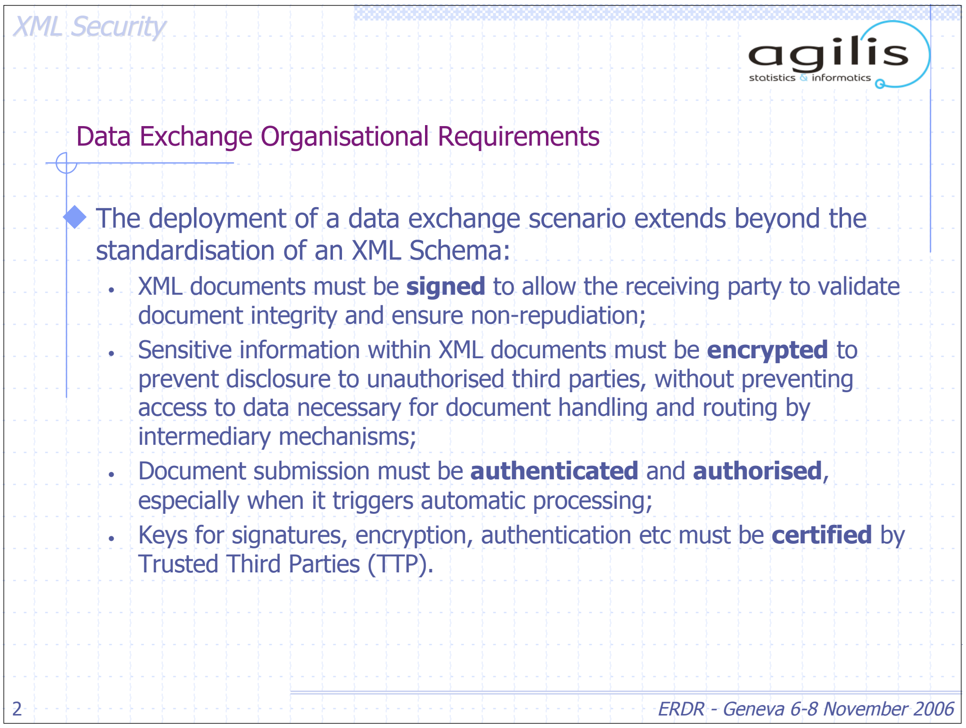
XML Security

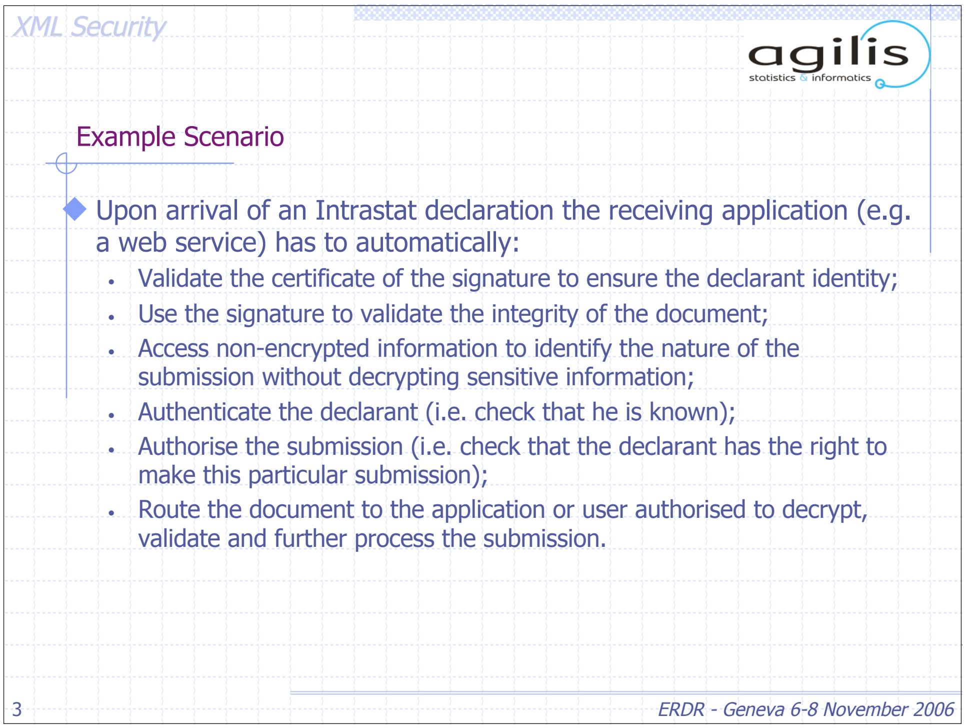
Gregory Farmakis
Agilis SA

Electronic Raw Data Reporting
Geneva, 6-8 November 2006



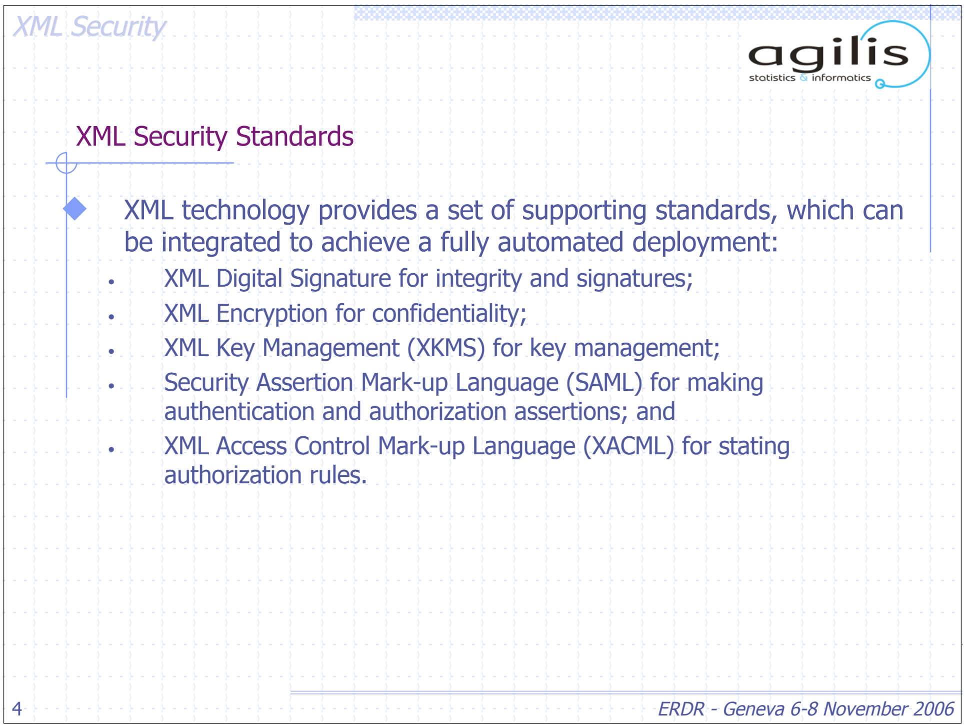
Data Exchange Organisational Requirements

- The deployment of a data exchange scenario extends beyond the standardisation of an XML Schema:
  - XML documents must be **signed** to allow the receiving party to validate document integrity and ensure non-repudiation;
  - Sensitive information within XML documents must be **encrypted** to prevent disclosure to unauthorised third parties, without preventing access to data necessary for document handling and routing by intermediary mechanisms;
  - Document submission must be **authenticated** and **authorised**, especially when it triggers automatic processing;
  - Keys for signatures, encryption, authentication etc must be **certified** by Trusted Third Parties (TTP).



