PKI – related technologies

Tadej Pukl
head of marketing and sales

SETCCE

Agenda

- SETCCE – short company introduction
- Results and partners
- SETCCE’s products and services
- SETCCE’s products in business practice
- eKeeper – trusted archive service

Company introduction

- **SE**curity **T**echnology **C**ompetence **CE**ntre

- Ljubljana, Slovenia, EU

- 15 people
- Young team
- Highly educated, experienced and motivated

- Over 10 years experience in PKI


Poland
Germany
Czech Republic
Slovakia
France
Austria
Hungary
SLOVENIA
Italy
Croatia

SETCCE delivering trust in e-business

Company introduction

- **Software development** through **research projects**
- **Research**: EU-projects in telecommunications security and privacy protection
- **Software**: Introduction of *digital signature* in business and governmental processes
  - Objecticve: fully de-materialized business processes
  - A wide range of technologies and components
- **Mission**: bridging the gap → technology transfer from research projects into industry / commercial sector

Company introduction

- **Legislative environment**
  - **Act on electronic commerce and electronic signature** (+ revisions).
  - Act on value added tax
  - Accounting standards
  - (Slovenian) archiving act

Company introduction

- **Act on electronic commerce and electronic signature** (+ revisions):
  - In force since 2000
  - Based on European directives (1999/93/EC, 2000/31/EC)
  - Framework for equalisation of paper and electronic format of documents
  - (Qualified) Digital signature
  - Management of digitally signed electronic documents

Company introduction

- **SETCCE's products:**
  - Compliant with EU's and local legislation
  - Compliant with global standards
  - Highest level of security
  - Related to Public Key Infrastructure
  - Introduction of digital signature (and supporting technologies) in current business practice

Company introduction

- **SETCCE's products:**
  - Specialized components intended for system integrators and developers...
  - Upgrades / add-ons to **existing** applications and information systems
  - Recognized and used worldwide

SETCCE's reference list

Some of our partners:

- nCipher
- H&S Software AG
- S&T
- SRC.SI
- ZZi
- Institute Jozef Stefan
- University of Ljubljana, Faculty of electrical engineering
- Univeristy of Stuttgart
- IAIK, Austria
- T-Systems
- Telenor, Norway
- Slovenian Chamber of Commerce etc.

- ...and still looking for fruitful long-term partnerships...

SETCCE's reference list

- **Most important users of SETCCE's technology:**
  - VeriSign, Inc.
  - Halcom (→Slovenian banks)
  - SiOL d.o.o.
  - Datalab tehnologije d.d.
  - Valmesa Property&Asset Valuations
  - Slovenian Ministry of Defense
  - Dafolo S/A
  - H&S Software AG
  - Chinese gov't: tax authority, ZhuHai
  - Sella bank, Italy
  - Italian Chamber of Commerce (Infocamere)
  - Simobil Vodafone, etc.

SETCCE’s products and services

SETCCE's products

proXSign product range

SETCCE's products (www.**proXSign**.com)

- **Components and software development kits for:**
  - **Digital signing** (W3C XMLDSig standard, XADES and PKCS7) + verification of signatures
  - **Encryption** (asymmetric - W3C XMLEnc),
  - **Timestamping** (RFC3161 and XML by Entrust)
  - Instant integration!
  - Widely used in the banking sector, ERP systems, real-estate companies, telecomm operators, governments, etc.

SETCCE's products (www.**proXSign**.com)

- **Practical examples:**
  - Integration into ERP systems for digital signing of single electronic invoices or any other documents (one by one)
  - In ERP systems: verification of incoming digitally signed electronic invoices
  - Integration into workflows (non-disputalbe audit-trail)
  - Digital signing of payment orders in e-banking
  - Pharmaceutical industry (tracing drugs from the production plant to the end-user)

  - Timestamp client, encryption tool, *W3C-recognized*

SETCCE's products

WebSign

SETCCE's products **(WebSign)**

- **Workflow systems:**
  - Instant generation of XML electronic forms (based on pre-set templates)
  - Secure exchange between involved parties
  - In the process each party can fill in the e-forms and apply digital signatures
  - Based on web-browser technology
  - Fully configurable (no limits)
  - Output = digitally signed XML document (optional stylesheet). No paper!
  - Used in governmentnal processes (MoD), employment agencies, telecomm operators

SETCCE's products **(WebSign)**

- **Practical examples:**
  - Signing of electronic contracts (ISPs) over the internet, signing of annexes, self-provisioning, etc.
  - Student employment agencies (filling in, signing and exchange of work reports)
  - Ministry of defense (requests for working tools for newly employeed, ...)

