

Secure Document Circulation

S. Bracher P. Krishnan

Centre for Software Assurance
Bond University, Australia

JeH,SAC08

Background

- Interoperability for e-business
 - Different units share information
 - These units can be from different organisations
 - Multiple documents
 - Easier to enforce security properties
 - Loses logical structure
 - Hard to get a unified view
 - A single document will have different types of information
 - Easy to get a unified view
 - Security is a major issue
 - Possible to have a “single logical” view; but most tools require them to physically together.

Security Goals

- Workflow management and security of data need to interact
- Different nodes have different policies
- There are also global policies
 - Separation of duty
 - Secrecy/Privacy
 - Need to know principle
- Hard to anticipate all security issues
- Design and develop a general architecture: policy driven

Understanding DRM

- Digital Rights Management claims to address access related issues
- Policies are global: outside the data
- Enforcing rules centrally is hard when data can move from one entity to another

Example–1

- Customer applies for loan
- Pre-processing clerk: identity check
- Credit checking agency: has information not available to others
- Post-processing clerk: decision based on result from the credit check

Post-processing clerk is not the same as pre-processing clerk

No one can see how the other person arrived at a decision

Example-2

- Doctor recommends tests after a series of consultations
- Result from pathology can be read by the doctor
- Doctor prescribes medication

Pathology cannot access consultation notes

Pharmacist can look only at the prescription

Doctors: recommender and prescriber should normally be identical

Example–3

- Inspired by WEMS : Ecomessage
- Person on the field enters data on “environmental crime”
- Data shared with various departments: forestry, crime branch, researchers:data aggregation

Only crime branch needs to know the passport details of alleged offender

Data aggregation should be anonymised

All field data should be routed to federal ministry via state offices

Observations

- One workflow/service has many related data items
- Security requirements on these items
- History on access required for checking validity

E-Health Standards

- Many standards organisations: ASTM, ANSI, ISO, CEN
- Many standards available
 - Messaging: HL7, ASTM-E1238, IEEE1073.2.1.2
 - EHR: Dicom, HL7, ASTM E1384
 - Security: too many

Issues

- Standards are prescribed
- Product(s) to support interoperability
 - Standards have optional parts
 - Even if agreement in common parts behaviour undefined when different optional parts exist
- Security issues totally ignored

Standards solve nothing unless vendors agree on the specifics.

Goals

The key requirements to support *security* aspects in such applications are:

- Support workflows
- Support role based access control
- A single document having many components towards solving the interoperability problem

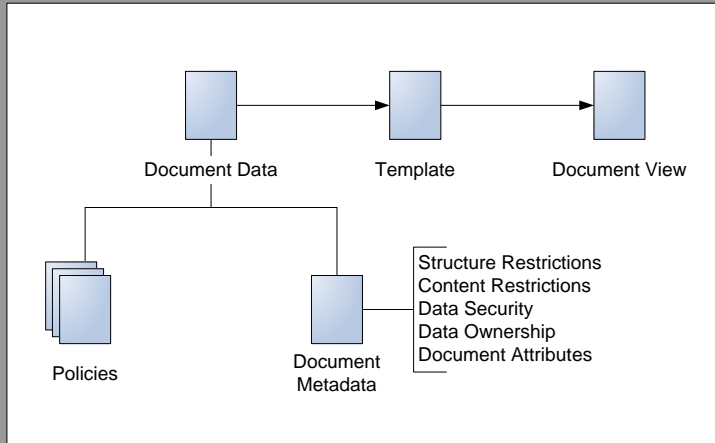
The standardisation, assurance and semantic interoperability processes are *not* considered.