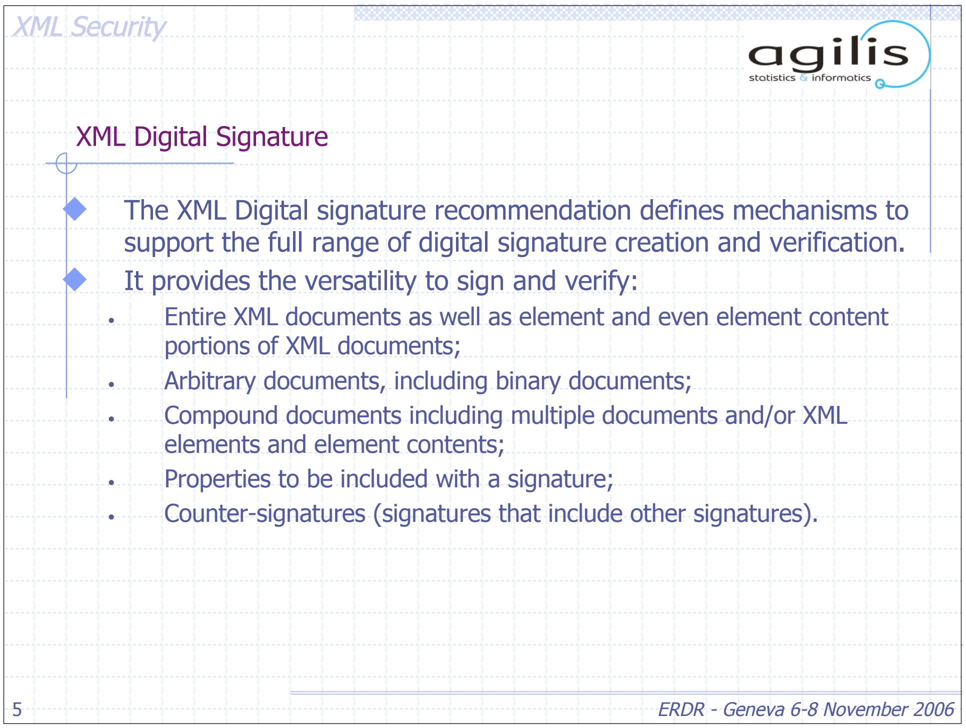
Example Scenario

- Upon arrival of an Intrastat declaration the receiving application (e.g. a web service) has to automatically:
  - Validate the certificate of the signature to ensure the declarant identity;
  - Use the signature to validate the integrity of the document;
  - Access non-encrypted information to identify the nature of the submission without decrypting sensitive information;
  - Authenticate the declarant (i.e. check that he is known);
  - Authorise the submission (i.e. check that the declarant has the right to make this particular submission);
  - Route the document to the application or user authorised to decrypt, validate and further process the submission.



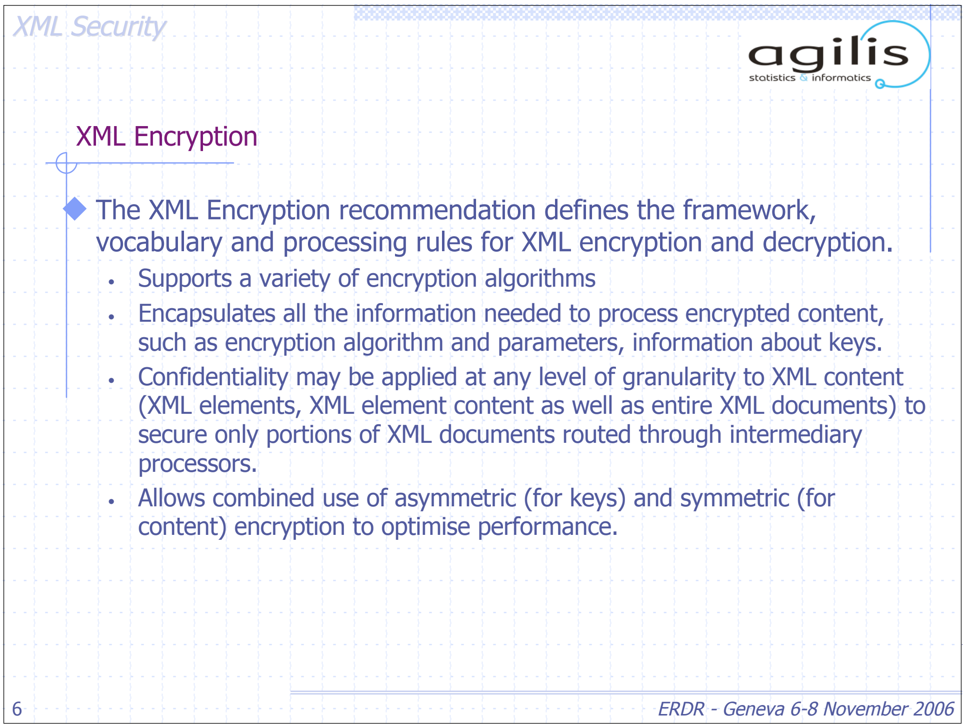
XML Security Standards

- XML technology provides a set of supporting standards, which can be integrated to achieve a fully automated deployment:
  - XML Digital Signature for integrity and signatures;
  - XML Encryption for confidentiality;
  - XML Key Management (XKMS) for key management;
  - Security Assertion Mark-up Language (SAML) for making authentication and authorization assertions; and
  - XML Access Control Mark-up Language (XACML) for stating authorization rules.