SETCCE's products

eBiller

SETCCE's products **(eBiller)**

- **Electronic mass-"invocing" systems:**
  - Automated **generation** of documents (XML, TXT,..., e-invoices or any other documents)
  - Multiple **controls** and checkpoints are integrated
  - Automated digital **signing** of generated documents
  - Automated generation of **messages** (S/MIME, SOAP, HTTP)
  - Automated **distribution**
  - Used by ISPs, telecomms, banking industry

SETCCE's products **(eBiller)**

- **Practical examples:**
  - Mass generation and distribution of monthly invoices for users of mobile telephony and internet services
  - Monthly banking acount statements

SETCCE's products

eKeeper

SETCCE's products **(eKeeper)**

- **Trusted electronic archive service:**
  - Storage of digitally signed and non-signed electronic content
  - According to the legislation
  - Not really an archive, but rather en **electronic notary**
  - An upgrade for existing DMSs, or as an independent instance on top of a FS or existing e-archive
  - Also available as a DMS-bundle
  - Used in governmental processes, telecomm operators, ISPs, banking sector

SETCCE's products **(eKeeper)**

- **Practical examples:**

...to be continued later

SETCCE's products

- **Certification authorities:**

  WWW.SI-CA.ORG

  – Set-up of the first CA in Slovenia in 1995
  – Part of EuroPKI
  – Still functioning

  – No business case in Slovenia

  – Experimental and demonstration purposes

SETCCE's products

- **Custom-projects:**
  - For large end-customers
  - Integration of SETCCE's technologies into cusomers' applications
  - Custom development of new applications
  - Consultancy and educational projects

Bottom-line

- **Conclusion: output/result is always *a* *digitally signed document*!**

- Total elimination of paper documents from a business process!

- **Questions:**
  - **how do we store/archive the output?**
  - **how do we manage the output?**

...electronic documents have “some” limitations!

Bottom-line

- **Answer = ...** **eKeeper**

SETCCE eKeeper

- General definitions
- Formal requirements (integrated in eKeeper)
- Functional requirements
- What is eKeeper?
- What does eKeeper do?
- How eKeeper works
- Infrastructure / implementation
- Extra features
- Technology

General definitions

- **Archiving** is a set of procedures of submission, retrieval, preservation, maintenance, professional management and usage of documentary and archival material, which is not used for current business anymore. Such procedures need to be performed over periods defined by formal and legislative requirements.

  (i.e. archiving is much more than storage)

- **An archive** is a collection of records and documents that have historical, cultural, scientific or business value and are stored on physical media.

Formal requirements for eKeeper

- Electronic records must be kept so that:
  - Data or content is accessible and usable at any time,
  - Archived content is preserved in its original form or in any other form that undeniably represents the original data,
  - The origin, time, location and the “owner” of an electronic record or message are undeniably identifiable
  - ...see next page

Formal requirements for eKeeper

- Electronic records must be kept so that:
  - Technology and procedures used must prevent any sort of modification, alteration or deletion of record, data or content – integrity is guaranteed at any time,
  - Complementary data and means for security attributes (e.g. digital signatures) are preserved for the same archiving period as records
  - Procedures and means for extending the validity of electronic attributes are accordingly implemented.

Functional requirements for eKeeper

- Trusted archive service must have the following basic operations:
  - Submit data objects to archive
  - Retrieve archived data objects
  - Delete archived data objects
  - Specify an archive period for submitted data objects
  - Extend or shorten the archive period for an archived data object
  - Specify metadata associated with an archived data object
  - Specify an archive policy under which the submitted data should be handled

Functional requirements for eKeeper

- Trusted archive service accepts
  - Raw data
  - Digitally signed data
  - Time stamped data
  - Encrypted data

What is eKeeper?

- A solution for long-term electronic archiving
- *A replacement for costly hardware solutions (Centera)*

  – Based on national and international legislation and directives for long term documents preservation
  – Based on global technical directions and standardization initiatives (IETF LTAP Protocol, encryption and hashing algorithms...)

