

THALES
UNIVERSITAT POLITÈCNICA DE CATALUNYA

➤ OASIS Digital Signing Service and E-Invoicing in Europe

Nick Pope – Thales eSecurity
Juan Carlos Cruellas - Universitat Politècnica de Catalunya

NIST PKI Workshop – April 2007

Outline ⏪

⏩

EU Requirements for eInvoices

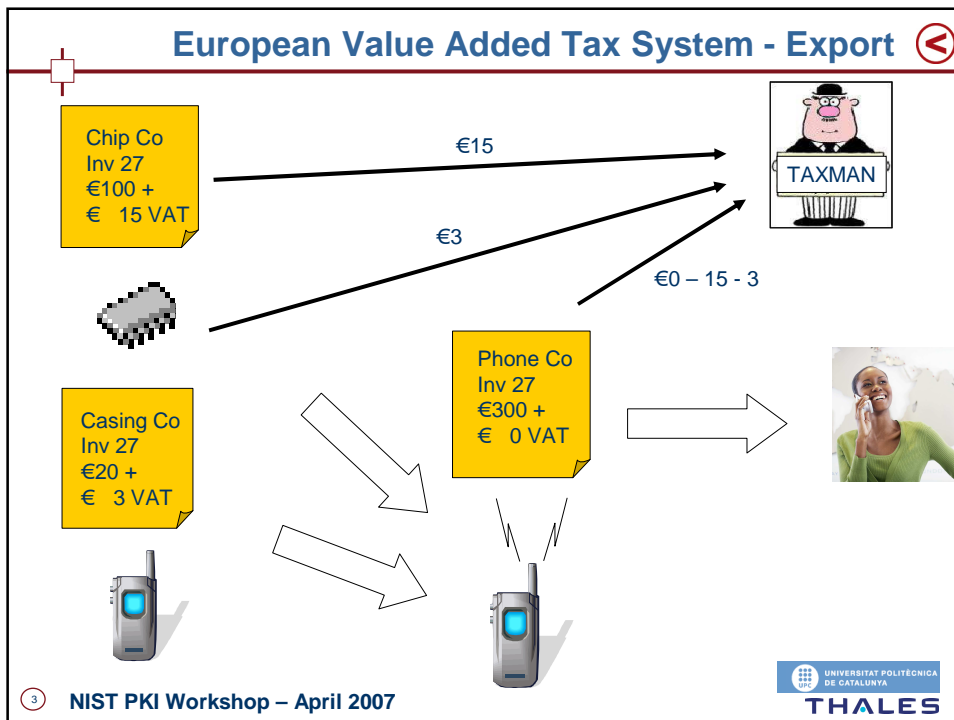
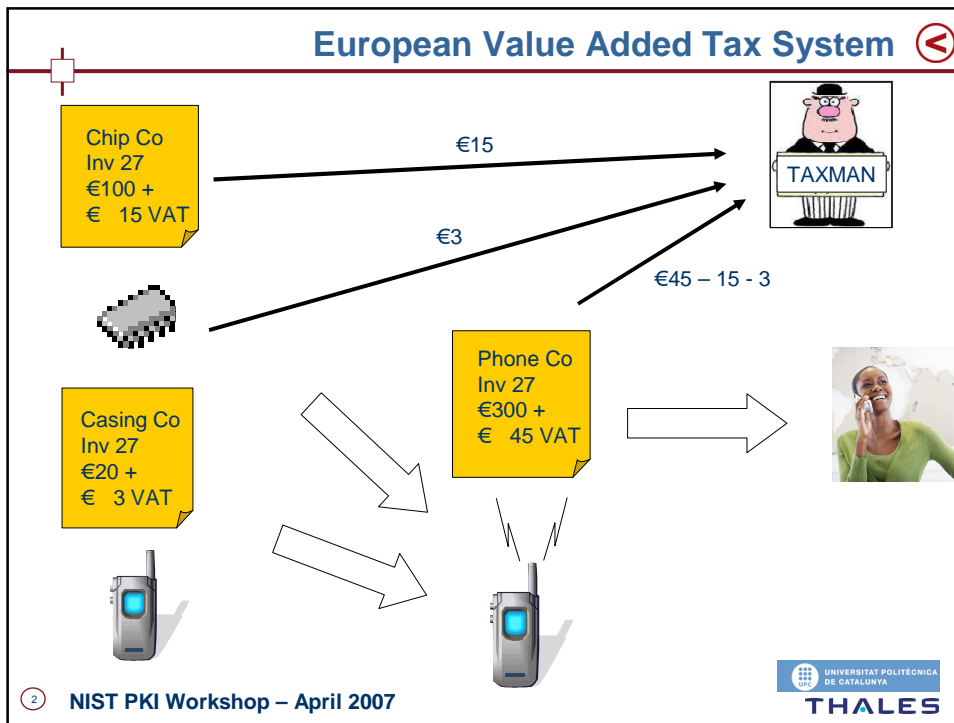
- Need for security in electronic invoices under European VAT Tax System
- How can be met by digital signatures
- Requirements for verifiability of stored signature