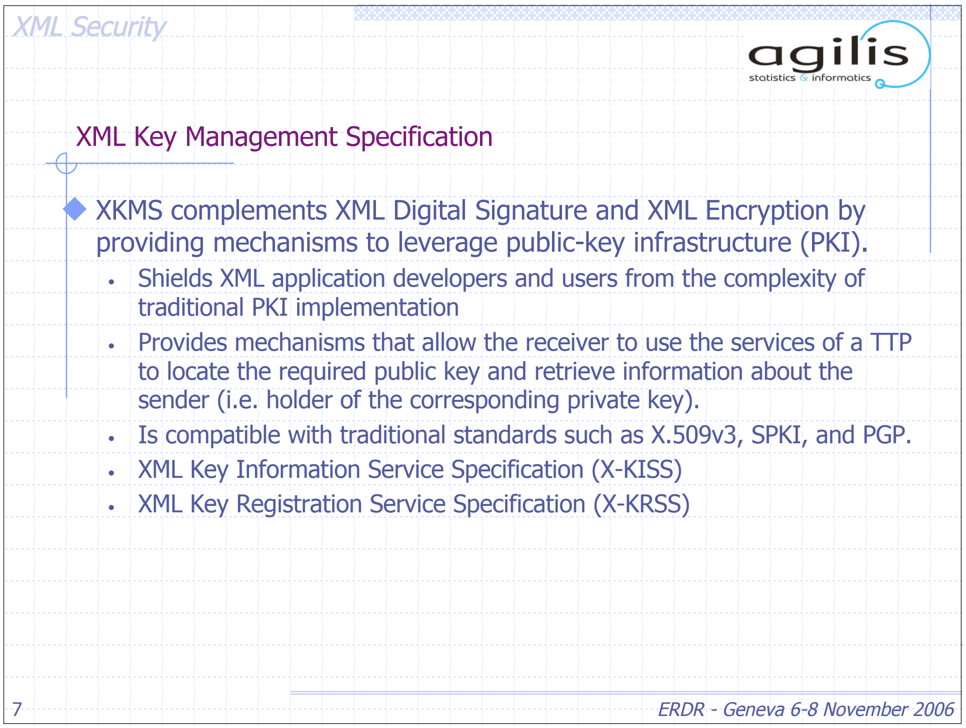
XML Digital Signature

- The XML Digital signature recommendation defines mechanisms to support the full range of digital signature creation and verification.
- It provides the versatility to sign and verify:
  - Entire XML documents as well as element and even element content portions of XML documents;
  - Arbitrary documents, including binary documents;
  - Compound documents including multiple documents and/or XML elements and element contents;
  - Properties to be included with a signature;
  - Counter-signatures (signatures that include other signatures).



