



Co-funded by the Horizon 2020  
Framework Programme of the European Union  
Grant Agreement Number 825532

# Large-scale EXecution for Industry & Society



  [www.lexis-project.eu](http://www.lexis-project.eu)

## KEYCLOAK IN CROSS DATA-CENTER REPLICATION MODE

[www.lexis-project.eu](http://www.lexis-project.eu)

FREDERIC DONNAT

OUTPOST24





Co-funded by the Horizon 2020  
Framework Programme of the European Union  
Grant Agreement Number 825532

# Large-scale EXecution for Industry & Society



  [www.lexis-project.eu](http://www.lexis-project.eu)

Topic:	HPC and Big Data enabled Large-scale Test-beds and Applications
Topic identifier:	ICT-11-2018-2019
Type of action:	IA Innovation action
Scope:	<p>11a) targeting the development of large-scale HPC-enabled industrial pilot test-beds supporting big data applications and services by combining and/or adapting existing relevant technologies (HPC/BD/cloud) in order to handle and optimize the specific features of processing very large data sets. The industrial pilot test-beds should handle massive amounts of diverse types of big data coming from a multitude of players and sources and clearly demonstrate how they will generate innovation and large value creation. The proposal shall describe the data assets available to the test-beds and, as appropriate, the standards it intends to use to enable interoperability. Pilot test-beds should also aim to provide, via the cloud, simple secure access and secure service provisioning of highly demanding data use cases for companies and especially SMEs.</p>
Project Coordinator:	Jan Martinovič, IT4Innovations, VSB-TU Ostrava
Budget:	14,036,272.5 euro
EC Contribution:	12,218,545.5 euro
Partners:	16
Project duration:	January 2019 – December 2021



Co-funded by the Horizon 2020  
Framework Programme of the European Union  
Grant Agreement Number 825532

# Large-scale EXecution for Industry & Society



[www.lexis-project.eu](http://www.lexis-project.eu)

Topic: HPC and Big Data enabled Large-scale Test-beds and Applications

Topic: **LEXIS project builds an advanced engineering platform at the confluence of HPC, Cloud and Big Data which leverages large-scale geographically-distributed resources from existing HPC infrastructure, employ Big Data analytics solutions and augments them with Cloud services.**

Scope: **Driven by the requirements of the pilots, the LEXIS platform builds on best of breed data management solutions (EUDAT) and advanced distributed orchestration solutions (TOSCA), augmenting them with new efficient hardware capabilities in the form of Data Nodes and federation, usage monitoring and accounting/billing supports to realize an innovative solution.**

Project duration: January 2019 – December 2021

ng big  
ologies  
e data  
g data  
nerate  
e test-  
t-beds  
ing of

# LEXIS CONSORTIUM



# COMPANY DESCRIPTION 1/2



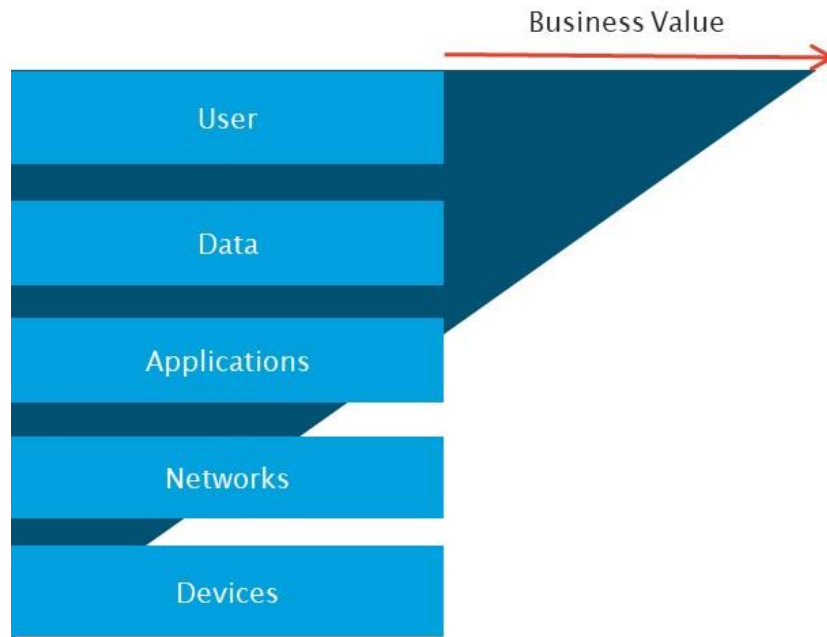
We don't think it's fair that businesses are targets of cybercriminals. As a leading cyber assessment company, we're on a mission to help our customers tighten their cyber exposure before their business can be disrupted. Our ethical hackers and the tools they've created provide a complete view of your security posture with solution-based insights that facilitate and prioritize remediation efforts.

