Ascertia Trust Solutions

Welcome to a Secure Digital World ...

Ascertia eID Solutions Presentation

November 2011

"Leveraging e-ID trust infrastructure for business and citizens"

eID schemes provide the core trust services that enable real business use

For successful solution delivery it is important to have simple to use, advanced digital signature services for documents and also be able to preserve data for years into the future

Rod Crook, Solutions Director
Ascertia Limited

Where can e-Identities be used

Web based end-user signing

- User interacts with a web app using standard browser
- There is no requirement for pre-installed signing software
- A signed Java applet is downloaded and interfaces with the user's e-ID card

Desktop end-user signing

- Various desktop applications
- Standalone (and offline) signing using e-ID card

Central signing

- In some cases keys can be held centrally for business users
- Business applications may need to sign on behalf of an organisation or department
- Bulk signing of documents (e.g. e-invoices)
- User and corporate eID signing keys held in a central HSM

A Digital Signature Framework is needed

The digital signature framework must:

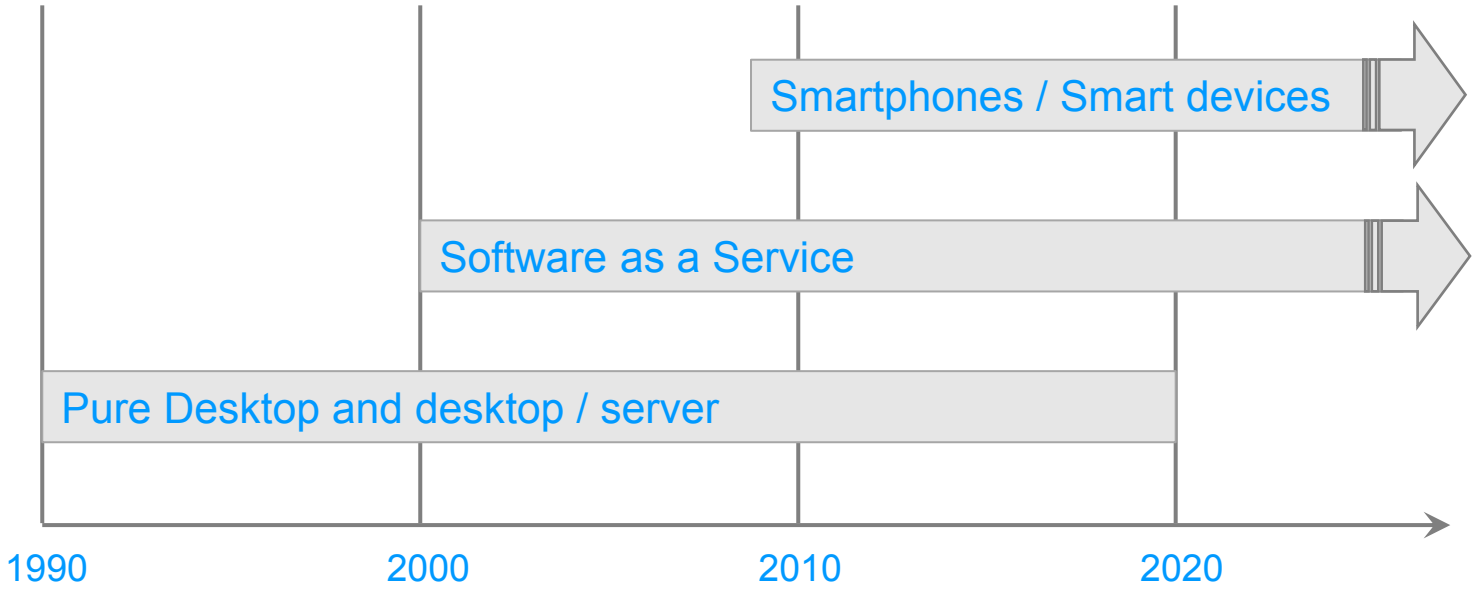
- Leverage the value and trust of the eID scheme
- Enable new and existing business applications to easily add digital signature and signature verification capabilities
- Ensure that the integration is simple and standardised
- Provide standards based interoperability for business documents
- Be able to verify EU Qualified Signatures
- Understand EU PEPPOL quality ratings
- Understand and apply long-term signatures