OASIS Digital Signature Services

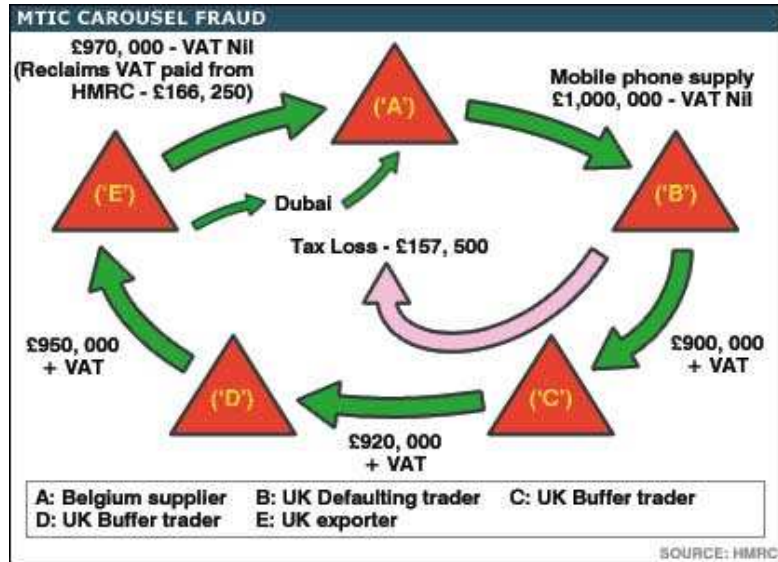
- Web based service for digital signatures
- Application to signing tax invoices

① NIST PKI Workshop – April 2007

UNIVERSITAT POLITÈCNICA DE CATALUNYA
THALES



Example VAT Fraud



4 NIST PKI Workshop – April 2007



EU VAT Harmonisation Directive

“Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed ..”

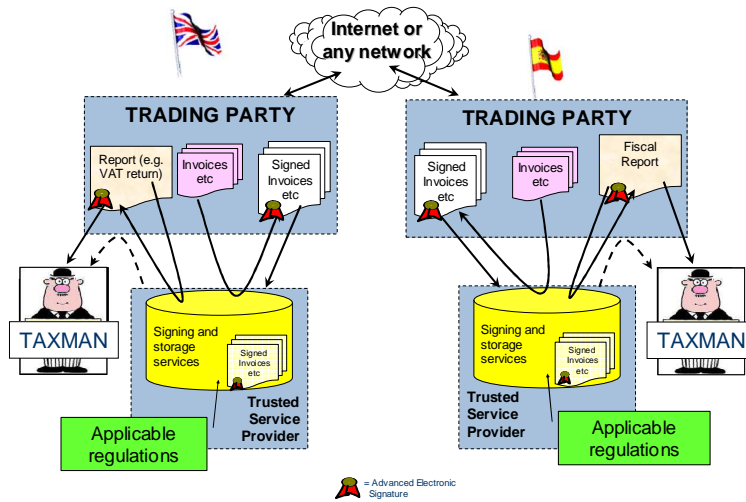
Recognised mechanisms

- “EDI Service Provider”
- “Advanced Electronic Signature”
 - X.509 based Digital Signature
 - From company / company officer

5 NIST PKI Workshop – April 2007



Requirement for Storage of Signed Invoices



6 NIST PKI Workshop – April 2007

UNIVERSITAT POLITÈCNICA DE CATALUNYA
THALES

Requirements for stored signed documents

Technical

- Information used to verify signature when stored
 - Certificate path
 - OCSPs / CRLs
- Time of verification
 - Signature Time-stamp
- Means to maintain integrity beyond algorithm life-time (e.g. 10 years)
 - Archive time-stamp (e.g. LTANS)

