

eInvoicing Public Meeting
Brussels, 19 June 2008



WG 3: Cost effective means to guarantee authenticity & integrity

Johan Borendal – Trustweaver (Chair)

Nick Pope – Thales e-Security (Technical Editor)

CEN eInvoicing Workshop – Phase 2



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

Terms of Reference



“**Cost-effective** authenticity and integrity of electronic invoices and related business documents regardless of formats and technologies”

- Minimise unnecessary costs to businesses
- Ensure that major risks identified by Tax Authorities are addressed



CEN eInvoicing WG 3: Terms of Reference



“Cost-effective authenticity and integrity of electronic invoices and related business documents regardless of formats and technologies”

→ Authenticity & integrity in transfer

→ Maintain authenticity & integrity over period of storage



CEN eInvoicing WG 3: Terms of Reference



“Cost-effective authenticity and integrity of **electronic invoices and related business documents** regardless of formats and technologies”

- eInvoicing main legal pressure point for business
- Applicable to other aspects of eBusiness & eGovernment



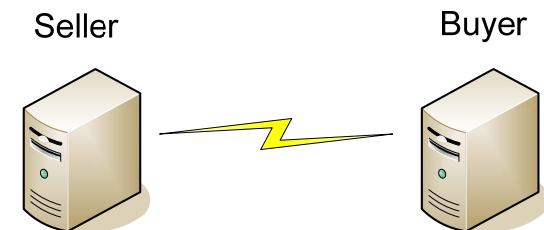
CEN eInvoicing WG 3: Terms of Reference



“Cost-effective authenticity and integrity of electronic invoices and related business documents **regardless of formats and technologies**”

Addressing Authenticity & Integrity by:

- Electronic Signatures
- Electronic Data Interchange (EDI)
- Other means



What Already Done

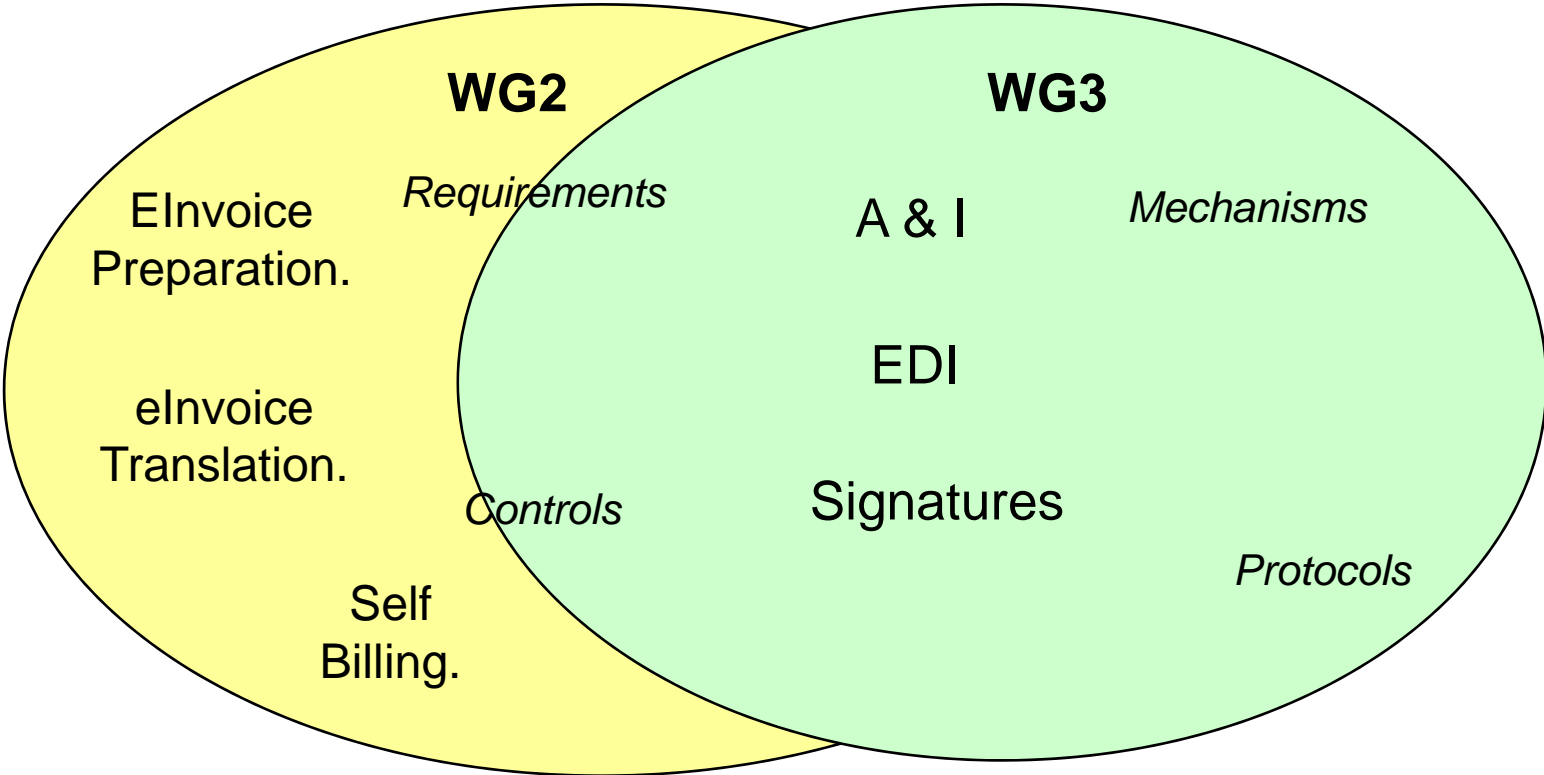


- Inventory of Authenticity & Integrity Requirements
 - Spreadsheet of Requirements against 28 EU States / EFTA members

- Integrity and authenticity Requirements in common e-invoicing scenarios
 - Model of eInvoicing exchanges
 - Requirements derived from Directive 2006/112/EC + national implementations

- Authenticity and Integrity Requirements & Controls

WG2 Good Practice vs WG3 Requirements & Controls



Conclusion

- Lets join forces



CEN WG2 & WG3 / FISCALIS e-Invoicing Good Practice Guidelines

WG3 Current Approach

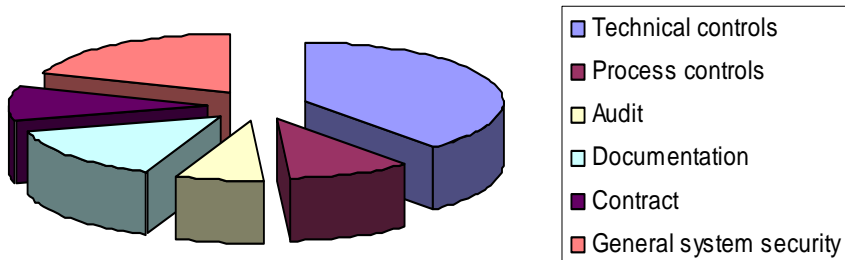


Authenticity & Integrity Controls

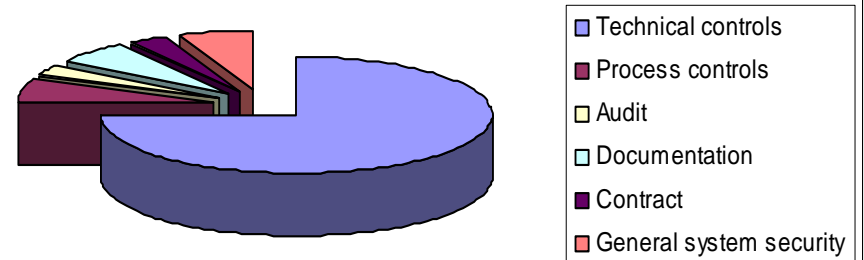
- ❑ Option 1: General procedural and technical controls to protect data at each stage of process (EDI / Other), or
- ❑ Option 2: Advanced electronic signatures protecting data from creation through whole storage lifetime (AdES)

Baseline security controls (e.g. audit, access control, contracts) should be applied throughout

No end-to-end long-term signatures



With end-to-end long-term signatures



WG3 – Example Authenticity & Integrity Controls



- Baseline controls
- Example controls for EDI (other) Scenario
- Example controls for Advanced Electronic signature based scenario

