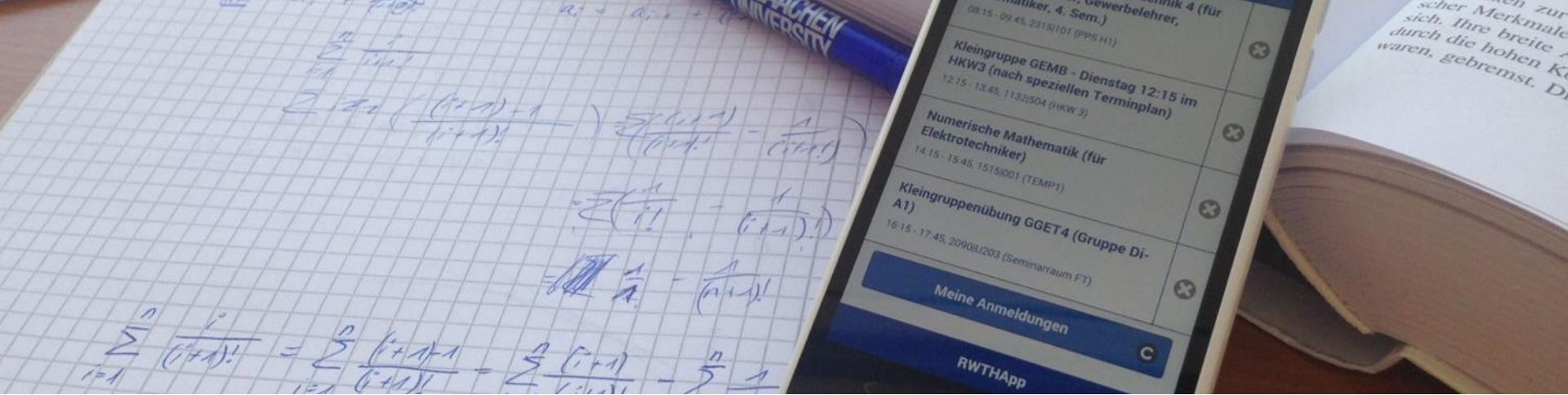




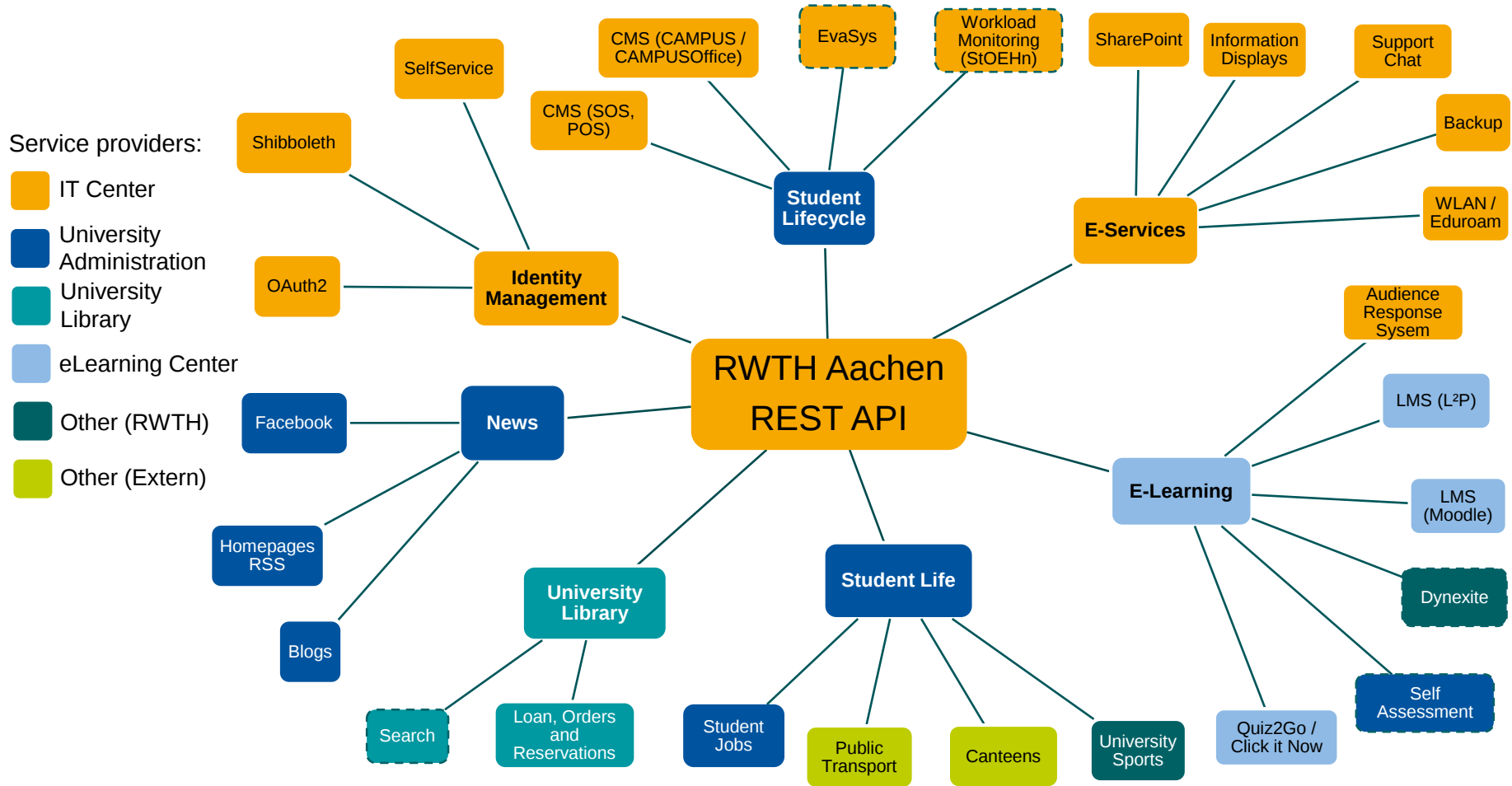
Extending the OAuth2 Workflow to Audit Data Usage for Users and Service Providers in a Cooperative Scenario

