



**THALES**

**Workshop on  
Digital Signatures and PDF  
May 21-22, 2008**

**Requirements for Long Term Validation  
using Advanced Electronic Signatures (AdES)**

**Nick Pope – Thales e-Security**



# Long Term Validation using AdES

## Topics



- Use cases
  - eInvoicing
  - Registered Email
  
- Requirements

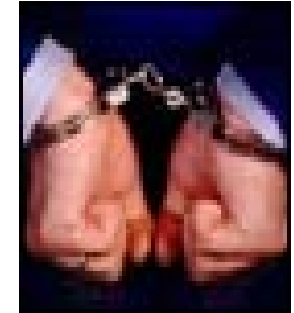
# Electronic Invoicing - Need for Evidence



TAX Authorities want evidence to reduce fraud:

“Nine men have been charged with fraud relating to a suspected £250m value added tax (VAT) scam.”

BBC News 6 February 2007



Businesses want evidence to demonstrate correct practices:

“A businessman is ordered to pay back more than £1m to the government following a huge tax fraud.”

BBC News 28 Nov 2007



# COUNCIL DIRECTIVE 2006/112/EC on VAT Harmonisation



## Article 233.1

“Invoices sent or made available by electronic means shall be accepted by Member States provided that the authenticity of the origin and the integrity of their content are guaranteed by one of the following methods:

(a) by means of an advanced electronic signature....,

...(b) by means of electronic data interchange (EDI)...

Invoices may, however, be sent or made available by other electronic means, subject to acceptance by the Member States concerned.”



## Article 246

“The authenticity of the origin and the integrity of the content of the invoices stored, as well as their legibility, must be guaranteed throughout the storage period.”

Aim: Stimulate further standardization work in the domain of electronic invoices in Europe building on Phase 1 activities:

WG 1: Adoption

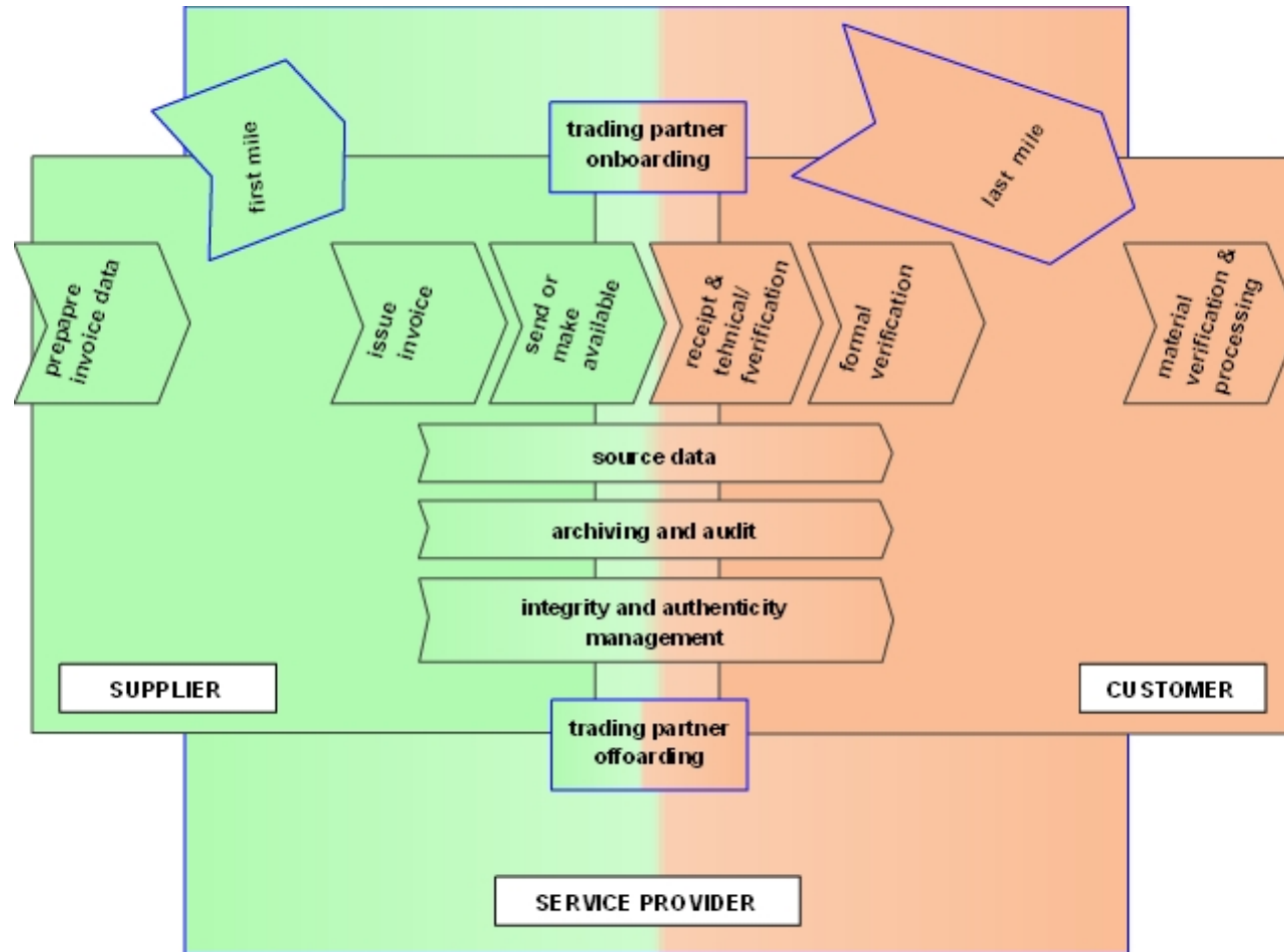
**WG 2: Compliance of electronic invoice implementations**