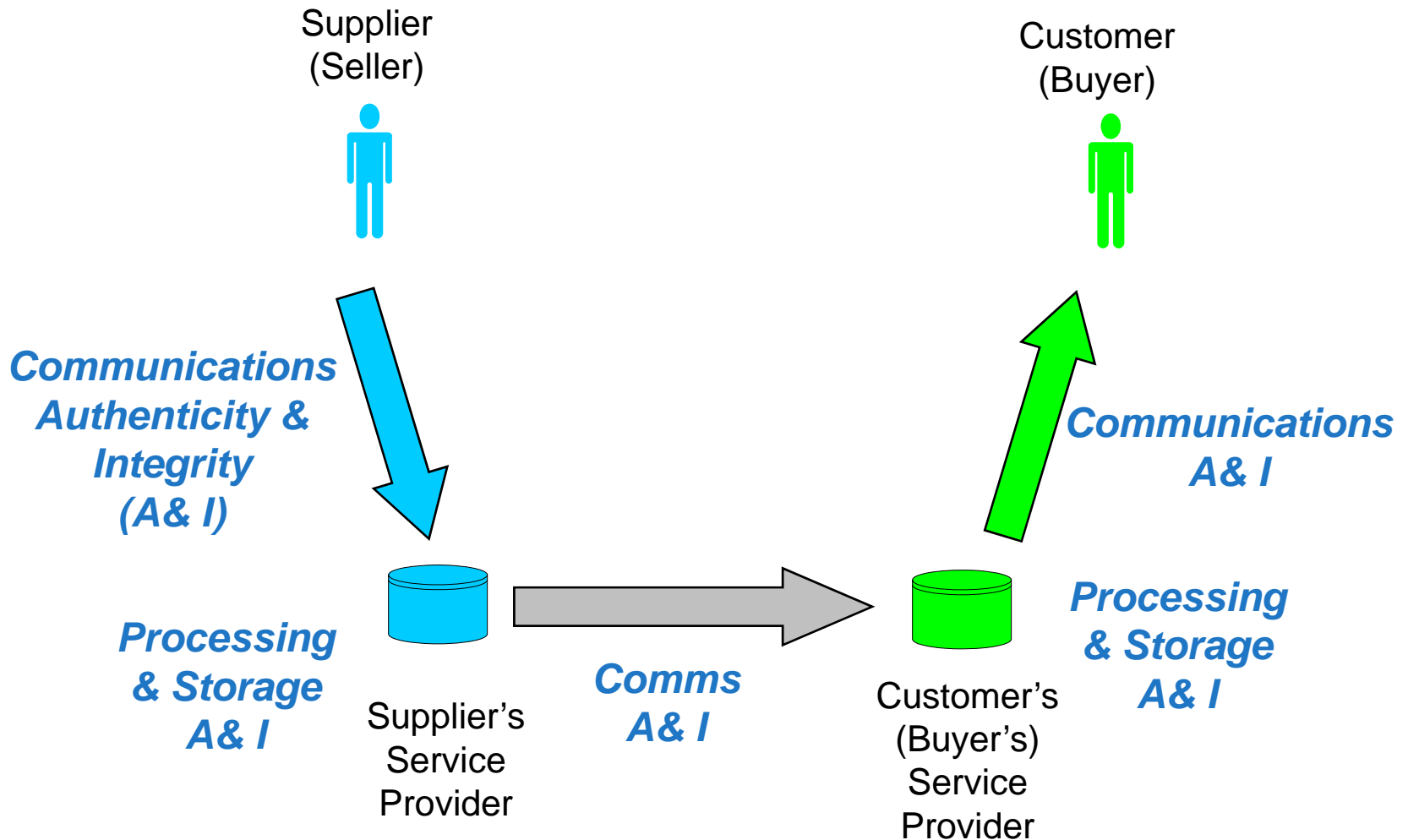
Baseline controls

- Recognised standard based practices for the security and integrity:
 - e.g. ISO 27001,
 - SAS70,
 - OECD Guidance on Tax Compliance for Business and Accounting Software