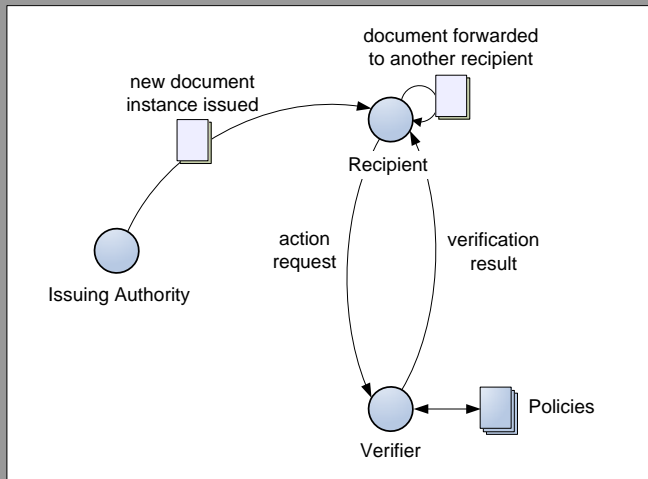
Problems Raised

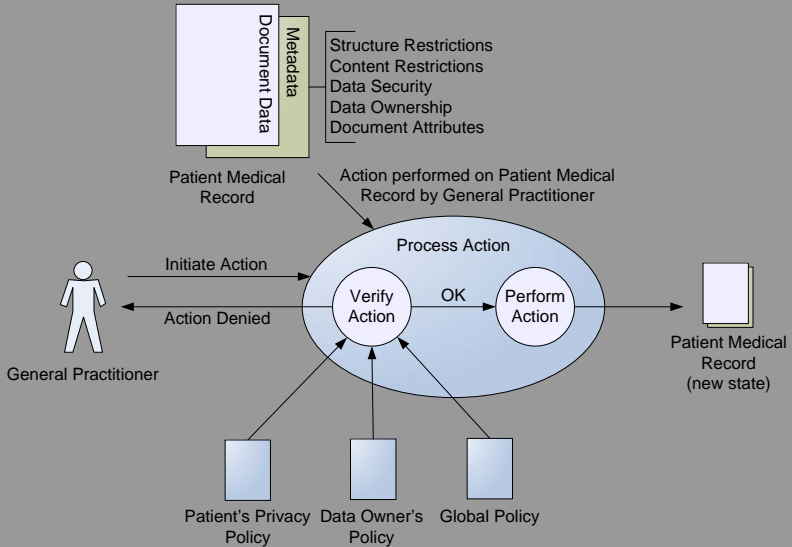
- Single document introduces privacy concerns
- How to safeguard information in the document
- Cannot rely on local security domains
- Policy can be “global” or “owner-based”
- Check if document satisfies the policies

Document Model

- Document has sections: each section can be encrypted differently
 - Each section can be stored separately
 - Implementation for each situation is more involved
- Access to decryption keys determined by policies
- Each section has metadata which encodes the relevant policies
- Cannot prevent a rogue agent from 'munging' data
 - Validate data before accepting it







General Example

- *A* can read all sections
- *B* and *C* can read and write sections 1 and 2
- *D* can append to the document

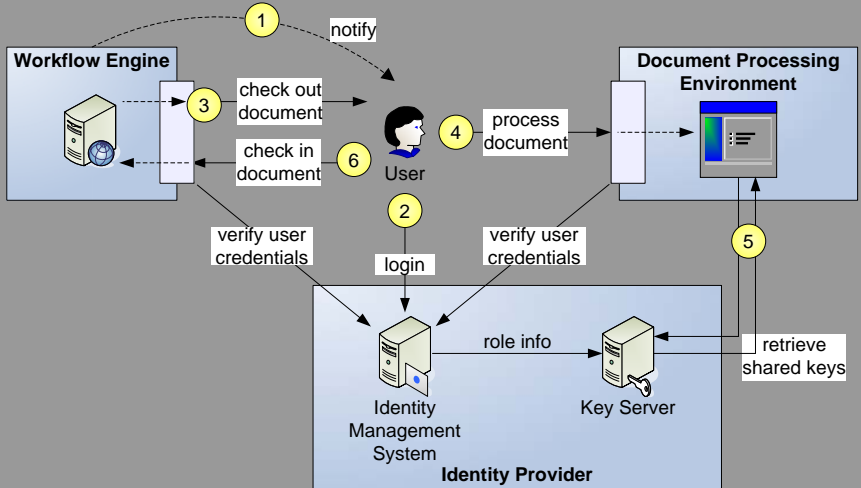
Solution

- Document encrypted with K_{doc}
 - Decrypted only when A , B or C present their credentials
- Sections 1 and 2 encrypted with $K_{A,B,C}$
- Verifier
 - Check A has not modified sections 1 and 2
 - Check B , C have not added any new section
- Checkin : B , C and D 's changes, section 3 (created by D) encrypted with K_A

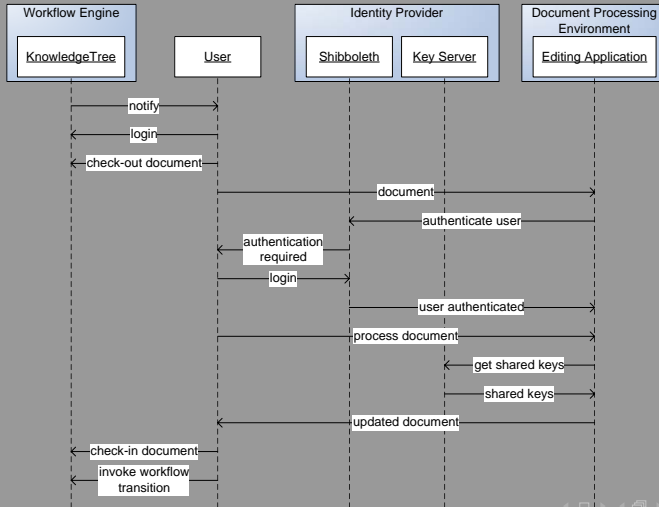
Components

- Workflow engine: Knowledgetree
- Knowledgetree also acts as document server
- Identity provider: Shibboleth/Central Authentication Service
- Document Processing Environment
 - Depends on application
 - Common parts such encrypting/decrypting/signing