A Digital Signature Framework is needed

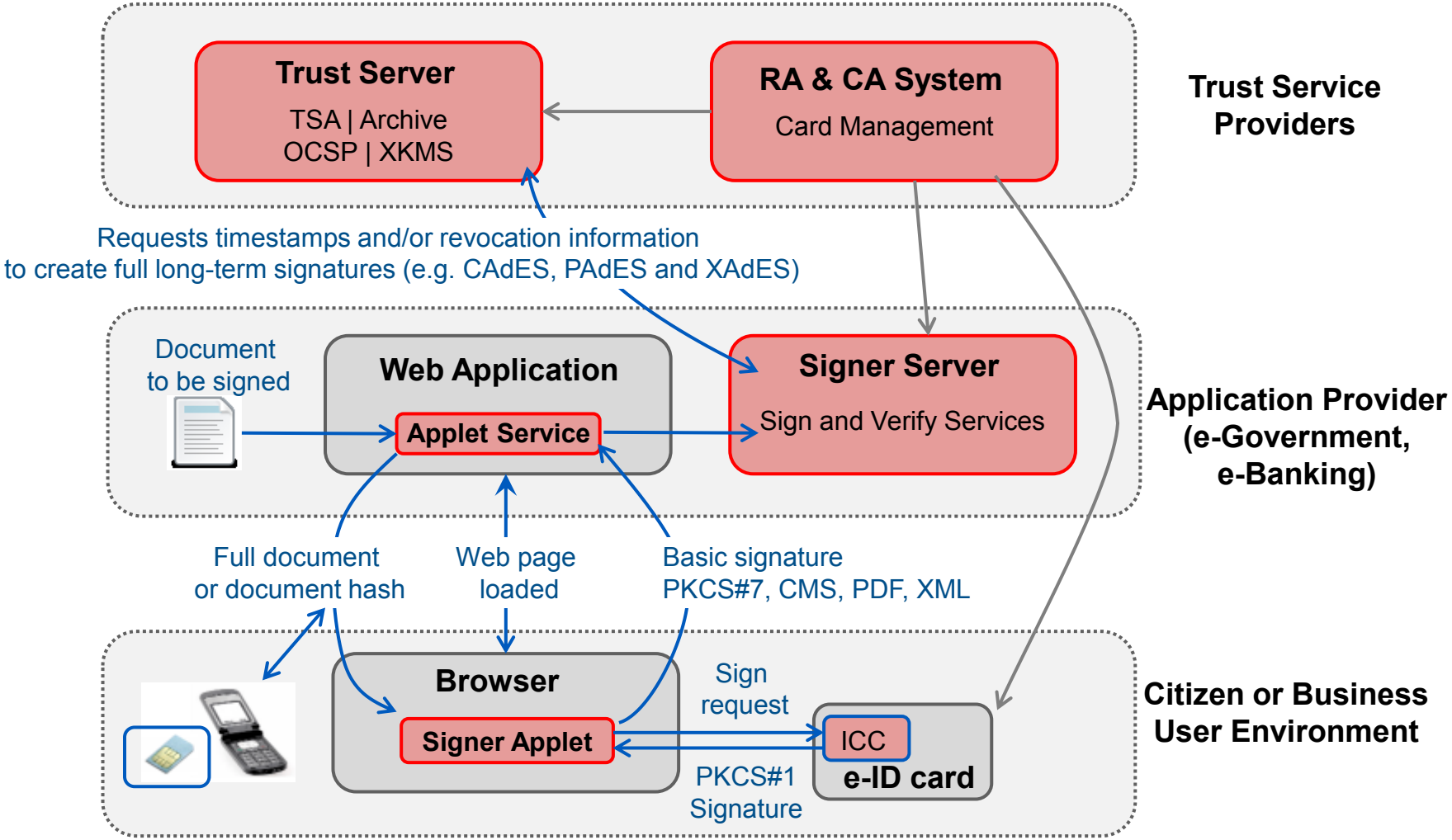
The digital signature framework must be flexible to:

- Support a full range of desktops / devices into the future
- Support a full range of open standard document and data types
- Support a full range of signature types
- Allow customised user interfaces
- Allow government or business level branding and localisation
- Interact easily with e-ID cards
- Select the right certificate without asking the user
- Make the whole signing process easy and prevent users from making mistakes
- Allows strong non-repudiation through WYSIWYS capability
- Support multiple platforms and allow user portability