- Includes general controls for:
 - Audit trails
 - Access control enforcing business roles
 - Protected Communications
 - Data correctness and accuracy checks

- Prior agreement for security of communications

EDI/Other Example: Requirements & Controls



EDI/Other Example: Communications A & I



Requirement	Control
Ensure authenticity and integrity of invoice whilst being sent.	<p>The electronic invoice shall be sent through a secure channel which :</p> <ul style="list-style-type: none">a) Protects the integrityb) Authenticates the invoice issuer ... <p>Implementation examples:</p> <ul style="list-style-type: none">i) TLS with passwords.ii) AS/1-3 with signatures <p>.....</p>

EDI/Other Example: Storage A & I



Requirement	Control
<p>The authenticity and integrity of the content of the invoices stored must be guaranteed throughout the storage period..</p>	<p>The invoice and audit records regarding handling of the invoice, including information on authentication checks carried out, shall be protected by mechanisms that assure the integrity of data throughout the storage period.</p> <p>Implementation examples:</p> <ul style="list-style-type: none">- WORM,- Secure archive

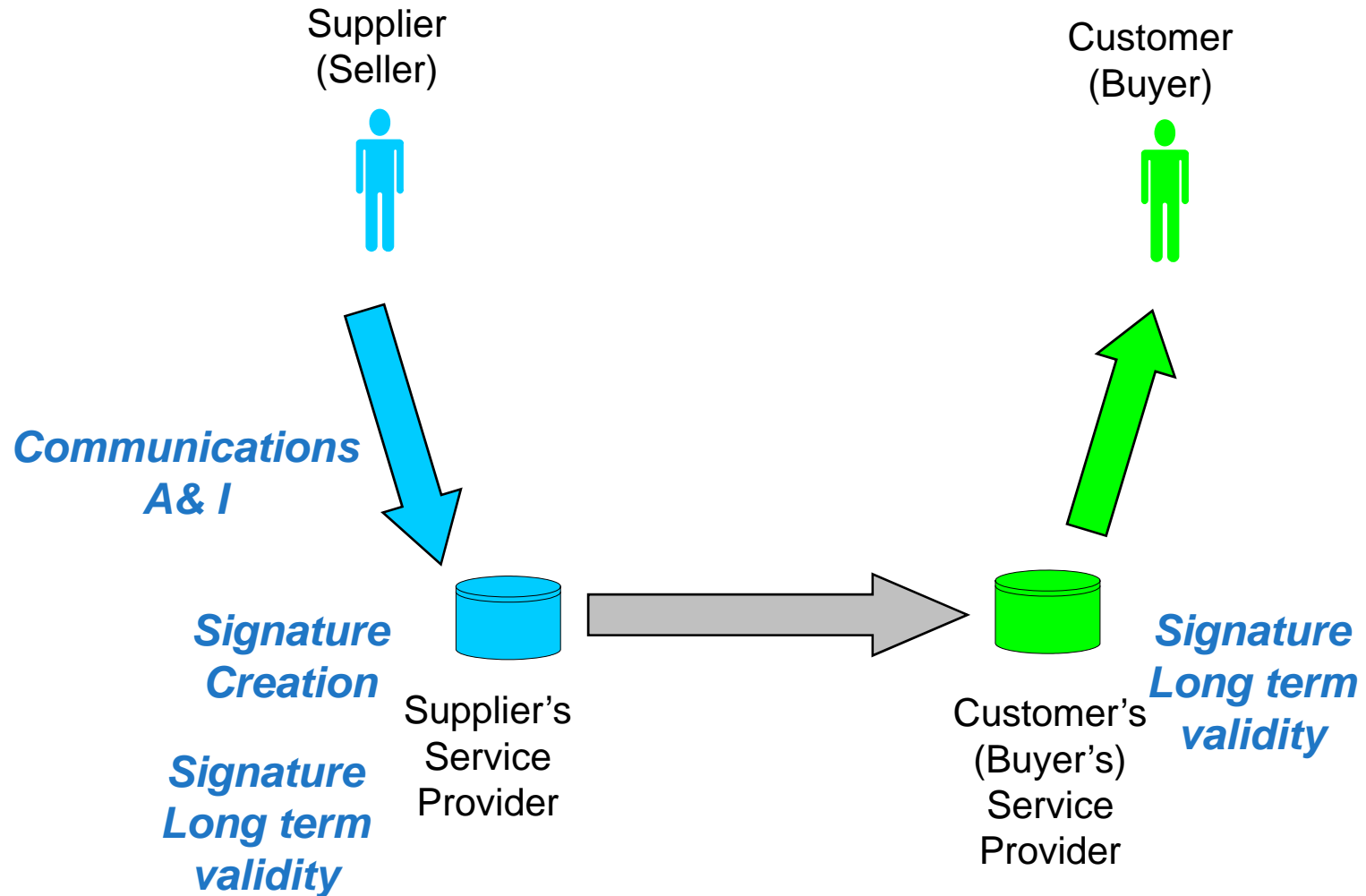
EDI/Other Example: Processing A & I



Met by a range of controls:

- Baseline security controls
- General eInvoice process requirements

AdES Example Requirements



AdES Example: Signature creation



Requirement	Control