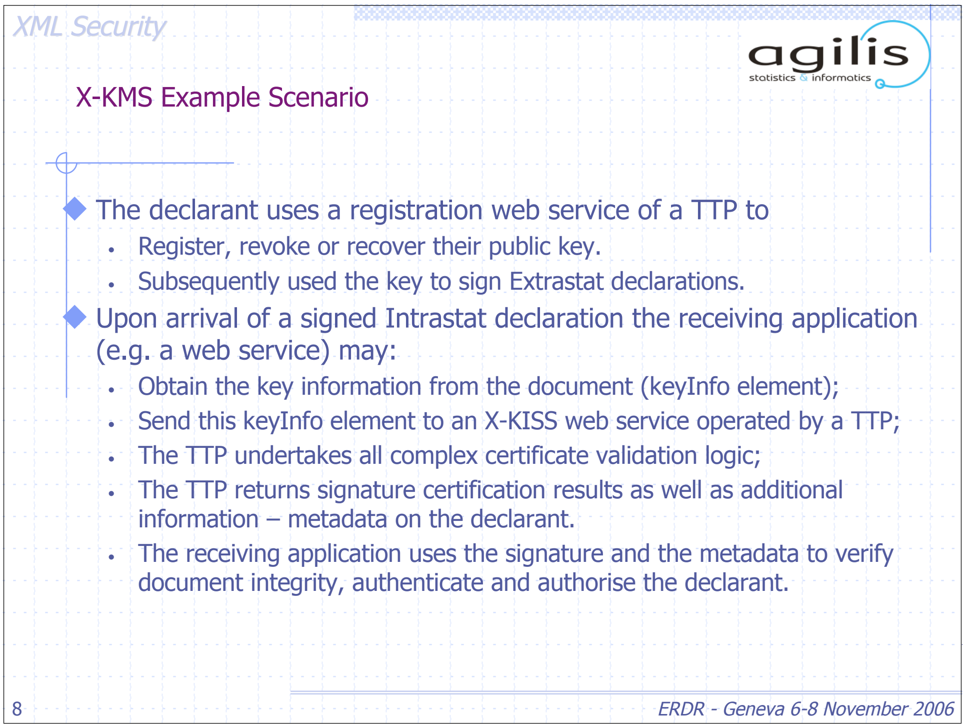
XML Encryption

- The XML Encryption recommendation defines the framework, vocabulary and processing rules for XML encryption and decryption.
  - Supports a variety of encryption algorithms
  - Encapsulates all the information needed to process encrypted content, such as encryption algorithm and parameters, information about keys.
  - Confidentiality may be applied at any level of granularity to XML content (XML elements, XML element content as well as entire XML documents) to secure only portions of XML documents routed through intermediary processors.
  - Allows combined use of asymmetric (for keys) and symmetric (for content) encryption to optimise performance.



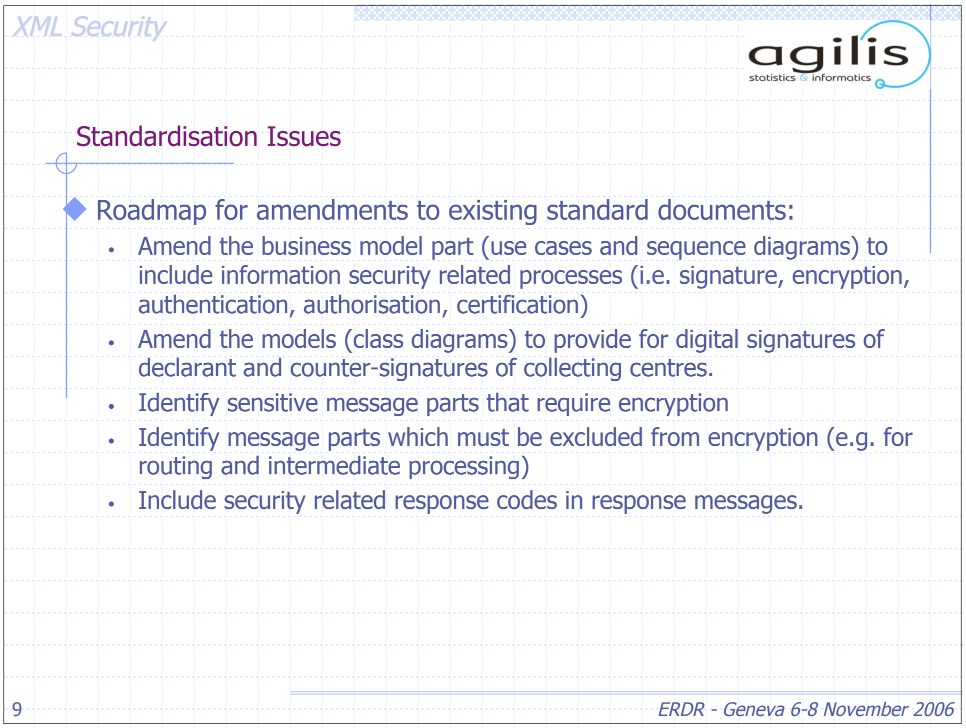
XML Key Management Specification

- XKMS complements XML Digital Signature and XML Encryption by providing mechanisms to leverage public-key infrastructure (PKI).
  - Shields XML application developers and users from the complexity of traditional PKI implementation
  - Provides mechanisms that allow the receiver to use the services of a TTP to locate the required public key and retrieve information about the sender (i.e. holder of the corresponding private key).
  - Is compatible with traditional standards such as X.509v3, SPKI, and PGP.
  - XML Key Information Service Specification (X-KISS)
  - XML Key Registration Service Specification (X-KRSS)



