WP 5 Work Package Meeting

Security architecture and framework
Design and pilot implementation

3rd AGM in Munich, 17 February 2015

TUM: Raffael Bild, Florian Kohlmayer, Helmut Spengler
EBI: Olga Melnichuk, Marco Brandizi, Ugis Sarkans
Session moderation: Wolfgang Kuchinke
Security architecture and framework

- Guideline for secure, privacy preserving, ethically and legally sound data bridges between RIs
- Builds upon results from WT 5, 6, D5.1, and D5.2:
  - Usage scenarios developed for D5.1
  - Legal and ethical groundwork performed for D5.1 and D5.2
  - Two security and privacy related surveys carried out in WT5
  - A threat and risk analysis performed in WT6
- Designed in WT7
- Reported in D5.3
- Is laying the foundation for D5.4
Based on surveys, a threat and risk analysis was performed in WT6, using a variant of the
- STRIDE [1] methodology (security threats),
- LINDDUN [2] methodology (privacy threats), and

The threat and risk analysis comprised 7 process steps which were applied to the use case WPs:

1. Define usage scenarios
2. Gather a list of external dependencies, as-is state of security measures, and security assumptions
3. Create one or more Data Flow Diagrams (DFDs) of the application being modeled
4. Determine threat types
5. Identify the threats to the system
6. Determine risk
7. Plan mitigation

- usage scenarios from D5.1
- based on the surveys
- by suggesting countermeasures based on literature review
## Threat and risk analysis - Results

<table>
<thead>
<tr>
<th>Privacy Threat (LINDDUN)</th>
<th>Example</th>
<th>Risk</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linkability</td>
<td>Possibility to detect that different data items are related to the same entity</td>
<td>++ - ++ +++ ++</td>
<td>- Anonymization&lt;br&gt;- Pseudonymization&lt;br&gt;- Encryption&lt;br&gt;- Access Control</td>
</tr>
<tr>
<td>Identifiability</td>
<td>Possibility to relate a set of data to a specific entity / person; to recognize a person by characteristics of data</td>
<td>+++ + +++ +++ ++</td>
<td>- Legal regulations&lt;br&gt;- Informed Consent Mgmt.&lt;br&gt;- Data Provider Forms&lt;br&gt;- Ethics Committee approval&lt;br&gt;- Data Access Comm. approval&lt;br&gt;- Data Use Agreement&lt;br&gt;- Material Transfer Agreement</td>
</tr>
<tr>
<td>Content unawareness</td>
<td>A patient is unaware of the information used/shared by the system</td>
<td>++ ++ +++ ++ ++</td>
<td>- Informed Consent Management</td>
</tr>
<tr>
<td>Policy/consent non-compliance</td>
<td>Lack of evidence that data shared by the system meets applicable legal, policy or consent requirements</td>
<td>+++ ++ +++ +++ ++</td>
<td>- (not relevant), + (low), ++ (medium), +++ (high)</td>
</tr>
</tbody>
</table>
Security architecture - Overview

- Based on requirements collected in WT 5 and on the threat and risk analysis performed in WT 6
- Countermeasures against threats identified in the risk analysis
  - For each countermeasure:
    - Definition of measure
    - Description of threats addressed
    - Options for implementation and deployment
- Specification of three access tiers
  - Open
  - Restricted
  - Restricted & committee-controlled
- Activity diagrams describe actions for each access tier
Security architecture - Elements

- Specific countermeasures presented and discussed in detail include
  - Authentication
  - Authorization
  - Secure data communication
  - Encryption of data
  - Anonymization
  - Pseudonymization
  - Auditing and provenance management
  - Regulatory elements, such as
    - Data Use Agreements (DUAs),
    - Material Transfer Agreements (MTAs),
    - Informed Consent (IC) management,
    - Data Access Committee (DAC) approval, and
    - Ethics Committee (EC) approval.
Security architecture - Workflow

e.g. activity diagram for the restricted & committe-controlled access tier:

1. ALL data (on all tiers) transmitted between participating OEs have to be sent over secure communication channels.
2. It is assumed that standard web technology will be used (i.e. the provider has a SSL-Certificate [process of certificate acquisition omitted here]).
3. This works the consumer to verify the identity of the provider and to establish a secure connection.
4. This allows the consumer to verify the identity of the provider and to establish a secure connection.
5. Most probably using HTTP over SSL/TLS protocol (browser use case).
6. The client authentication is performed if restricted data is requested. No statement will be made regarding the used client credentials (certificates, smartcards, passwords, biometric identification, multi-factor authentication) as they will probably differ for different providers.
7. It is required that each requesting user has either an local account at the providing entity or is registered at an identity provider accepted by the data provider.
8. All relevant actions have to be locally audited/logged by the responsible provider.
Pilot for the security framework

- Demonstrates feasibility and usefulness of the security architecture by implementing it for a concrete WP4 use case
- Constitutes a collaborative implementation of secure access to biobank data involving ELIXIR and BBMRI
  - Based on results of WT 5, 6, 7, and D5.3
- Integrates and extends already existing results of WP4
- Integrates the policy administration repository from D5.2
- Is being implemented in WT8
  - Lead: EMBL-EBI
- Will be reported in D5.4
Pilot - Overview

- **Use case**
  - Researcher wants to obtain microdata / samples
  - Researcher looks for biobanks focusing on disease group x, containing at least y samples of material type z

- **The pilot will implement a complete research workflow**
  - To answer such queries in a secure, privacy preserving, legally and ethically sound manner
  - Instantiating the security architecture with all access tiers
Pilot - Central elements

- **BioSamples Database** from ELIXIR
- A prototype instance of the BBMRI catalogue (bbmri.eu, bbmri-lpc) comprising a MIABIS [1] layer and a data cube layer in order to provide a realistic environment
- **Single Sign On** service
- **Resource Entitlement Management System**
- **Legal Assessment Tool** built for D5.2

Pilot - Workflow specification
Pilot - Detailed progress

Work performed:
- Adaptation of the BBMRI software
- Implementation of SSO using Shibboleth
- Integration of REMS

Remaining tasks:
- Integration of (mockup) biobanks
- Integration of the LAT
Pilot - SSO login
Pilot - SSO login

Haka-test federation login page
Shibboleth Identity Provider Login to Service Provider "TUM SP"

This box demonstrates information gathered from MDUI-elements of the Service Provider. Read more from this link (in Finnish). You can enter the information about your service to Resource Registry.

Before logging in, please make sure information given below matches to the service you are trying to use and you agree with its privacy policy.

Service didn't report logo.

Service: TUM SP
Description: TUM SP
Privacy policy: Privacy Policy Service
Support contact: Oiga Melinchuk
Pilot - Refinement of the request
Pilot - REMS application form
Pilot - Provision of the requested data
Lessons learned

- All three access tiers are helpful regarding concrete use cases
- A risk analysis provided valuable input for the security architecture
- The BBMRI node can be integrated into a secure workflow
Thank you!

- Any questions?