It should support all user ‘desktops’ and gracefully enable future changes



Example Architecture



Standard signatures should be supported

	PDF documents	XML Data	Files / Forms
Basic signatures lifetime depends on signing certificate	**Basic PDF / PAdES Part 2** Certify / Vis / Invis	**XML DSig XAdES-BES**	**PKCS#7/ CMS S/MIME CAdES-BES**
Advanced signatures with ETSI policy information	PAdES Part 3 Sig	XAdES-EPES	CAdES-EPES
ETSI Long-term signatures containing timestamps and/or revocation references or full revocation information, and archive timestamps	**PAdES Part 2 + timestamp + Long-term** PAdES Part 4 (All CAdES options)	**XAdES-T** XAdES-C XAdES-X **XAdES-X-L** XAdES-A	**CAdES-T** CAdES-C CAdES-X **CAdES-X-L** CAdES-A
Ascertia support for signing & verification of all these signatures types	✓	✓	✓

What document types can you sign

- **What You See Is What You Sign (WYSIWYS) is important for good security**
- **PDFs are very good for this**
  - As flat PDF/A documents (no dynamic content)
  - As simple forms presented to a user
- **XML data and signatures are not so good**
  - Good for gathering web-form data
  - Not as good as PDF for WYSIWYS
- **Web-form data & file based signatures**
  - Not so good as PDF for WYSIWYS
  - Web-form data can be manipulated prior to signing

MITM and MITB security issues

- **Two issues exist now and for the future:**
  - Man In The Middle (MITM)
  - Man In The Browser (MITB)
- **MITM – can be prevented using client/server SSL**
  - Digital signatures on all key actions also prevent MITM
- **MITB – defence in depth is required**
  - Able to change web-forms behind the interface, so …
  - Use a web-form or PDF form and submit to the centre
  - The application converts everything as a signed PDF and signs this
  - The user is asked to review and add their signature
  - Document review is within a trusted viewer
  - Signing is within a protected applet / application
  - Any change is visible and detectable to the user and the centre

PDF Digital Signatures

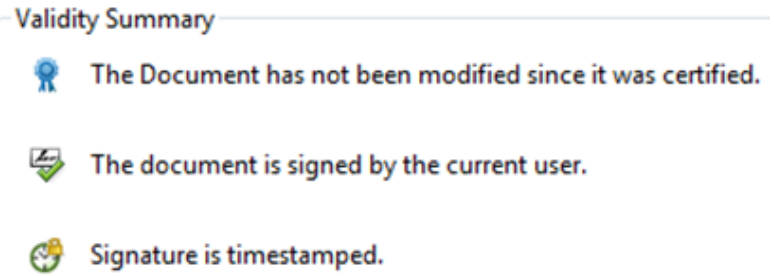
- **A good range of security options for multiple uses**
  - Visible and invisible signatures
  - Multiple signatures
  - Certify signatures, for controlling further edits to the document (e.g. one-way publishing and form content)
  - Supports long-term signatures with embedded timestamps and signer revocation information
  - Supports the latest algorithms e.g. SHA-2, RSA 2048
  - Example a signed datasheet….

ADSS Server Standards Compliance:

Interface standards:	OASIS DSS and OASIS DSS-X services (including over SSL/TLS), high speed HTTP/S protocols, Auto File Processor (AFP) Watched folders, Secure Email Server for email support, Java and .NET APIs
Signature generation:	PDF, PDF/A, XML DSig, PAdES 2,3,4, XAdES, CAdES (ES, -T, -C, -X, -Long, -EPES, -A), PKCS#7, CMS, S/MIME
Signature verification:	One or multiple PDF, XML DSig, PAdES, XAdES, CAdES, PKCS#7, CMS and S/MIME signatures
Signature enhancement:	Enhances PAdES 3,4, XAdES and CAdES signatures to include timestamp and certificate revocation data
Certificate validation:	Uses OCSP, CRLs, Delta CRLs, DPD/DPV or even XKMS and SCVP
Time stamping:	TSP (RFC3161)
HSM Support:	Any PKCS#11 compliant HSM, smartcard or token, e.g. SafeNet, Thales nCipher, Utimaco, AEP and others
Operating Systems:	Windows 2003 / 2008 (32/64 bit) Server, Linux (32/64 bit), Solaris 10, others on request
Databases:	SQL Server 2005/ 2008 (including Express), Oracle 10g, 11g, MySQL 5, PostgreSQL 8
Options:	**ADSS CA, TSA and OCSP Servers can also be used to provide advanced trust infrastructure services**