  – An upgrade of existing DMSs

  – Provides long term stability of
    - Documents
    - Digital signatures

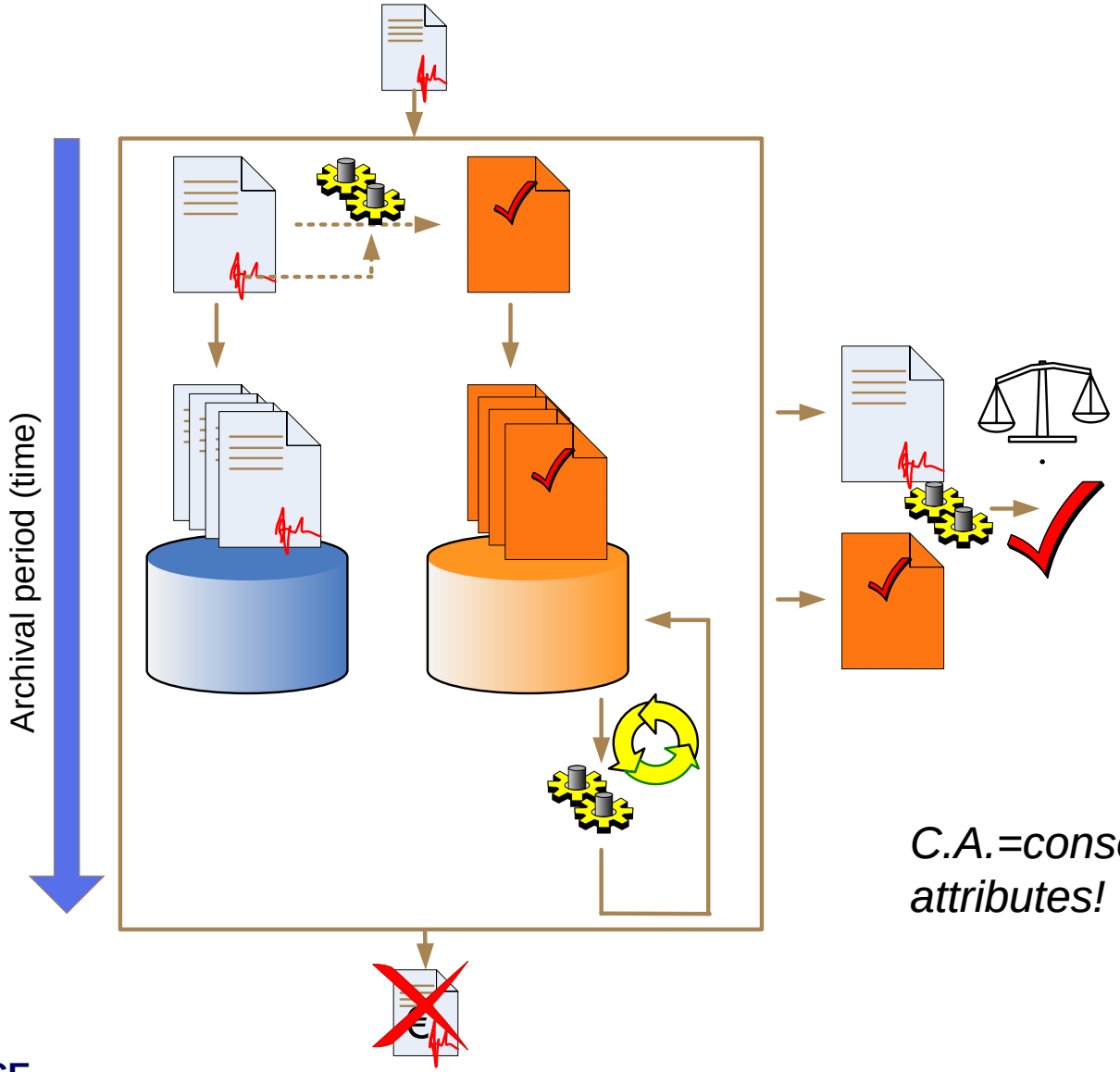
  – Designed for critical and heavy loaded environments

What does eKeeper do?

- It **provides evidence** that an archived document:
  - **existed** at a certain (clearly defined) time in the past
  - has **not been compromised** since it was digitally signed (or since it was submitted to the archive if it was not signed)
  - is still **legally valid** and will remain so **for the whole archival period**
  - still bears a **valid digital signature** (if applied). Validity of the signature will be maintained throughout the whole archival period!

- *In other words: eKeeper can demonstrate inegrity and legal validity of archived digital content for the complete archival period*

How eKeeper works



C.A.=conservation attributes!