Marius Politze, Bernd Decker
IT Center RWTH Aachen University

Support the core processes: Teaching, Learning and Research

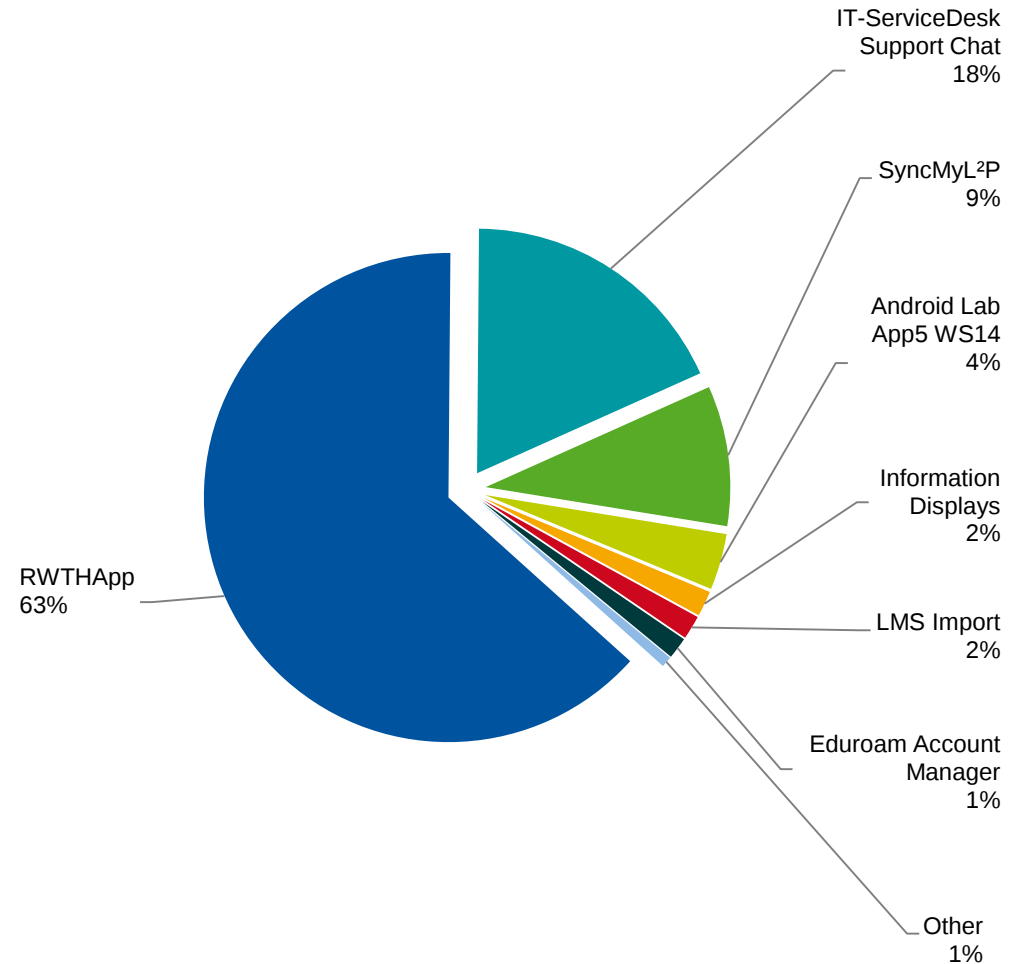
- Connect legacy systems with a single, consistent API
- Develop an SOA that fits to the processes at the university
 - Start with eLearning
 - Generalize and try to apply to other fields:
 - Campus Management, Identity Management
 - Research Data Management / eScience
- Security by design
 - Confidentiality
 - Integrity
 - Availability
- Protect personal and confidential data