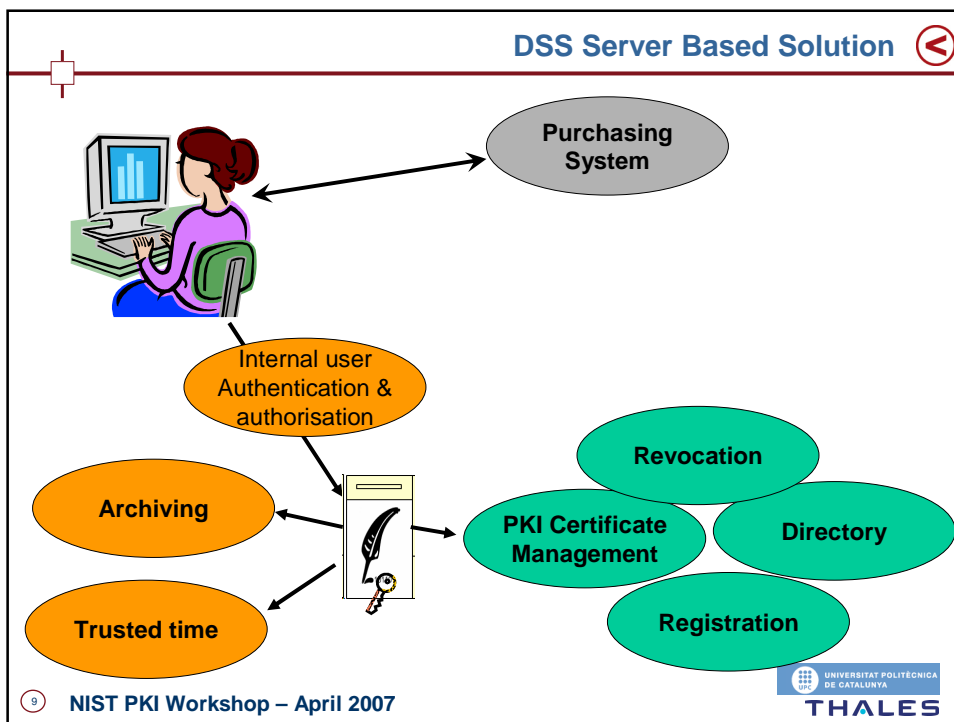
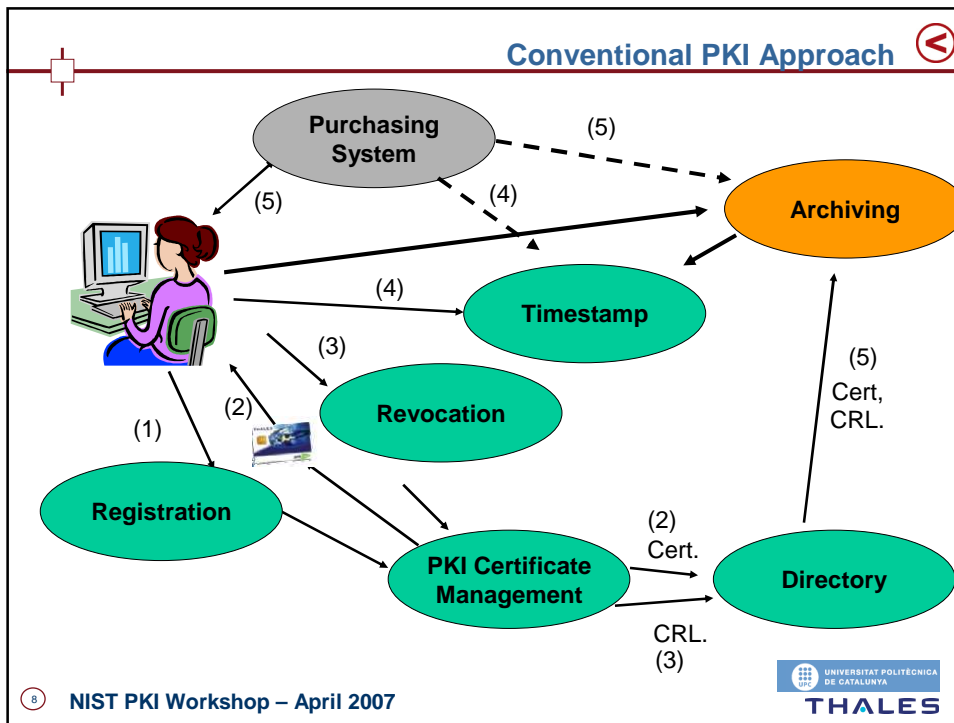
Or trusted organisation