## Objective

Secure the assets that improve business resilience

## Shifts

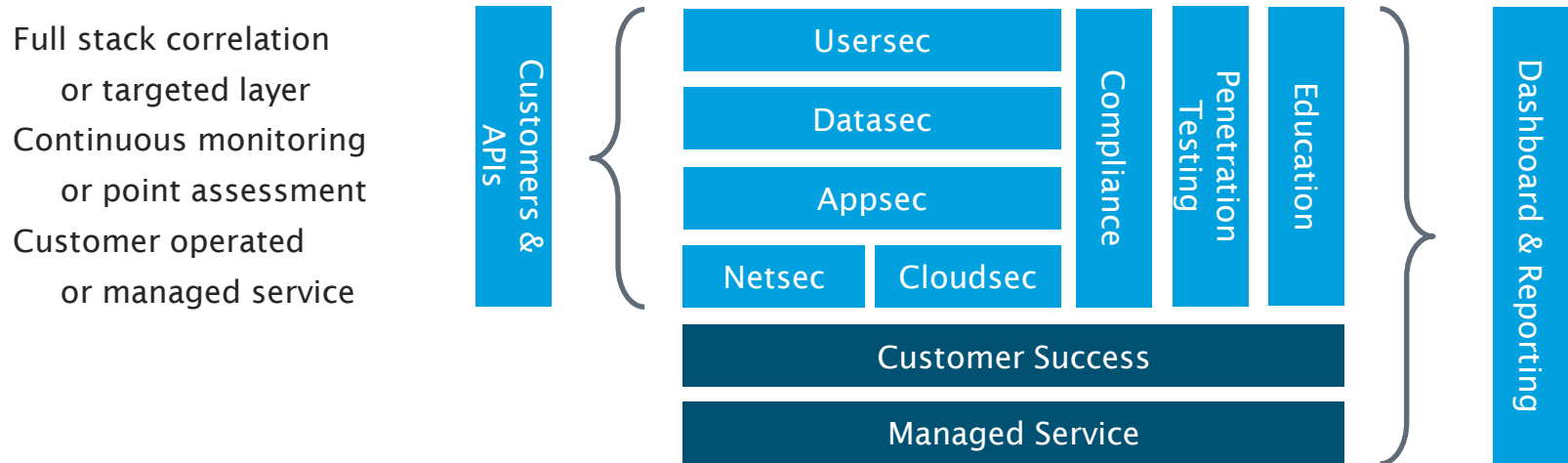
- Move beyond owned infrastructure assessment, assess cloud workloads
- Integrate application security testing, and combine with container assessments
- Evaluate data access rights, user access levels then correlate systems, data, and users