System Landscape by Service Provider



App Landscape

- Since 2014 as a service
- 35 active apps
 - 10 by Institutes
 - 25 by Students
- 50.000 authorized app instances
- 22.000 active users



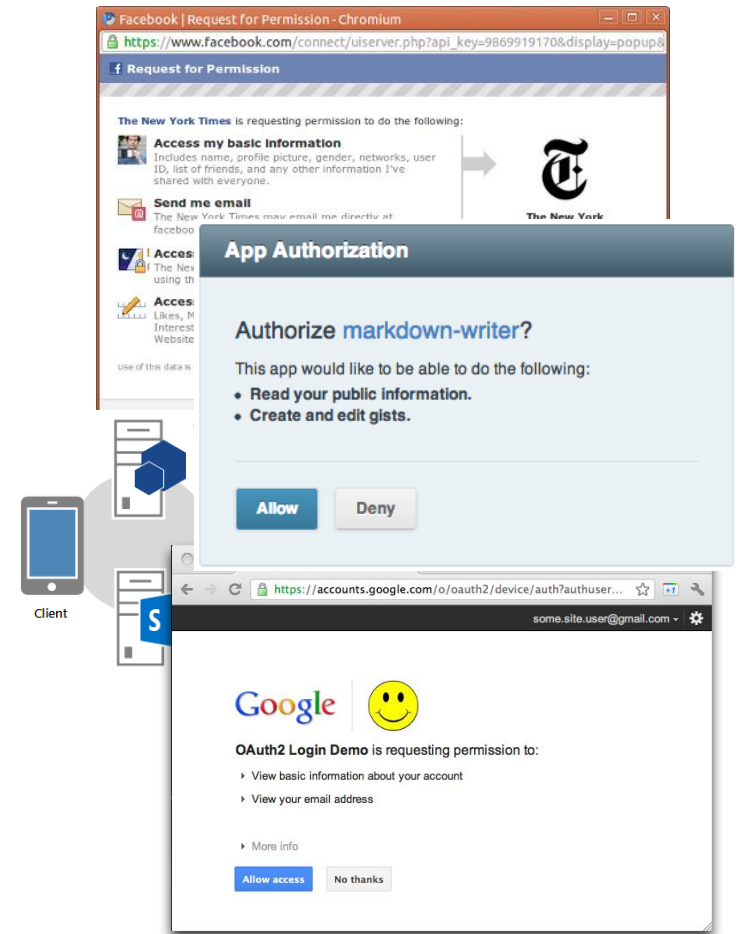
Authorized App-Instances in November 2016

Goals

- Provide an authorization system for
 - Distributed systems
 - Processes crossing system boundaries
- Allow users to check how their data is used
 - Real time and retrospective monitoring
 - Which systems are using data on my behalf?
- Provide Data usage and Analytics for
 - User-Centric Security
 - Distributed service providers
 - and (external) app developers