**WG 3: Cost effective authenticity & integrity**

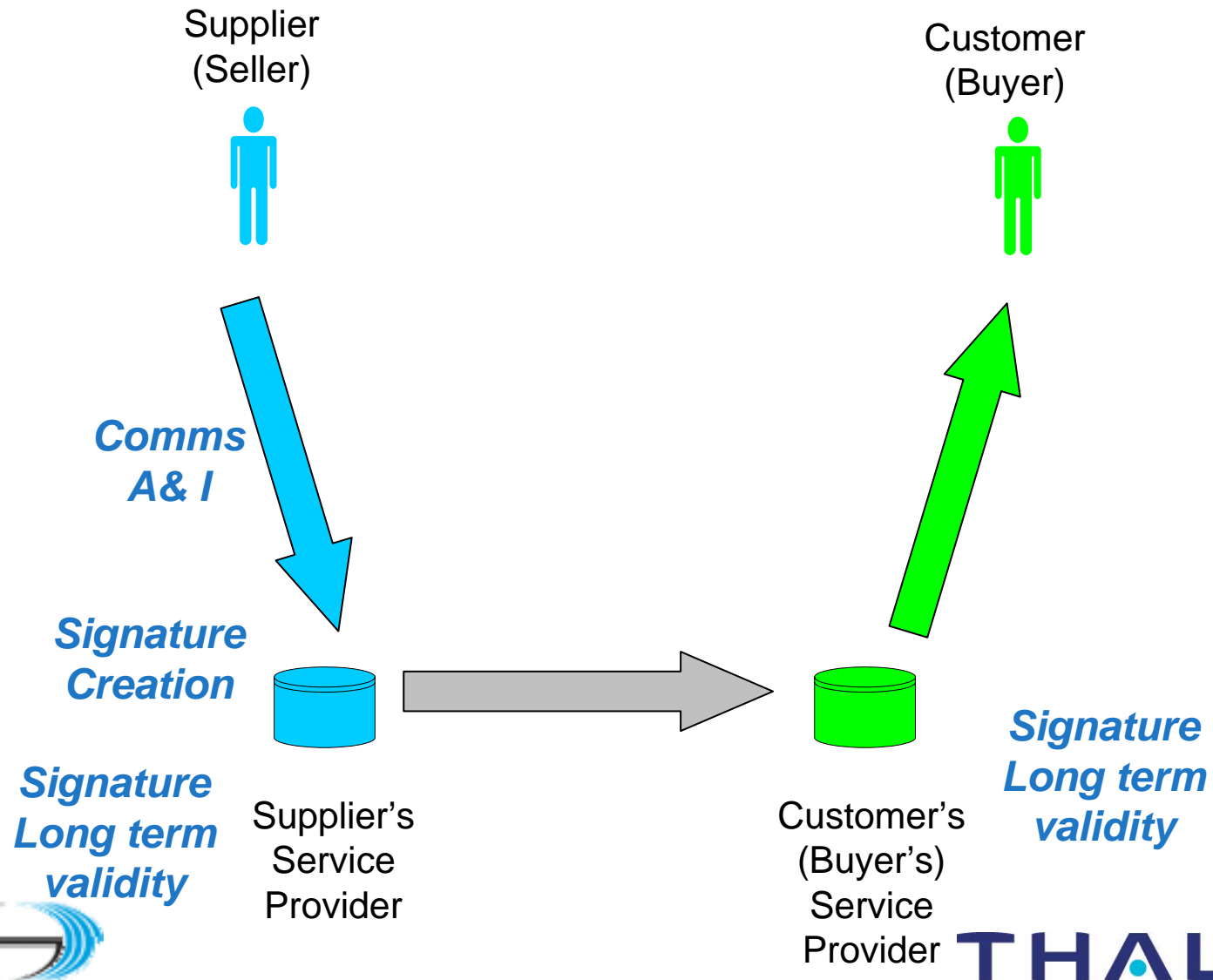
WG4: Emerging technologies and business processes