# MAIN COMPETENCES/SKILLS

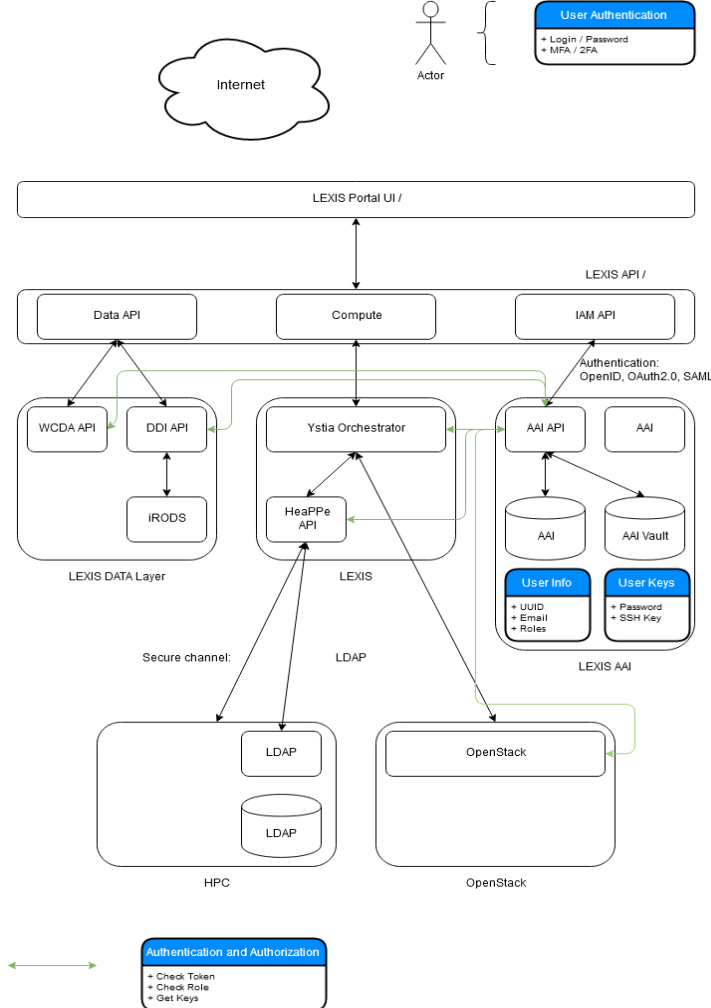
- Full Stack Cyber Exposure Assessment



# LEXIS AAI REQUIREMENTS

LEXIS federated platform security with IAM (Identity and Access management) delegated to LEXIS AAI (Authentication, Authorization & Identity) component

- Single-Sign-On
- OpenIDC, OAuth 2.0 and SAML 2.0
- Role Based Access Control or Attribute Based Access Control
- Identity Brokering
- “Security by Design”
  - “Least Privileges” principle
  - Establish “Secure Defaults”
  - Follow “No Trust” model
  - Keep “Security Simple”



# LEXIS AAI: IAM OPENSOURCE SOLUTION COMPARISON

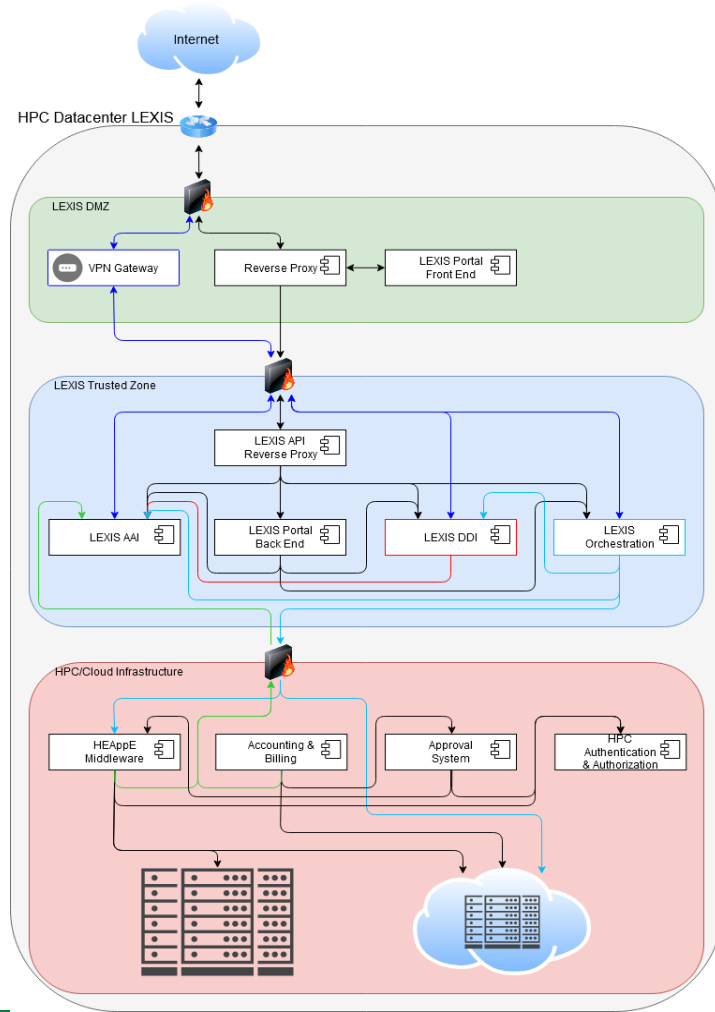
	PROS	CONS
KEYCLOAK	<ul style="list-style-type: none"><li>• Clustered and Distributed deployment</li><li>• Authorization Capabilities (ABAC, RBAC, UBAC, CBAC)</li><li>• Authentication frontend with SAML 2.0</li><li>• Auditing capabilities</li></ul>	<ul style="list-style-type: none"><li>• Lack of LDAP or Kerberos frontend protocols</li></ul>
OPENSTACK KEYSTONE	<ul style="list-style-type: none"><li>• OpenStack ready</li><li>• Auditing capabilities (CADF)</li><li>• Authentication frontend with SAML 2.0</li></ul>	<ul style="list-style-type: none"><li>• Lack of LDAP or Kerberos frontend protocols</li><li>• Limited authorization capabilities RBAC</li></ul>
UNITY	<ul style="list-style-type: none"><li>• Authentication frontend with SAML 2.0</li></ul>	<ul style="list-style-type: none"><li>• Lack of LDAP or Kerberos frontend protocols</li></ul>