OAuth2 at Commercial Service Providers

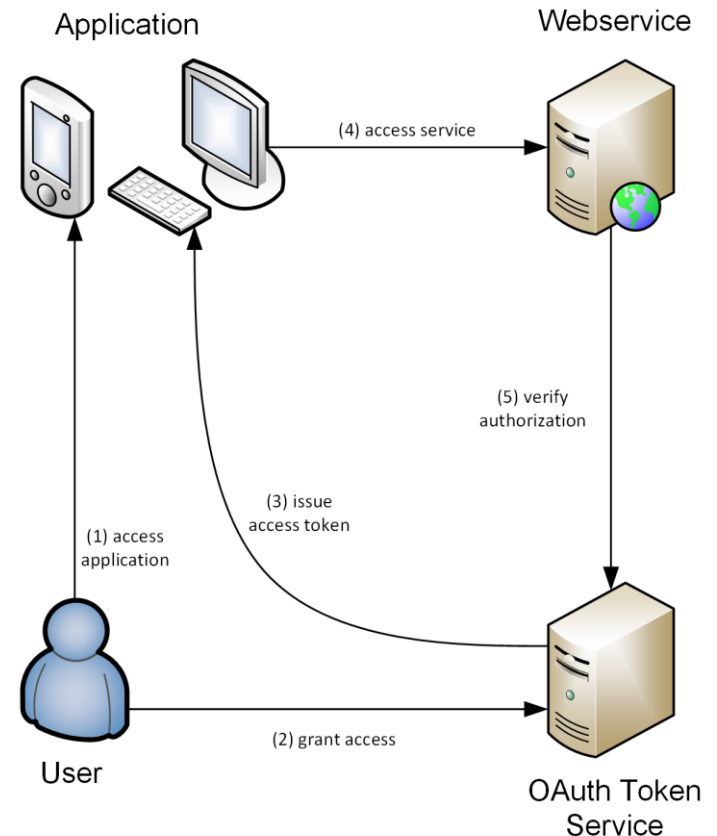
- Tightly coupled with their web services
 - Authorization for *local* scopes
 - Used for applications
- Applications using multiple services still require multiple logins
 - 1:1 mapping of services providers and logins
 - Crossing system boundaries not supported
- Authentication via authorization
 - Use *user info* supplied by a service provider to identify the user
 - Leads to possible security vulnerabilities [1]



[1] R. Yang, W. C. Lau, and T. Liu, Signing into One Billion Mobile App Accounts Effortlessly with OAuth2.0, in Black Hat Europe, 2016.

OAuth2 at RWTH Aachen University

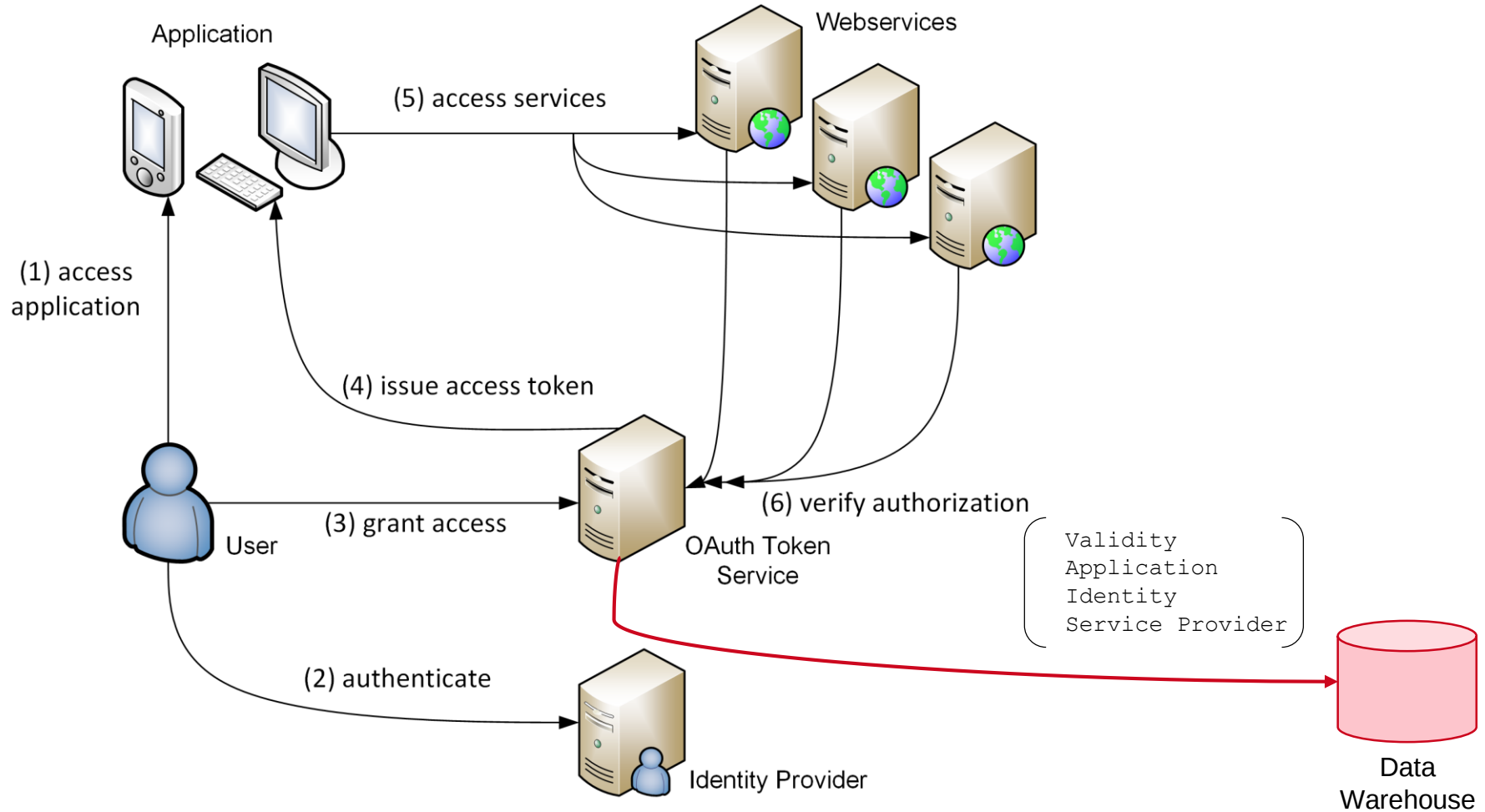
- Secure, device based Authorizations
 - (De)Authorizations via Webinterface
 - No credentials are passed to apps
- OAuth2 as a service
 - Integrates Shibboleth as authentication
 - Possibility to provide a federative service (DFN, ...)
- Established at RWTH
 - RWTHApp has ~20.000 active users
 - Procedure scales across different applications



