A secure infrastructure for mobile blended learning applications

M. Politze, S. Schaffert, B. Decker
IT Center RWTH Aachen University
Overview

• Motivation & Goals
• Current State
• Case Studies
• Lessons Learned
• Future Work
Goals

Support the core processes: Teaching, Learning and Research

• Connect legacy systems with a single, consistent API

• Develop an SOA that fits to the processes at the university
  – Start with E-Learning
  – Generalize and try to apply to other fields:
    ▪ Campus Management, Identity Management
    ▪ Research Data Management / E-Science

• Security by design
  – Confidentiality
  – Integrity
  – Availability

• Protect personal and confidential data
Goals

Be able to adopt to the students and institutes processes

• Processes of students and institutes change faster than central IT

• Use custom code to trigger workflows

• Run analytics and reports on their own data

• Offer advanced E-Learning scenarios to their students
Current State

Where we are coming from

• Project started in September 2013

• Initial goal:
  “Develop a mobile app to support students’ daily routines”

• Initially funded by the student council

• Set priorities according to students’ feedback
System Landscape in June 2016
Technical Details
OAuth at RWTH Aachen University

- Secure, device based Authorizations
  - (De)Authorizations via Webinterface
  - No credentials are passed to apps

- OAuth2 as a service
  - Integrates Shibboleth as authentication
  - Possibility to provide a federative service (DFN, …)

- Established at RWTH
  - RWTHApp has ~20,000 Users
  - Procedure scales across different applications
On Top of OAuth2

Expansion to additional scenarios with…

• Anonymous access
  – Identification of the application and not the users themselves

• Authorization of Apps and Web Applications
  – Different levels of trust for applications with different scopes
  – Transparency for the user and the owner of the service

• Claim-Based Authorization
  – For „Full Trust“ B2B Applications
  – Self-Authorization for Webservices
  – Multiple Authentication Mechanisms
Cache Implementation

Cache Invalidation

- Reduction of expiration time not possible
- Automatic invalidation on change

Reference Data

- Keep data in cache and refresh in regular intervals
- Update more often in background

Proactive Caching

- Caching of possible future requests based on current actions
- Data set: Sequence of actions for a user session (30 minutes)
- Sequential rule mining:
  "If action x is performed, in ..% of all cases, action y will be performed at a later point in time"
App Landscape

- Since 2014 as a service
- 35 active apps
  - 10 by Institutes
  - 25 by Students
- 50,000 authorized app instances
- 20,000 active users

Number of authorizations of different apps using the university APIs
Content Driven Apps: Interactive Tour Guide

- collect multimedia resources
- compose articles
- view in (mobile) app
Directfeedback: An audience response system using Smartphones

- Get Feedback from students in large-scale lectures (1000+ students)
- Acoustics in big lecture halls is usually too bad to understand questions
- Students do not dare to ask
- Lecture is streamed to multiple room so students have no physical contact with the teacher
- Low threshold: easy to use for students and teachers
**Dirctfeedback Core Features**

**Interactive Polls**
Classic „Audience Response System“ to evaluate and discuss multiple choice questions during the lecture.

**Filter and categorize**
For better evaluation and handling so the focus can stay on the topic of the lecture.

**Exchange Textmessages between teachers and students**
Send messages from smartphone to the teachers notebook and respond to students questions.

**Handwritten Formulas and Drawings**
A picture is worth a thousand words: Exchange images with the teacher.
Device Based Authorization for Eduroam

Reduce the effects of Evil Twin Attacks [1]

- Allow single devices to be granted or denied access to Eduroam
  - e.g. when after selling or losing a device
  - regularly in fixed intervals

- Automatic creation of credentials for Eduroam
  - To create credentials a internet connection is needed
  - An app can configure the WLAN connection

- Passwords are randomly generated
  - Cracking the Eduroam password does not harm other services
  - New passwords can be generated using the app

http://syssec.rub.de/media/infsec/veroeffentlichungen/2015/05/07/eduroam_WiSec2015.pdf
Lessons Learned

- OAuth2 subsystem offers flexibility to securely expand system landscape
- Redundancy is key to achieve high availability
- Failures in attached systems produce failures in our infrastructure
  - Unit tests often do not only test our code but also if the legacy systems still work as expected
Lessons Learned

- **Cache Evaluation**
  - Different configuration for every server
  - Comparison of individual server performance

- **For some applications more general services are needed**
  - Caching / In-Memory-DB
  - Queriable Storage
  - Mass / Object Storage

- **Speedup in developing new applications on top of the services**
  - Better understandable
  - Better maintainable

<table>
<thead>
<tr>
<th></th>
<th>LRU</th>
<th>Proactive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hit Rate</strong></td>
<td>48.32%</td>
<td>70.89%</td>
</tr>
<tr>
<td><strong>Avg. Duration</strong></td>
<td>1557.47 ms</td>
<td>1004.24 ms</td>
</tr>
<tr>
<td><strong>Requests &lt;700 ms</strong></td>
<td>81.03%</td>
<td>87.63%</td>
</tr>
<tr>
<td><strong>Dirty Reads</strong></td>
<td>2.27%</td>
<td>2.29%</td>
</tr>
</tbody>
</table>
Future Work

• Apply infrastructure to other applications
  – E-Science and Research Data Management
  – Campus Management

• Case studies need further improvements
  – Eduroam configurator app
  – Publish a reference design for content driven apps

• Create formal definition and apply maturity rating
  – Measure if the infrastructure fulfills current requirements
  – Support continual improvement process

• Supply more detailed reporting…
  – for services
  – for apps
  – for users

• Further extend scope of the API
Thank you for your attention

Vielen Dank für Ihre Aufmerksamkeit