Setup



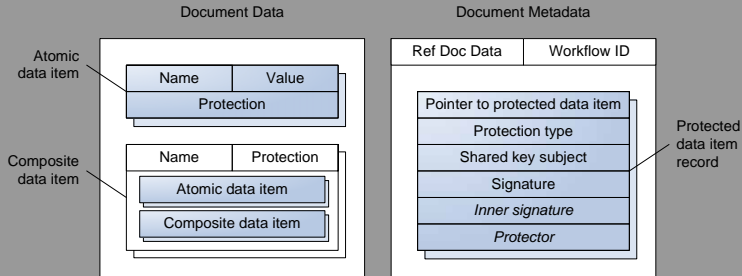
Behaviour



Overview

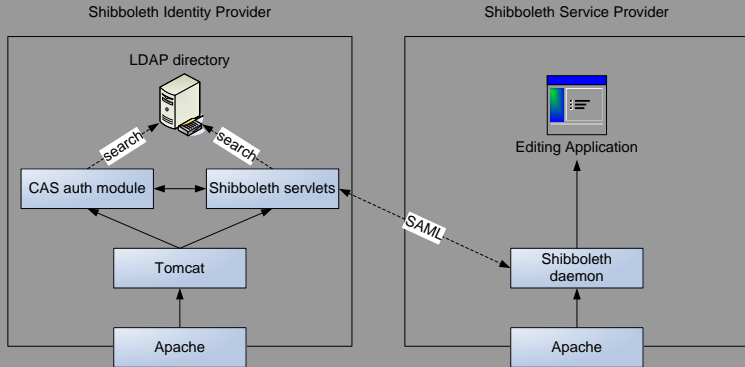
- All access is controlled by the identity provider
- The workflow engine stores the documents but they are not accessible
- At any given time only one user can work on a document (there is no inbuilt concurrency control)

Document Design



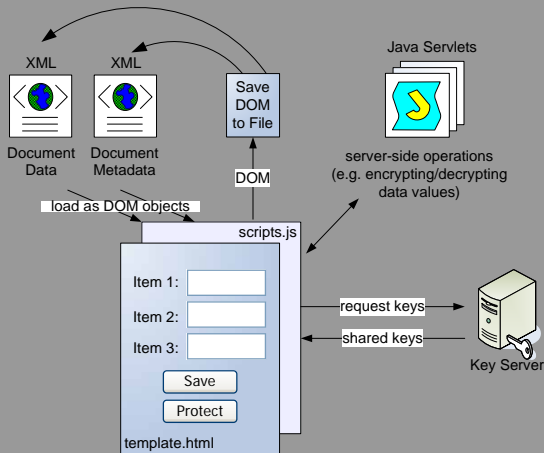
- The metadata points to the document
- The protection determines the type of keys/signature

Identity Provider

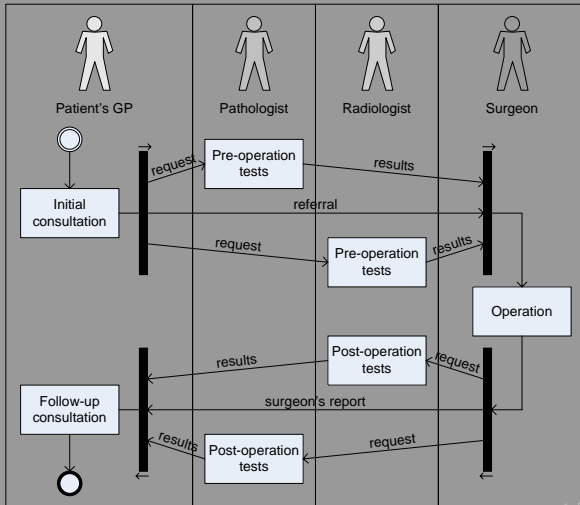


Standard set up

Document Processing



Medical Example



Implementation

- The document management system (DMS) is the eHealth authority
- GPs, specialists, laboratories log into the DMS
- Concurrency present: but on different “sections”
- Individual test results are writeable/readable only to the lab that conducted the test.
- Individual test results are readable by:
 - Patient
 - GP
 - Specialist

Data Records

- Workflow history: signed by user and role
- Medical record: application specific: referrals, requests, results, reports
- Such data records are application specific and require the most work

Key Aspects

- The architecture provides a general infrastructure
- Need to write only the application specific components
 - Logic/flow of data
 - Document metadata: History?
 - Verifier
- Number of shared keys can be high: depends on which subsets can access data
- Provides a plug/play set up

Conclusions

- Security can be combined with workflow
- The prototype implementation works well
- Further experimentation is needed to determine scalability
 - Key Servers
 - Single document
- How does this architecture relate to SoA, Web Orchestration etc.?
- What are the principles?