Endpoints in the Cooperative Workflow

- Authorize
 - Code
 - Token
 - TokenInfo
- Endpoints for web application and device workflow
-
- Context — Endpoint for cooperative workflow
 - Resolve (user) context of an authorization
 - 4-Tuple: (Validity, Application, Identity, Service Provider)

OAuth2 in the Cooperative Workflow

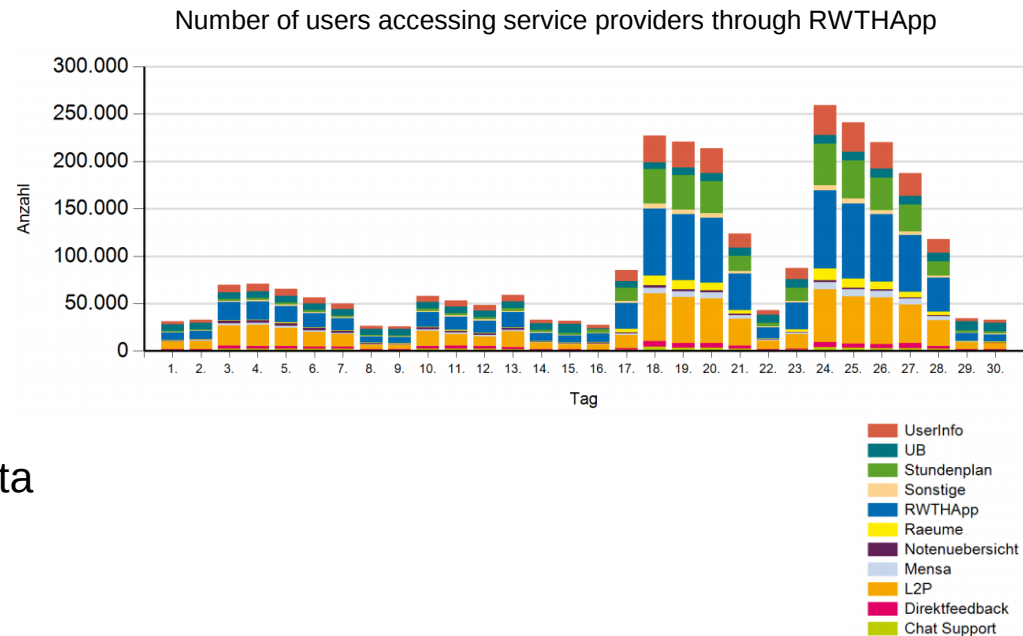


Auditing Data Usage in the Cooperative Workflow

- Use information about resolved contexts for auditing
 - Record existing 4-tuples
 - No information about actual data usage

- Make collected data available to
 - ... service providers
 - ... app developers
 - ... users