WG5: eInvoice service operators and mobility of users

# CEN / FISCALIS Good Practice for Electronic Invoicing



# AdES Requirements



# AdES Example Requirements & Controls 1



The Invoice must be protected with an Advanced Electronic Signature

The signature shall be created in accordance to an internationally recognised standard signature format. The signature should include a trusted time-mark or time-stamp applied on or around the signing time.

.....

## AdES Example Requirements & Controls 2



The authenticity of the origin and the integrity of the content of the invoices stored must be guaranteed throughout the storage period.

The OCSP / CRLs and CA certificates used to verify a signature shall be identifiable and accessible throughout the lifetime of the document (about 10 years).

The signed invoice, and at least the identity of the OCSP / CRLs and certificates used, shall be protected by mechanisms that assure their integrity throughout the storage period

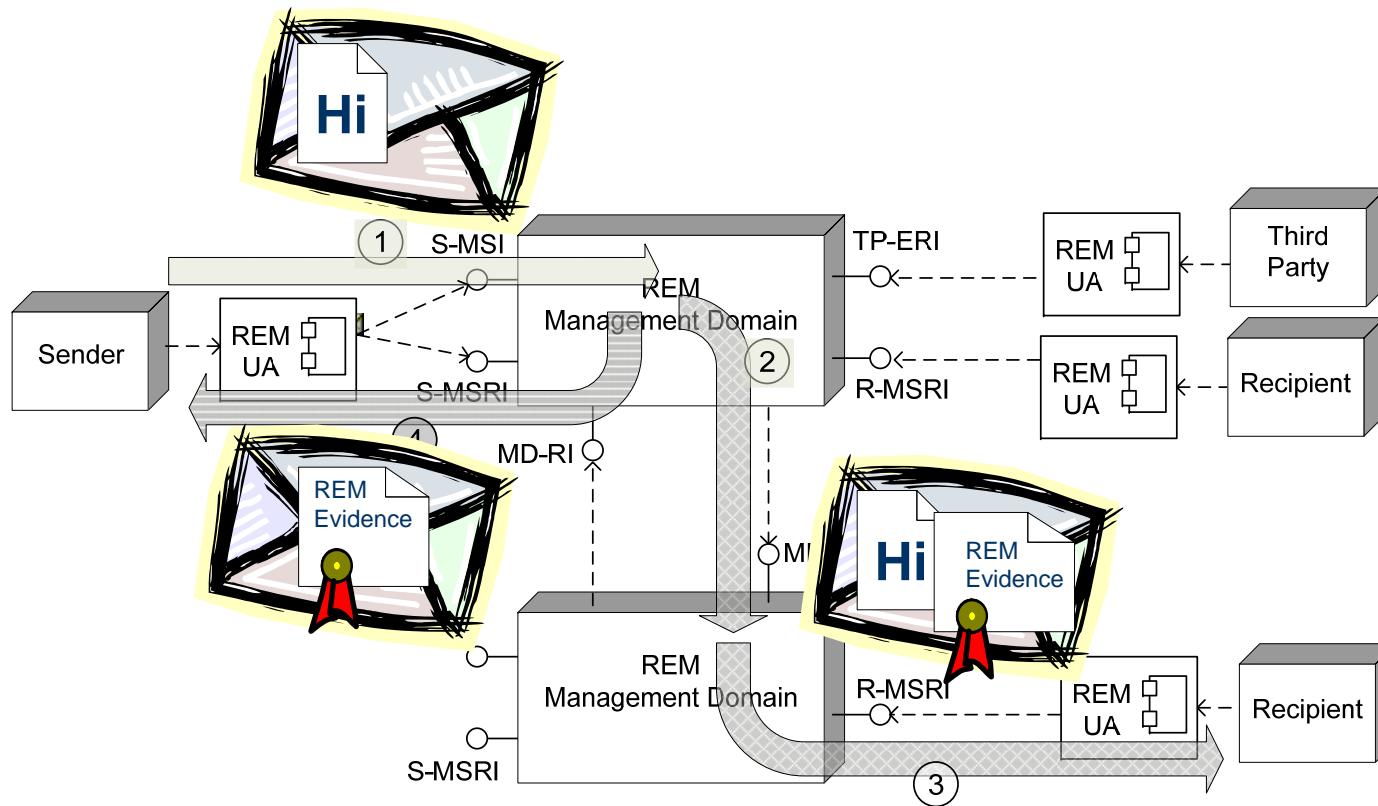
.....