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

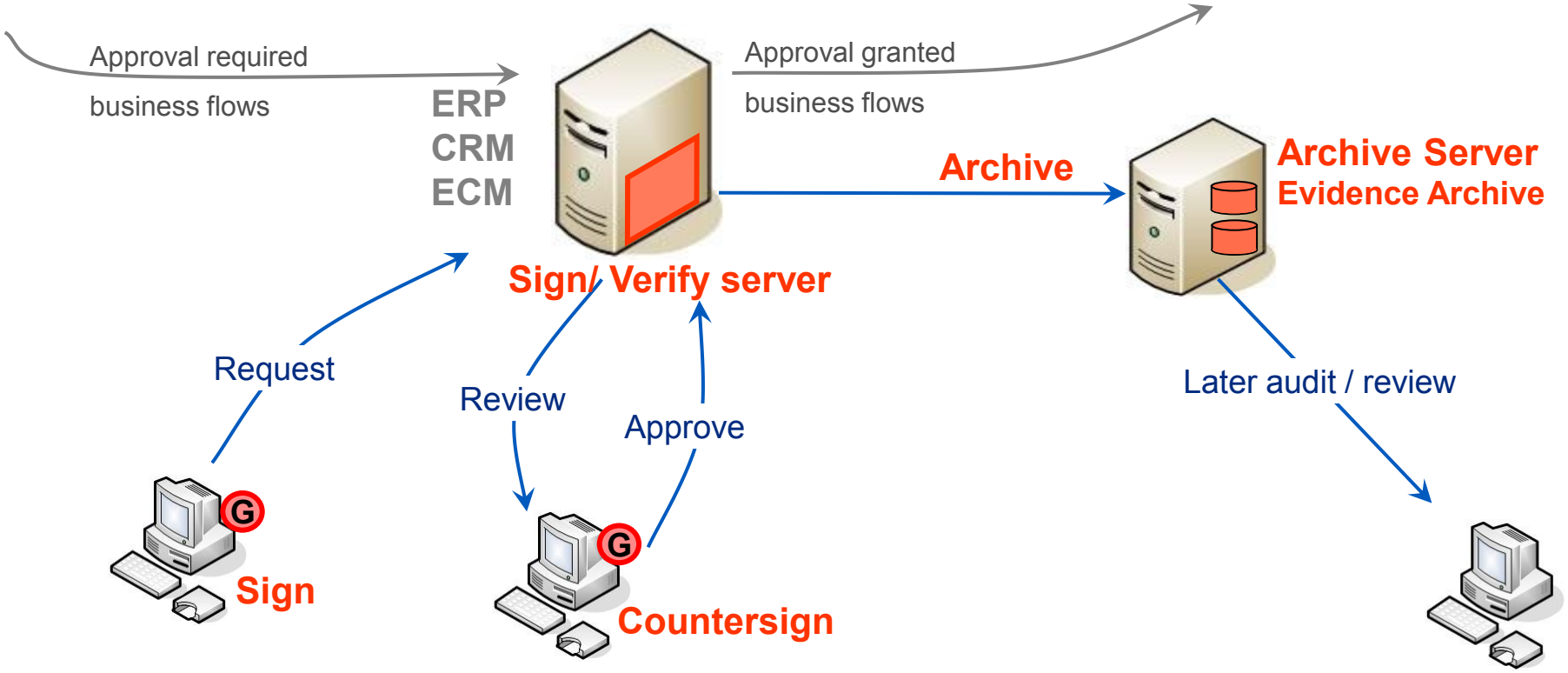
Digitally Signed By: Rod Crook
Reason: I approve this document
02/09/2011 12:47:13 GMT +01:00