How eKeeper works

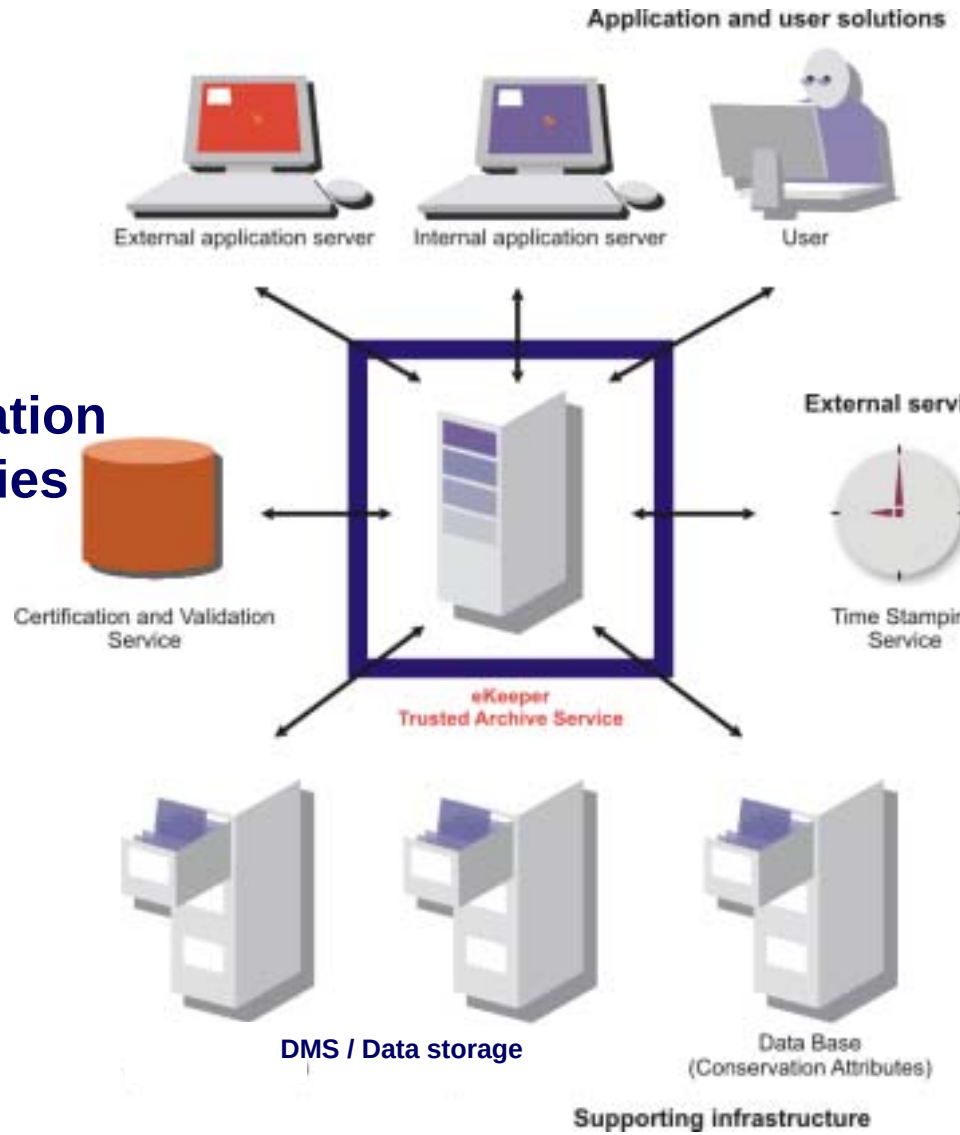
- Archived documents are left intact!
- Conservation Attributes are created upon entry
- Conservation Attributes are used to demonstrate documents' validity and integrity
- Conservation Attributes are refreshed periodically
- Timestamping is used (DSE!)

- Documents' validity is assured

Infrastructure

- Supporting infrastructure of trusted archive service
  - Communication network (and PKI)
  - Security mechanisms
  - Time stamping service
  - Data storage or document management system
  - Application systems and services

Infrastructure



nCipher DSE

(internal or outsourced)

Extra features (competitive advantage)!

- Grouping of archived documents to minimize the cost of timestamping!
- De-grouping without re-timestamping
- Privacy protection upon verification of documents

eKeeper is a substitute for dedicated hardware archiving solutions

Platform

- eKeeper Client
  - C++ / Java based
  - Integrated LTAP (long-term archive protocol)
  - Supported modes
    - Conservation attributes generation and storage
    - Conservation attributes generation and storage + document storage
  - Application programming interface included

Platform

- eKeeper Server
  - Java based
  - Integrated LTAP
  - Supported modes
    - Conservation attributes generation and storage
    - Conservation attributes generation and storage + document storage
  - Interfaces
    - DB interface (Oracle, mySQL, MSSQL…)
    - HSM interface (nCipher)
    - TCP/IP or SOAP interface

Operation requirements

- Platforms
  - Microsoft Windows, Linux, Solaris, HP-UX, AIX…
- Databases (conservation attributes)
  - Oracle, mySQL, MSSQL, DB2…
- Supported document management systems/environments
  - IBM Lotus Domino/Notes, EMC Documentum, H&S PAM Storage…
  - SAP R/3, Navision…

Standards

- Implemented standards
  - Data structures
    - W3C XML
  - Interaction
    - IETF LTAP
    - W3C SOAP
  - Integrity evidence
    - SHA1, SHA256, SHA384, SHA512
    - RIPEMD160
  - Signatures
    - RSA PKCS#7
    - W3C XMLDSig
    - ETSI/W3C XAdES
  - Evidence record
    - IETF RFC3161
    - Entrust XMLTS

Contact

SETCCE

Jamova 39
1000 Ljubljana
Slovenia, EU

++386 (0)1 477 3861
info@setcce.org

www.setcce.org