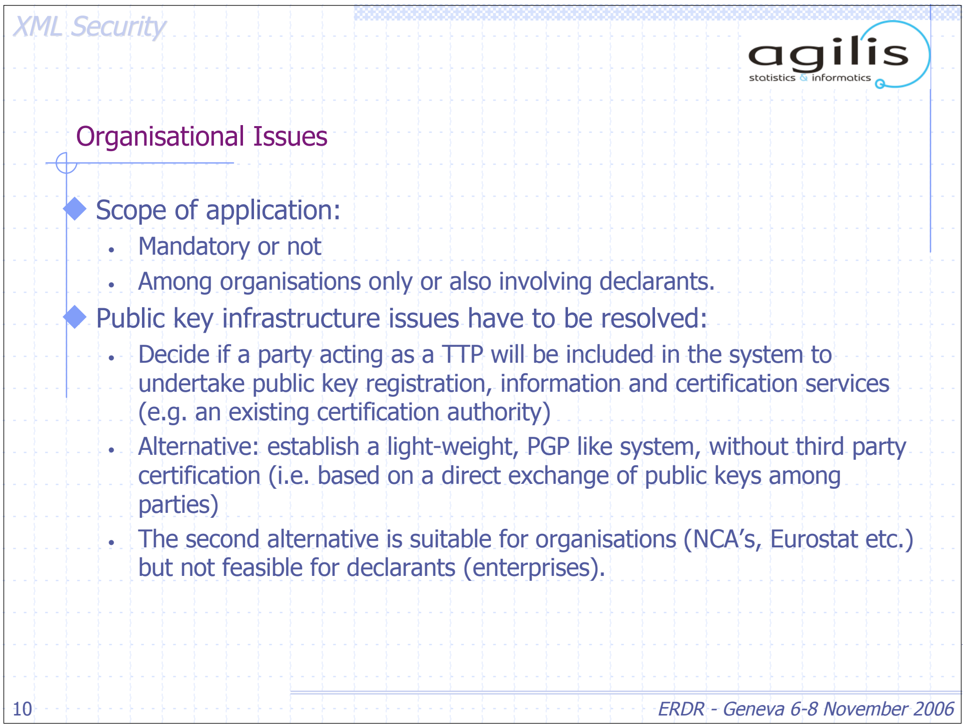
X-KMS Example Scenario

- The declarant uses a registration web service of a TTP to
  - Register, revoke or recover their public key.
  - Subsequently used the key to sign Extrastat declarations.
- Upon arrival of a signed Intrastat declaration the receiving application (e.g. a web service) may:
  - Obtain the key information from the document (keyInfo element);
  - Send this keyInfo element to an X-KISS web service operated by a TTP;
  - The TTP undertakes all complex certificate validation logic;
  - The TTP returns signature certification results as well as additional information – metadata on the declarant.
  - The receiving application uses the signature and the metadata to verify document integrity, authenticate and authorise the declarant.



Standardisation Issues

- Roadmap for amendments to existing standard documents:
  - Amend the business model part (use cases and sequence diagrams) to include information security related processes (i.e. signature, encryption, authentication, authorisation, certification)
  - Amend the models (class diagrams) to provide for digital signatures of declarant and counter-signatures of collecting centres.
  - Identify sensitive message parts that require encryption
  - Identify message parts which must be excluded from encryption (e.g. for routing and intermediate processing)
  - Include security related response codes in response messages.



Organisational Issues

- Scope of application:
  - Mandatory or not
  - Among organisations only or also involving declarants.
- Public key infrastructure issues have to be resolved:
  - Decide if a party acting as a TTP will be included in the system to undertake public key registration, information and certification services (e.g. an existing certification authority)
  - Alternative: establish a light-weight, PGP like system, without third party certification (i.e. based on a direct exchange of public keys among parties)
  - The second alternative is suitable for organisations (NCA's, Eurostat etc.) but not feasible for declarants (enterprises).