<p>The invoice is provided with an electronic signature to protect its integrity and authenticity.</p>	<p>The application should ensure that signatures are applied when appropriate. The signature shall be created in accordance to an internationally recognised standard signature format.</p> <p>Implementation examples: eg: CAdES-T / XAdES-T</p> <p>...</p>

AdES Example: Signature verification



Requirement	Control
<p>The authentication of origin and integrity of the invoice must be verified by verifying the signature.</p>	<p>The validity of the AdES signature shall be checked and the results recorded including verification time and information (e.g. CRLs or OCSP and certificates) used to verify the signature.</p> <p>.....</p>

AdES Example: Signature long term validity



Requirement	Control
<p>Electronic signatures must remain verifiable during the storage period.</p>	<p>The integrity of the signed invoice, including information used to reverify the signature (see above under invoice creation), shall be maintained beyond the lifetime of the signature algorithm and certificates.</p> <p>Implementation examples:</p> <ol style="list-style-type: none">1) Applying archive timestamp to signature as in XAdES-A, CAdES-A2) WORM devices. <p>.....</p>

Next Steps

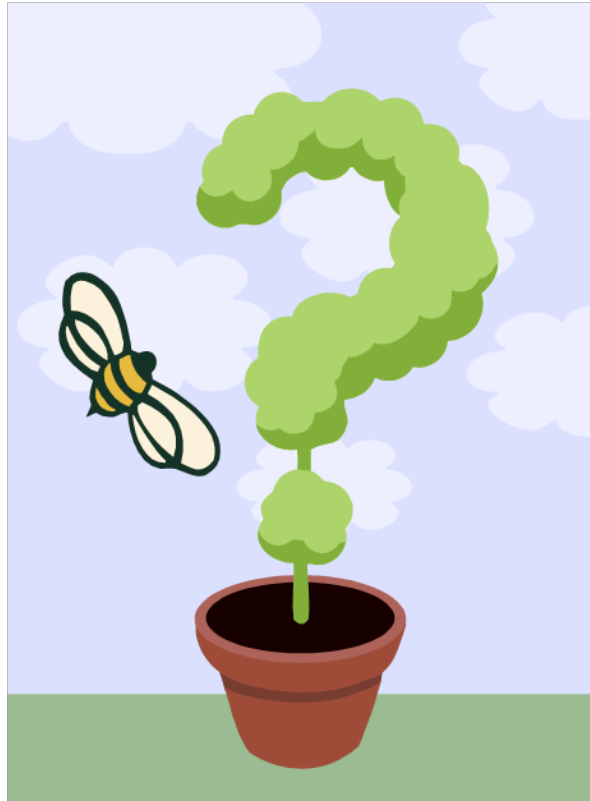


- Continue working with Good practice Authenticity & Integrity Controls (Joint deliverable with WG2)

- Further Guidance on Authenticity and Integrity
 - Further guidance on example mechanisms and protocols

 - Developed in next phase

Thank you



Thanks any questions?

**nick.pope@thales-eSecurity
(editor)**

**johan.borendal@trustweaver.com
(chair)**

eInvoicing Public Meeting
Brussels, 19 June 2008