- Notary

Ref: CWA 15579
ETSI TS 102 573

7 NIST PKI Workshop – April 2007

UNIVERSITAT POLITÈCNICA DE CATALUNYA
THALES



OASIS Digital Signing Services

Networked web service protocol

Supports range of signature formats:

- W3C XML Signature
- Cryptographic Message Syntax (CMS - RFC 3852)
- RFC 3161 / XML Time-stamps
- Extended Formats
 - XML Advanced Electronic Signature
 - CML Advanced Electronic Signature
- ... extensible for other formats

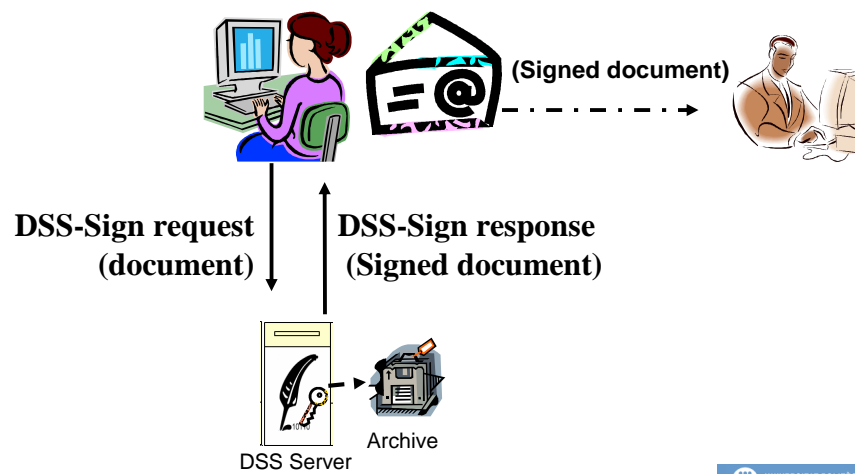
Two basic operations:

- Create signature
- Verify signature

 NIST PKI Workshop – April 2007



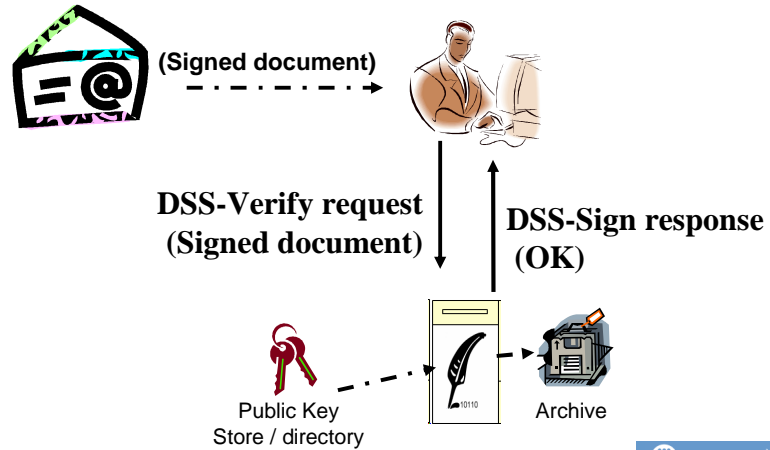
DSS Sign Protocol



 NIST PKI Workshop – April 2007



DSS Verify



12 NIST PKI Workshop – April 2007



DSS Specifications

DSS Core

General purpose tools for range of applications

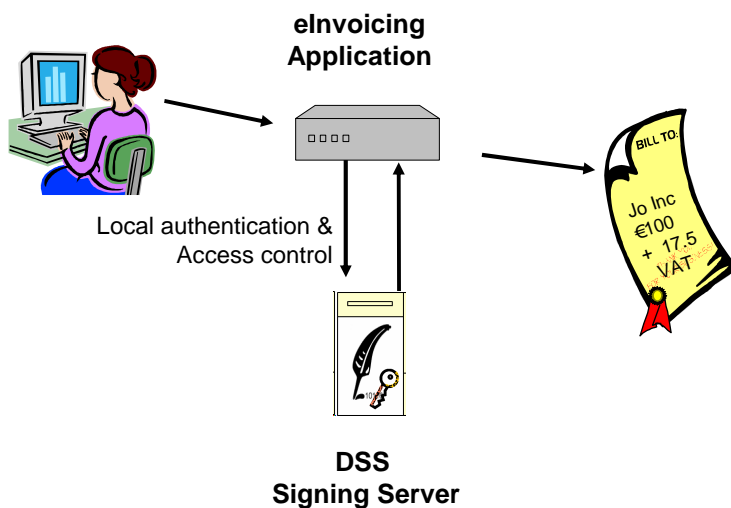
Includes:

- Sign request, Sign response
- Verify request, Verify response
- Optional inputs / outputs for handling common features of CMS / XML Signatures
- XML Signature Time-stamp Format
- Document value / Document Hash / SOAP Attachment
- Detached / Enveloped / Enveloping Signatures
- Transport request / response
 - HTTP, SOAP
 - SSL, Web Security Services

13 NIST PKI Workshop – April 2007



- XML Time-stamping
- Entity seal
- “Advanced” / Long term Electronic Signatures
(ETSI TS 101 733, TS 101 903, RFC 3126)
- Code Signing
- Electronic Post Mark
- German Signature Law
- Signature Gateway



DSS Signature Creation applied to invoicing

Authentication of user separated from management of signature key.

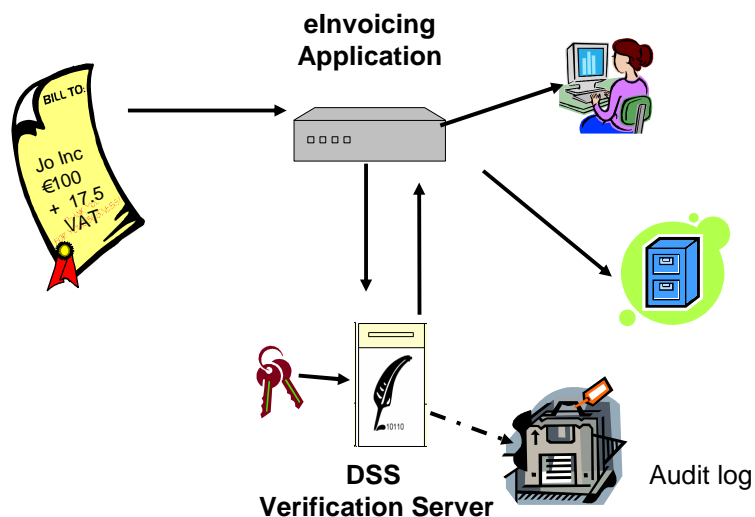
Hence:

- Can apply controls on who may apply “corporate” signatures
- Based on existing internal security controls using existing authentication and authorisation controls within normal work flow
- If user’s authorisation is revoked, organisation can stop use of signature
 - Immediate
 - No need to publish external revocation
- No need for special device on user system
- Strict organisational controls can be applied to handling of signing key
- Improved security & reduced per user cost

16 NIST PKI Workshop – April 2007



DSS Signature Verification applied to invoicing



17 NIST PKI Workshop – April 2007



DSS Signature Verification applied to invoicing

- Support for later “re-verification” of signature
 - DSS Server can maintain audit log of verification information (Cert, CRL/OCSP, verification time), or
 - Signature can be augmented to contain verification information

- All complexities of PKI hidden from user

 NIST PKI Workshop – April 2007



DSS Implementation

Now fully ratified as OASIS Specification !!!

DSS “Style” of operation used for a number of years

- Norwegian BankID
- Thales SafeSign

Interoperability trials between several implementations

Adopted in Universal Postal Union
- Electronic Post Mark

Major conformant implementation being operated by
CATCERT for public agencies in Catalunya, Spain

 NIST PKI Workshop – April 2007



Conclusions

- Can provide improved security at reduced per user costs
- By detaching individual user authentication from signing function reduces need for revocation handling
- Supports verification of signatures stored for up to about 10 years
- A number of implementations appearing in 2007
- Matches Corporate signing requirements of eInvoicing
- Provides the power of PKI without headaches

 NIST PKI Workshop – April 2007



Thank You

DSS Specification available at:
<http://www.oasis-open.org/committees/dss/>

Contact us at:
nick.pope@thales-ecurity.com
cruellas@ac.upc.edu

 NIST PKI Workshop – April 2007