- Central collection of audit data
 - OAuth2 system manages the audit data
 - Takes care of proper anonymization
 - ... and data security

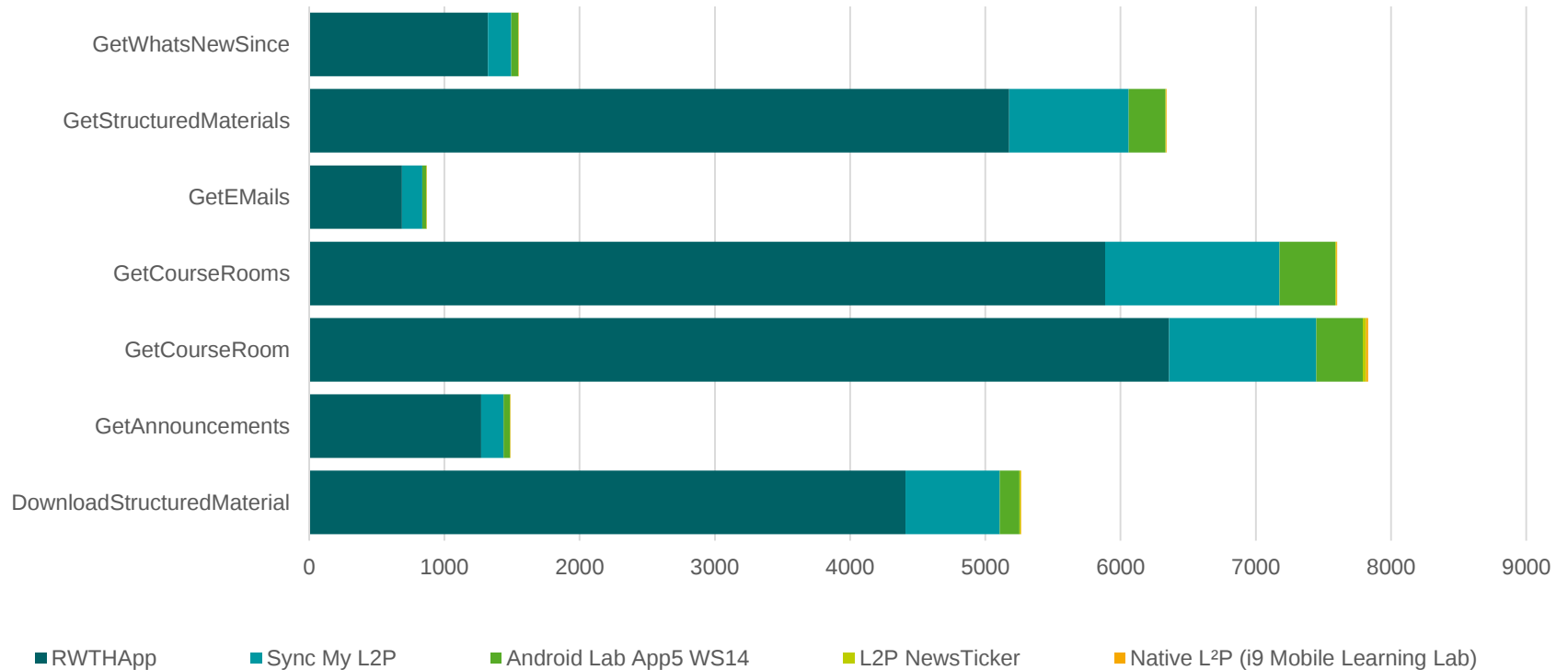


Extending Audit Logging

- Extend logged data by
 - Resource
 - Operation
 - Cost
- Cannot be generated directly from OAuth2 Workflow
 - Services need to provide data
 - Interpretation and granularity up to service providers
- Keep auditing data central
 - Enforce data and privacy regulations
 - Supply information to service providers, app developers and users

