Rights Delegation in the Trustworthy Healthcare Platform
healthcare trustworthy platform

TClouds Infrastructure

- TClouds Trusted Virtual Domains Service
- TClouds-Hardened Virtual Machines with Encryption
  - Healthcare Business Services
  - Data Sharing Control
  - Platform Database Management
  - TClouds Crypto Service
- TClouds Trustworthy Log Service
- Attestation of VM Requirements
- TClouds Secure Data Replication
characteristics

- Privacy Policies, End-User’s Responsibility & Third Parties
- Secure In-Transit Data
- Legal Compliances
- Trusted Audits and Log
- Security on Commodity Clouds
- Secure Data Storage
- Geolocalization of EHR Databases
- REST interfaces to support applications
ecosystem

Healthcare Professionals

Family

Patient/User

App market-like

Application (e.g., Smart-monitor, prog EHR mgmt, wellness, wellbeing...)

Healthcare Business Services

Data Sharing Control

Healthcare Trustworthy Platform

Platform's PHR User Data
requirements

- patient is in control of his or her personal health data (includes EHR)

- hospital personal needs access e.g.
  - doctor to add and read data
  - administrative personal to make appointments

- devices need to be able to add data e.g.
  - activity by ActiWatch
  - weight information by a scale
use cases

1. owner
   - user accesses his or her own data
2. client
   - user delegates right to access (part of) his or her data to an independent device
3. authorized user
   - user delegates right to access (part of) his or her data to another user
4. authenticated user
   - user delegates right to access (part of) his or her data to an application to be used by any identified user
User PHR/EHR

Relationship

Used (OAuth2.0) terminology

- Resource owner
- Consumer
- Resource server
- Client

- user
- app
- privacy policies

access to user’s PHR/EHR based on rights delegated to app
use case: owner

- user accesses his or her own data
- uses standard OAuth 2.0

AS = Authorization Server
RS = Resource Server

= Owner Grant
= Refresh Token
= Access Token
= Requested resource

Request resource

Request grant

Request grant

Grant accompanied by credentials
use case: client - setup

- Owner delegates rights to client
- OAuth2.0 framework is sufficient

Who?

owner credentials

Resource owner

Client

AS = Authorization Server
IP = Identity Provider
RS = Resource Server

= Owner Grant
= Refresh Token
= Access Token
= Requested resource
use case: client - resource access

- Refresh Token to generate Access Token with limited lifetime
- Same access token can be used to perform several accesses.
- Lifetime for refresh token established by owner.
- Difference w.r.t. to OAuth 2.0, client is autonomous
use case: authorized user - setup

- user delegates right to access (part of) his or her data to another user
- consumer are specific THP users, THP keeps track of delegations
- Identity of consumer required by client.
- Rights given by the owner to the consumers, not to the app/client.
- OpenIdConnect needed.
**use case: authorized user - resource access**

- Refresh Token to generate Access Token with limited owner-scope
- Same access token can be used to perform several accesses.
- Lifetime for refresh token short. One refresh token per session.
- Consumer must be online.

**Symbols**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>= Owner Grant</td>
<td></td>
</tr>
<tr>
<td>= Refresh Token</td>
<td></td>
</tr>
<tr>
<td>= Access Token</td>
<td></td>
</tr>
<tr>
<td>= Requested resource</td>
<td></td>
</tr>
<tr>
<td>= Signed Identity</td>
<td></td>
</tr>
</tbody>
</table>

**Consumers**

- **TPaaS**
  - IP
  - AS

**Notes**

- Consumer
  - owner id

**Diagram**

- Owner Grant
- Refresh Token
- Access Token
- Requested resource
- Signed Identity
use case: authenticated user - setup

- user delegates right to access (part of) his or her data to an application to be used by any identified consumer
- the consumers are any THP users.
- identity of both owner and consumer required by client.
- rights given by the owner to the client, not to the consumers.
- OpenIdConnect needed.

Who?

owner credentials

Resource owner

Client

THP

IP

RS

AS = Authorization Server
IP = Identity Provider
RS = Resource Server

= Owner Grant
= Refresh Token
= Access Token
= Requested resource
= Signed Identity
use case: authenticated user - “logon”

- user delegates right to access (part of) his or her data to an application to be used by any identified consumer
- the consumers are any THP users.
- identity of both owner and consumer required by client.
- rights given by the owner to the client, not to the consumers.
- OpenIdConnect needed.

Consumer credentials

Client

Who?

Consumer

THP

IP

RS

AS = Authorization Server
IP = Identity Provider
RS = Resource Server

= Owner Grant
= Refresh Token
= Access Token
= Requested resource
= Signed Identity
use case: authenticated user - resource access

- Refresh Token to generate Access Token with different consumer
- Lifetime for refresh token established by owner.
- Consumer must be online.

AS = Authorization Server
IP = Identity Provider
RS = Resource Server

= Owner Grant
= Refresh Token
= Access Token
= Requested resource
= Signed Identity
Summary

- extending OAuth2.0
- using OpenIDConnect
- logging all resource requests for auditing purposes
- REST full interface
demo description

- demo shows use cases 1 and 2
- 4 VMs
  - one running all databases
  - one running logservice
  - one running OAuth2Share
  - one running the applications
“The TClouds project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-257243.”

If you need further information, please contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55     Fax: +43 4242 233 55 77
E-Mail: coordination@tclouds-project.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.