# ARCHITECTURE SECURITY

## “Security by Design”

- Minimizing Attack Surface Area
  - Keeping “Security Simple”
  - Separation of duties
- LEXIS DMZ
    - Direct access to internet
    - Reverse Proxy + VPN Gateway
  - LEXIS “Trusted Zone”
    - Functional Services
  - HPC/Cloud Infrastructure
    - HPC Services
    - HEAppE “security middleware” from IT4I



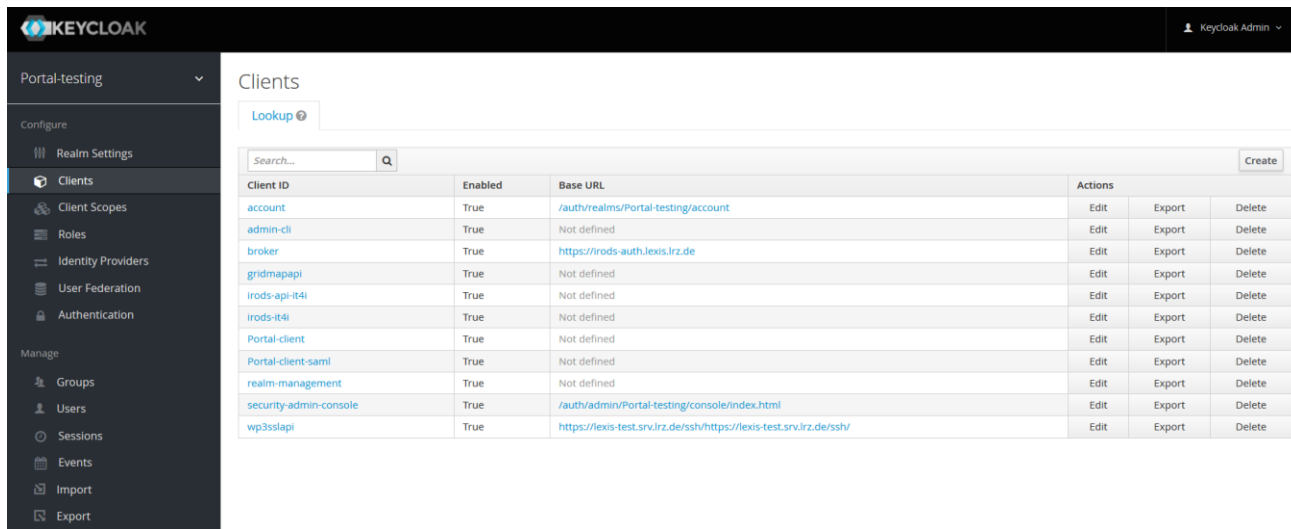
# RBAC MATRIX WITH KEYCLOAK

- Basic concept with 3 permissions
  - **List:** Users, processes or devices are able to list a resource and get its details; e.g., name, creation date, etc. We can refer to such details as the meta-data of the resource;
  - **Read:** Users, processes or devices can access the resource in read-only mode;
  - **Execute:** Users, processes or devices can execute actions on the resource such as creation, update, deletion.