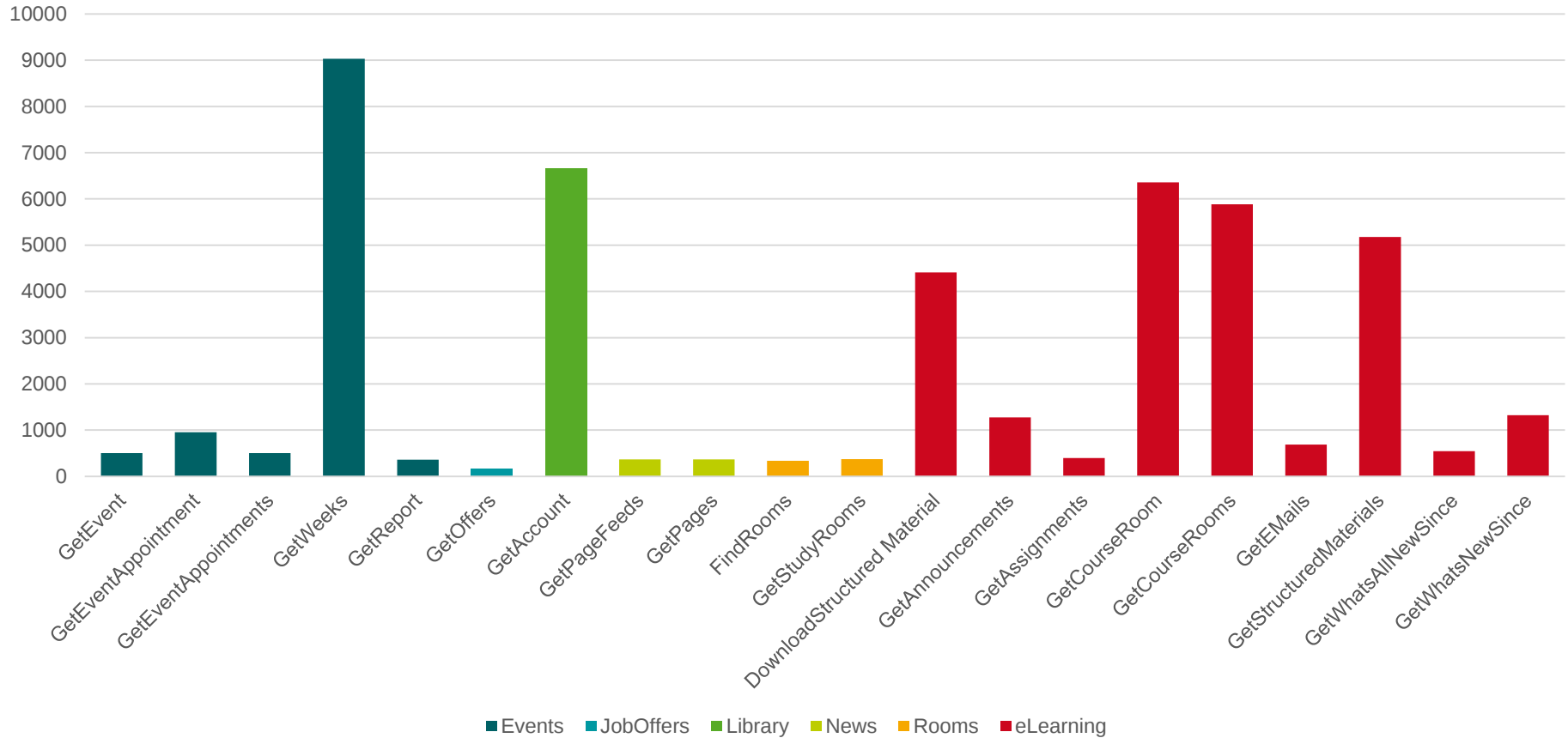
Detailed Statistics for Service Providers