Auditor view Invoice as in original



- Invoice data coming from
  - automated system
  - Person
- Send signed invoice
  
- Invoice processed
  - Automated
  - Person

# ETSI STF 318 – Registered E-Mail



- Signature by REM Evidence Issuer
- Verifiable for lifetime of evidence (e.g 10 years as for Invoice)

# Requirements for Long Term Validation of AdES

- Certainty of certificate used to sign document
- Certainty of signing time
- Certainty of information used to verify signature
- Integrity of signature and information used to verify signature
- Ensure document is presentation consistent

# Long Term AdES Requirements

## Certainty of certificate used to sign document



### Assumed Risk

- Certificate renew
- Two identities associated with same key
- Uncertainty over CA Practices (one key per certificate)
- Basic CMS Signature Attacker may swap certificates

### Mechanisms

- XAdES / CAdES Signature over certificate identifier



### Assumed Risk

- Uncertain whether certificate used were expired revoked at signing time

### Mechanism

- XAdES / CAdES Time-stamp over signature, or
- Time mark



### Assumed Risk

- Uncertain which CA Certificates / revocation information apply to the validity of the certificates which could effect validity

### Mechanism

- XAdES / CAdES Record CA Certificate / Revocation information applied in signature
- Have audit record from trusted verifier



### Assumed Risk

- After key / algorithm lifetime expired signature cannot be depended upon to ensure data integrity

### Mechanism

- XAdES / CAdES Archive time-stamp as part of signature
- RFC 4998 Evidence Record Syntax
- WORM (Write one read many) drive
- Use of Trusted Notary



## Assumed Risks

- Malware
- Hidden scripts
- Incremental updates

## Mechanism

- PDF-A ???

Any other requirements / risks ?

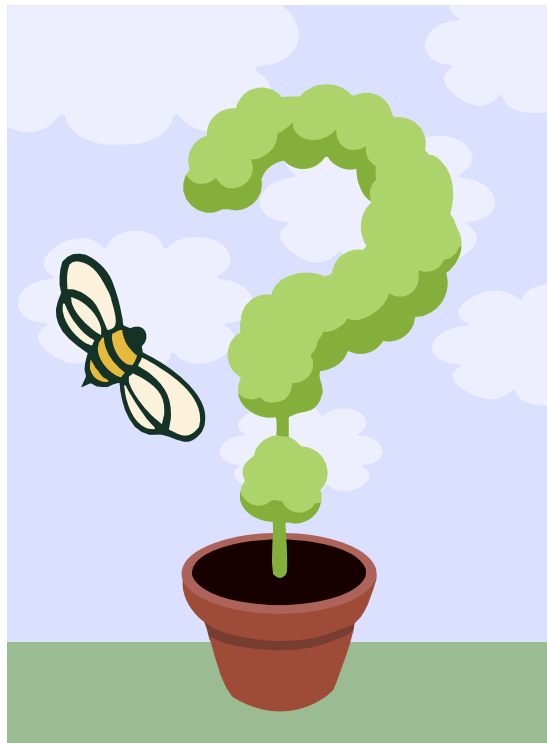
Other Long term requirements

- Can still read old files

Other AdES Requirements

- Qualified Electronic Signatures
- Trust Lists

- XAdES / CAdES + PDF/A supports all the mechanisms necessary for long term signatures
- What is included basic PDF Signatures ???



Thanks any questions?

[nick.pope@thales-ecurity](mailto:nick.pope@thales-ecurity)

)