		LEXIS PERMISSIONS																																																																							
		List Users			Read details of a User			Create/Delete/Update a User			List Organizations			Read details of an Organization			Create/Delete/Update an Organization			List Billing & Payment informations			Read details of a Billing & Payment information			Create/Delete/Update a Billing & Payment information			List Licensing informations			Read details of a Licensing information			Create/Delete/Update a Licensing information			List Projects			Read details of a Project			Create/Delete/Update a Project			List Workflows			Read details of a Workflow			Create/Delete/Update/Start/Stop a Workflow			List Computations			Read details of a Computation			Create/Delete/Update/Start/Stop a Computation			List Datasets			Read details of a Dataset			Create/Delete/Update/Import/Export a Dataset		
		iam_list	iam_read	iam_write	org_list	org_read	org_write	bil_list	bil_read	bil_write	lic_list	lic_read	lic_write	prj_list	prj_read	prj_write	wfl_list	wfl_read	wfl_write	cpu_list	cpu_read	cpu_write	dat_list	dat_read	dat_write																																																
LEXIS ROLES		Identity & Access Management			Organization Management			Billing Management			Licensing Management			Project Management			Workflow Management			Computation Management (jobs, tasks or differents)			Data Management (JRDDS DDI and WCDA)																																																		
LEXIS Administrator	lex_admin	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F																																																	
LEXIS Support	lex_sup	P (PO)	P (PO)		P (PO)	P (PO)		P (PO)			P (PO)			P (PO)	P (PO)		P (PO)	P (PO)		P (PP)			P (PP)																																																		
LEXIS Organization Manager	org_mgr	P (PO)			P (PO)	P (PO)	P (PO)	P (PO)			P (PO)			P (PO)																																																											
LEXIS Financial Manager	fin_mgr				P (PO)			P (PO)	P (PO)	P (PO)				P (PO)																																																											
LEXIS License Manager	lic_mgr				P (PO)						P (PO)	P (PO)	P (PO)	P (PO)																																																											
LEXIS Project Manager	prj_mgr	P (PO, PP)			P (PO, PP)									P (PO, PP)	P (PO, PP)	P (PO, PP)	P (PO, PP)			P (PP)			P (PP)																																																		
LEXIS Workflow Manager	wfl_mgr	P (PO, PW)			P (PO, PW)									P (PO, PW)			P (PO, PW)	P (PO, PW)	P (PO, PW)	P (PP)			P (PP)																																																		
LEXIS IAM Manager	iam_mgr	P (PO)	P (PO)	P (PO)	P (PO)									P (PO)																																																											
LEXIS User	end_usr	P (PO, PP, PW)			P (PO, PP, PW)									P (PO, PP, PW)	P (PO, PP, PW)		P (PO, PP, PW)	P (PO, PP, PW)		P (PP)	P (PP)	P (PP)	P (PP)	P (PP)	P (PP)																																																

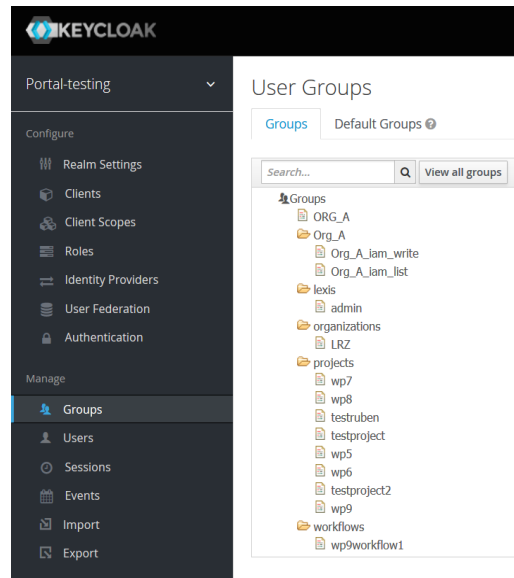
# KEYCLOAK STANDALONE FOR DEVELOPMENT

- Installation & Configuration: v6.0.1
  - Adding Keycloak “Clients”
  - Integration OAuth 2.0 + SAML 2.0
  - Testing Keycloak “Groups”
  - Configuring Keycloak “Mappers”



Keycloak Admin Console - Clients

Client ID	Enabled	Base URL	Actions
account	True	/auth/realms/Portal-testing/account	Edit Export Delete
admin-cli	True	Not defined	Edit Export Delete
broker	True	https://irods-auth.lexis.lrz.de	Edit Export Delete
gridmapapi	True	Not defined	Edit Export Delete
irods-api-it4i	True	Not defined	Edit Export Delete
irods-it4i	True	Not defined	Edit Export Delete
Portal-client	True	Not defined	Edit Export Delete
Portal-client-saml	True	Not defined	Edit Export Delete
realm-management	True	Not defined	Edit Export Delete
security-admin-console	True	/auth/admin/Portal-testing/console/index.html	Edit Export Delete
wp3sslapi	True	https://lexis-test.srv.lrz.de/ssh/https://lexis-test.srv.lrz.de/ssh/	Edit Export Delete



