Long Term Management of Private Digital Assets

Prof. Dr. Heinrich Jasper
Technische Universität Bergakademie Freiberg
Artificial Intelligence and Databases
09596 Freiberg, Germany
Observations

• Growing amount of individual digital assets:
  – Personal digital photos: these should be accessible to great-grandchildren
  – Contract documents that hold claims against third parties for decades
  – Personal communication like e.g. love-letters (e-mail, SMS)
  – Certificates, degrees etc. from professional organisations or universities

• Individual assets are or will be used via networks:
  – On-line admission to universities and other organizations
  – On-line / off-line digital documents like driving licence, passport etc.
  – Internet based personal services like banking, shopping etc.

• Result: Digital artefacts of individuals are of growing importance
Example: paperless student administration

**Students side**
- Admittance to Institution
- Define and send documents
- Documents delivered

**Administrations side**
- Admission request
- Completeness test
- Admission test
- Admission not successful
  - Additional docs. received
  - Docs. not complete
  - Additional docs. request
- Admission successful
  - Student accepted

**Icons:**
- Event
- Result
- Process step
Requirements / Goals

- Requirements for Private Digital Asset Management:
  - Provide long term \textit{preservation} of digital assets (LPDA: long living private digital asset)
  - Digital assets must be \textit{accessible} to humans today and in the future (accessible via eyes, ears, …)
  - Digital assets are used (on-line) in \textit{transactions controlled by owner}

- Resulting efforts
  - Digital assets should not depend on hardware/software/networking technologies
  - Digital assets must autonomously migrate into future environments
  - Secure interaction / exchange of assets assured in the long run

- Individual needn’t (shouldn’t!) care!
Known solutions / approaches

- Long term management of digital information:
  - Archaeological approach (secure old systems completely)
  - Emulation of old in existing (new) infrastructure (HW / SW)
  - Manual migration on a regular basis (e.g. every 2nd decade)
  - Special architectures for migration (e.g. UVC)
  - Technical support for migration (e.g. PLM)
  - HD-Rosetta (microscopic text on hardened nickel surfaces)
  - ...

- Secure on-line asset exchange:
  - Public key infrastructure for trustful interactions
  - Re-signature of assets necessary in the long run
Our approach

Provide Private Digital Asset Management in Time via:

• Virtual machine for
  – Persistent and secure storage (extension of the J2EE DAO pattern)
  – Information exchange (extension of J2EE TO pattern)
  – Metadata explicitly provided for each LPDA
  – Ontology for mapping each LPDA into private context

• Proactive Agents
  – Monitoring changes in the virtual machine instance: activating migration process if necessary
  – Monitoring the environment of the virtual machine: activating re-signature of assets if necessary
Digital Asset Management in Time

Cyberworld

Migrate assets

Retrieve asset

Insert asset

Sign asset

Re-signature (third party assets)

Re-signature (own assets)

LPDAs

LPDAs

LPDAs

ID(U1,T3)

ID(U1,T1)

ID(U2,T2)
Supporting Technology: Metadata and Ontology

- **Meta data**
  - Self-contained data (and meta data)
  - Extends standard RDF-types by
    - Formatting information (in abstract syntax)
    - Presentation algorithm (in abstract syntax)

- **Ontology**
  - Self-aware data and it-infrastructure
  - “Knows” IT infrastructure
    - Old and new,
    - Abstractions of storage principles, database formats, communication channels, security features, …
    - Hints for migration process
Architecture of Prototype

- "Event Shower" From Cyberworld
- PDAM Component
- Event Monitoring
- Proactive PDA-Monitoring Agent (PAPDAMA)
- PDAM Infrastructure Components (PDAMIC)
- PDAM Services
- Asset Storage
- Meta Data
- Public Ontology
- Private Ontology
- AI & DB, H. Jasper
Re-Signature of a digital asset

LPDA (Asset, Document)

Asset Data

Signature 1

Attribute (e.g. Algorithm)
Certificate
Signature 1

Signature 2

Attribute (e.g. Algorithm)
Certificate
Signature 2

Hash Value 1
Private Key 1
Signature 1
Hash Value 2
Private Key 2
Signature 2
The Migration / Preservation Process

- As much automated as possible

- Set-up for process (by IT-System supplier)
  - Define meta data for long term preservation
  - Define data conversion frames where necessary
  - Define migration ontology for migration of existing IT

- Process: each time a new IT-infrastructure is to be installed
  - Get Migration Ontology of new IT
  - Generate or construct migration routines (fill out frames)
  - Migrate data onto new platform
  - Migrate meta data onto new platform
  - Update archiving ontology of new IT
  - Get rid of old infrastructure
Status / Open Issues

• Feasibility study ongoing
  – PDAM based on virtual machine approach
  – Content of ASCII / UNICODE documents well suited
  – Open document infrastructures dito (e.g. TeX)
  – Standard Ontology technology incorporated

• Open Issues
  – Layout information critical
  – Graphics and pictures even more critical
  – Concentrate on well defined open formats for non-character-information (which one?)
  – Ontology must evolve over a very long time period (centuries)
  – Private Ontology not well understood

• Other topics
  – Ontology: “intelligent manual”, if necessary for future users
  – Proactive objects with own volition to survive migration of infrastructure might be the future
Thank you!