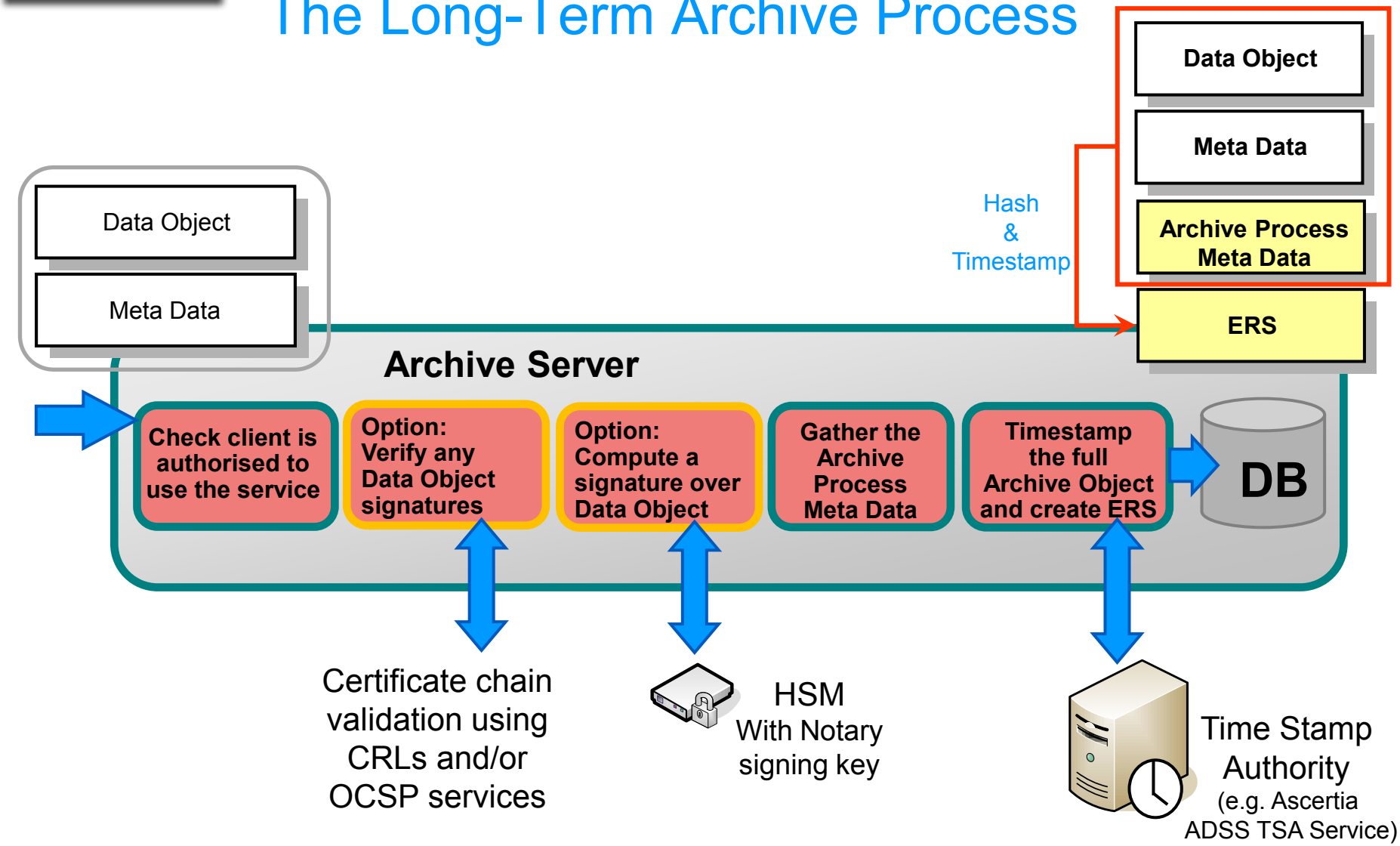
Archive and Protect Against Change

- **Document format changes**
  - Preserve any data or document as they are today
- **Preserve and protect weakening signatures**
  - Weakening algorithms and key lengths
    e.g. today SHA-1, RSA1024
    in future SHA-256, RSA2048
- **Allow for algorithm and key length changes**
  - Ensure hash and signing algorithm flexibility
  - Ensure key length flexibility
- **IETF LTANS**
  - is designed to create and continuously preserve document and data evidence records – useful for 2 to 100+ years