Keycloak Admin Console - User Groups

Groups

- ORG\_A
  - Org\_A
    - Org\_A\_iam\_write
    - Org\_A\_iam\_list
  - lexis
    - admin
  - organizations
    - LRZ
  - projects
    - wp7
    - wp8
    - teststruben
    - testproject
    - wp5
    - testproject2
    - wp9
    - workflows
      - wp9workflow1

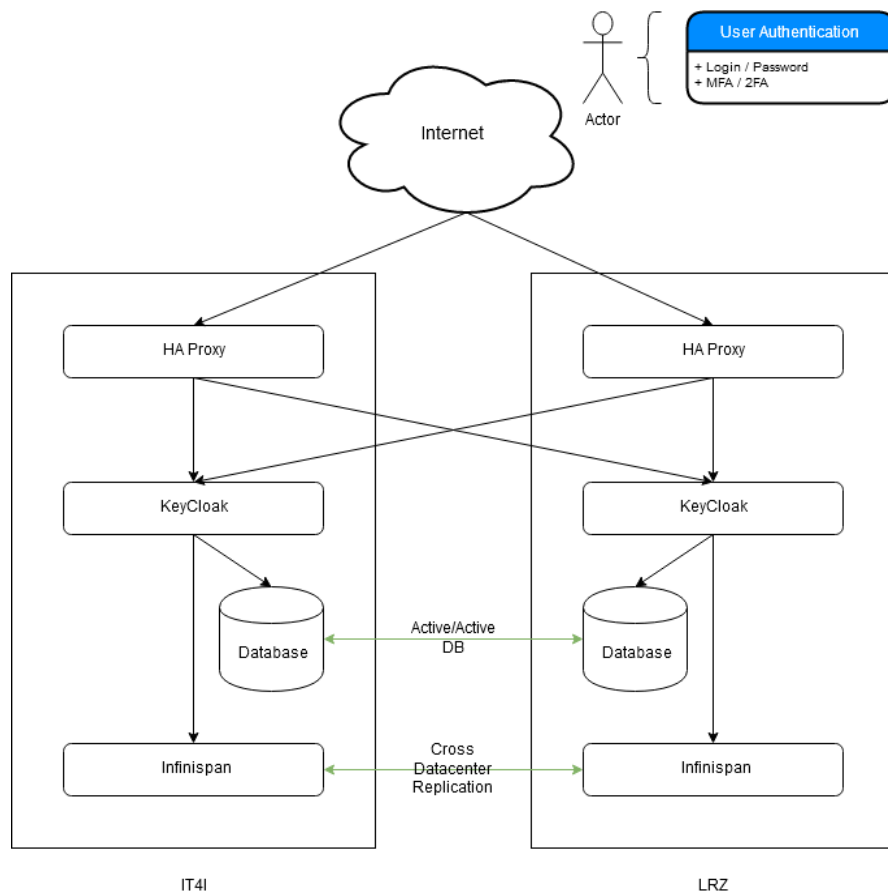
# KEYCLOAK CROSS DATA-CENTER REPLICATION MODE

- Goal

- Updating Keycloak (latest v10.0.2)
- High Availability
- Active/Active MySQL Cluster with Galera

- Current Challenges

- 2 Data-Centers
- Bandwidth over a site-2-site VPN
- Different Linux distribution (Ubuntu & CentOS)



# DOCUMENTATION & LINKS

---

- Keycloak:
  - [https://www.keycloak.org/docs/latest/server\\_installation/#crossdc-mode](https://www.keycloak.org/docs/latest/server_installation/#crossdc-mode)
- Galera Cluster:
  - <https://galeracluster.com/products/>
- Authentication
  - <https://oauth.net/2/>
  - <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>

# CONTACTS

Frederic Donnat  
fdo@outpost24.com

<https://lexis-project.eu>

Large-scale EXecution  
for Industry & Society

LEXIS

## CONSORTIUM

VSb TECHNICAL  
UNIVERSITY  
OF OSTRAVA

IT4INNOVATIONS  
NATIONAL SUPERCOMPUTING  
CENTER