Users per Application and Resource



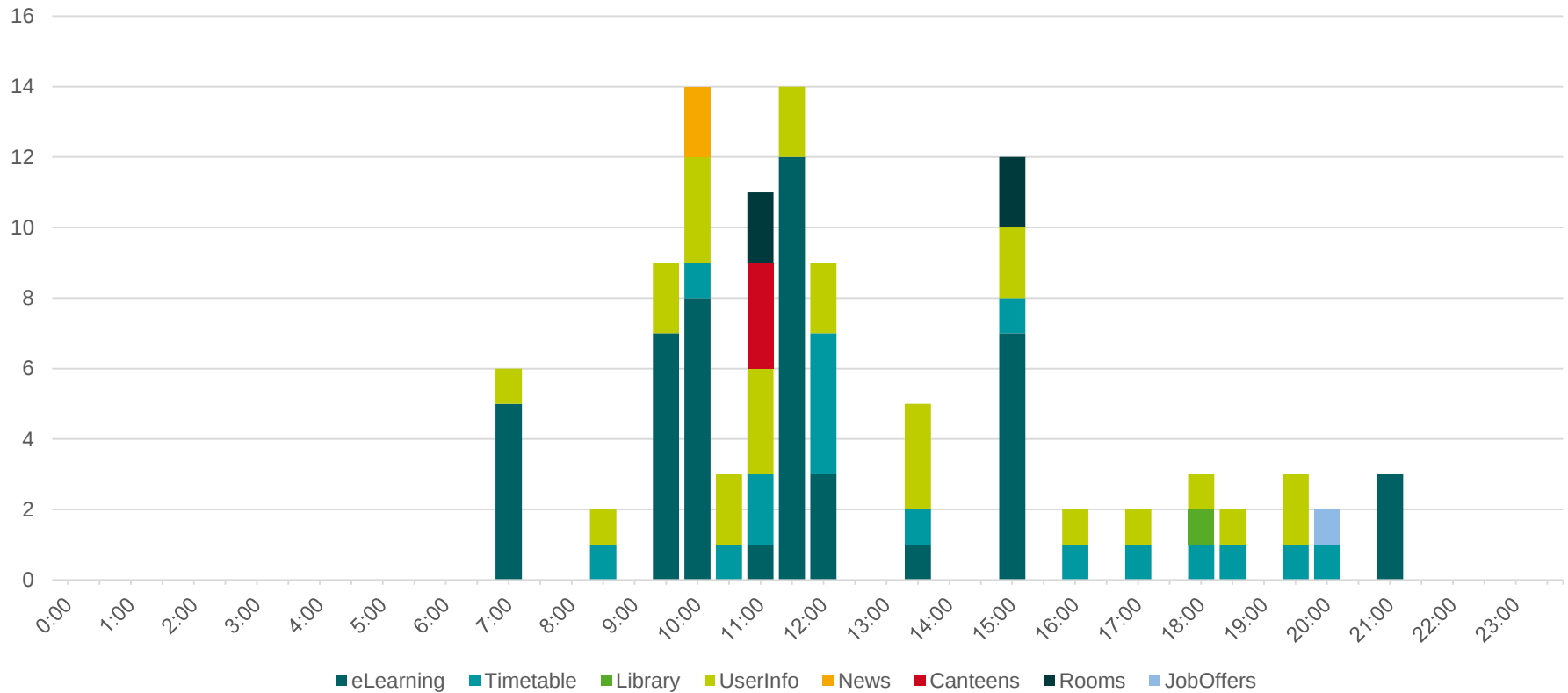
... App Developers

Users per Service Provider and Resource for RWTHApp



... and Users

Timeline of Calls per Service Provider for RWTHApp

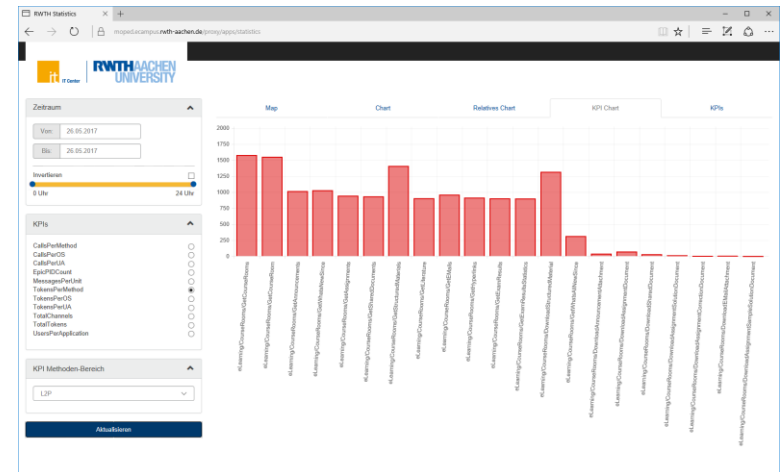


Wrap Up

- OAuth2 cooperative workflow
 - Single OAuth2 instance manages authorizations
 - Reuse authorizations for all service providers
 - Allows processes to cross system boundaries
- Simple centralized auditing
 - User-centric: Security by Transparency
 - Allows enforcement of privacy and data protection laws
- Extended audit logging
 - Detailed reports for service providers, app developers and users
 - Additional information controlled by service providers

What's Next?

- Current Reports limited to monthly PDFs
 - More interactive web based system
 - Prototype currently available to service providers
 - Allow explorative analysis and auditing
- Extend the Reach
 - Mostly used in eLearning services
 - Currently transferring to eScience services
- Further extensions to OAuth2 Workflows
 - Allow third party service providers
 - Federative model
- Automated usage analysis?



Thank you for your attention

Vielen Dank für Ihre Aufmerksamkeit