Workflow Agreement with Long-term Archiving



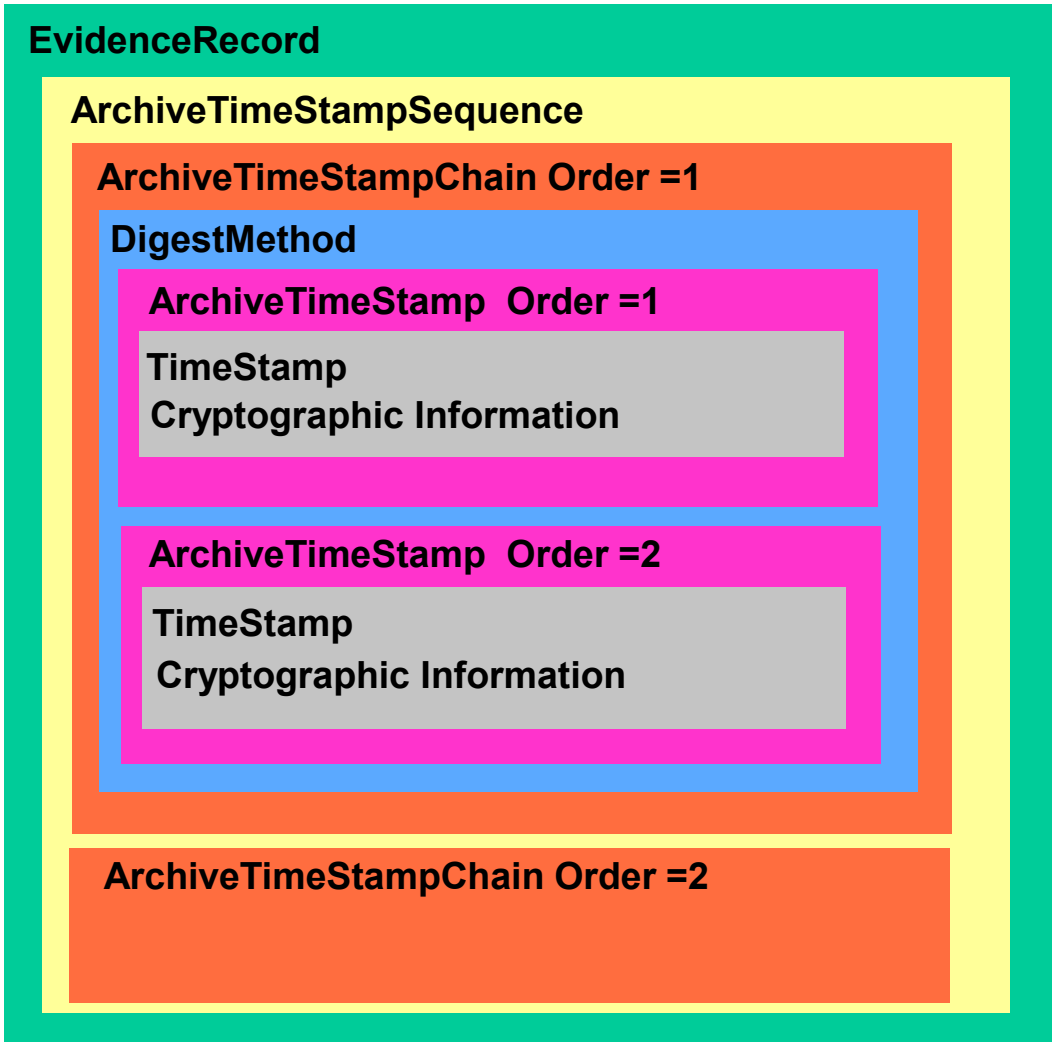
The Long-Term Archive Process



Evidence Record Renewal Structure

Evidence records are updated automatically during renewal following the Matryoshka Principle.

When algorithms change a new chain is started which includes a hash across the data object, meta data and existing ERS information



Trust Solutions Summary

- **Leverage the value of the eID trust scheme**
  - eID Certificates provide good trust
  - An OCSP Validation Authority helps long-term signatures
  - A Time Stamp Authority offers vital time-based assurance
- **Empower Government and Business use**
  - Use a capable and flexible digital signature framework
  - Use long-term signatures
  - Provide strong traceability, accountability & auditability
  - Use an Archive Authority for long-term data preservation
- **Make it easy for the user**
  - Avoid technically difficult questions or selections
  - Expect the user to make mistakes and prevent these

Identity Proven, Trust Delivered

info@ascertia.com www.ascertia.com

Ascertia is a global provider of e-trust products and solutions

Represented in Georgia by NGT Group