivered
Finally

- Legislator obligates you to store your digitally signed documents over long periods of time
- You have to preserve:
  - the signature
  - the document itself
- Solution: Secure METS (XadES & METS)

Links:
- System MailTresor / eBilling – http://www.xicrypt.com
- XadES – http://www.etsi.org
- METS – http://www.loc.gov/mets
Contact

Georg Lindsberger
XiCrypt Technologies GmbH
8046 Graz, Hub 109
Austria/EUROPE
http://www.xicrypt.com
georg.lindsberger@xicrypt.com