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

HPC & CLOUD SECURITY

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

LEXIS

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:	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.
Project Coordinator:	Jan Martinovič, IT4Innovations, VSB-TU Ostrava
Budget:	13 997 428,71 euro
EC Contribution:	12 218 545,50 euro
Partners:	17
Project duration:	January 2019 – December 2021

Topic:	HPC and Big Data enabled Large-scale Test-beds and Applications
Topic	
Type c	
Scope:	ng big logies e data g data nerate e test- t-beds ing of
Project	
Budge	
EC Co	
Partne	
Project duration:	January 2019 – December 2021

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.

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.

LEXIS TEAM

VSB TECHNICAL UNIVERSITY OF OSTRAVA | IT4INNOVATIONS NATIONAL SUPERCOMPUTING CENTER

lrz Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities

FONDAZIONE links PASSION FOR INNOVATION

ICHEC Irish Centre for High-end Computing

Atos

ECMWF

Outpost24

cima RESEARCH FOUNDATION

CYCLOPS

numtech INTELLIGENCE ENVIRONNEMENTALE

EIFFAGE TESEO

ITHACA

EURAXENT

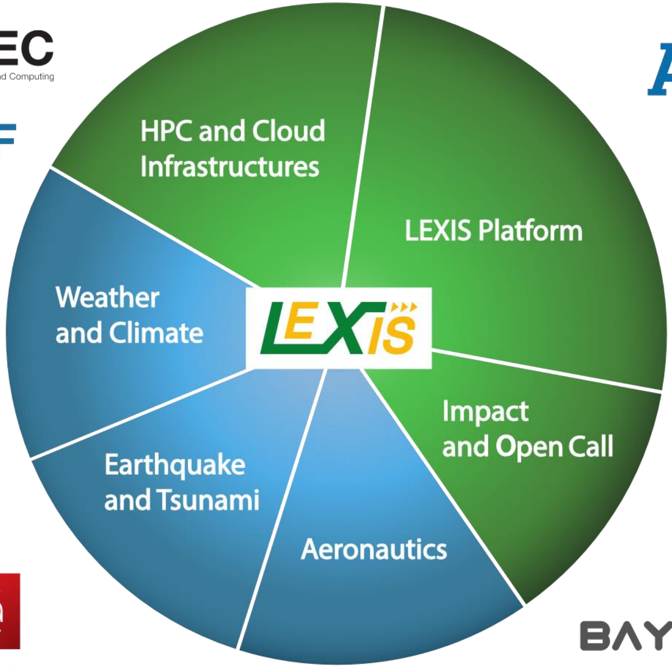
cea

BAYNCORE LABS

ANI

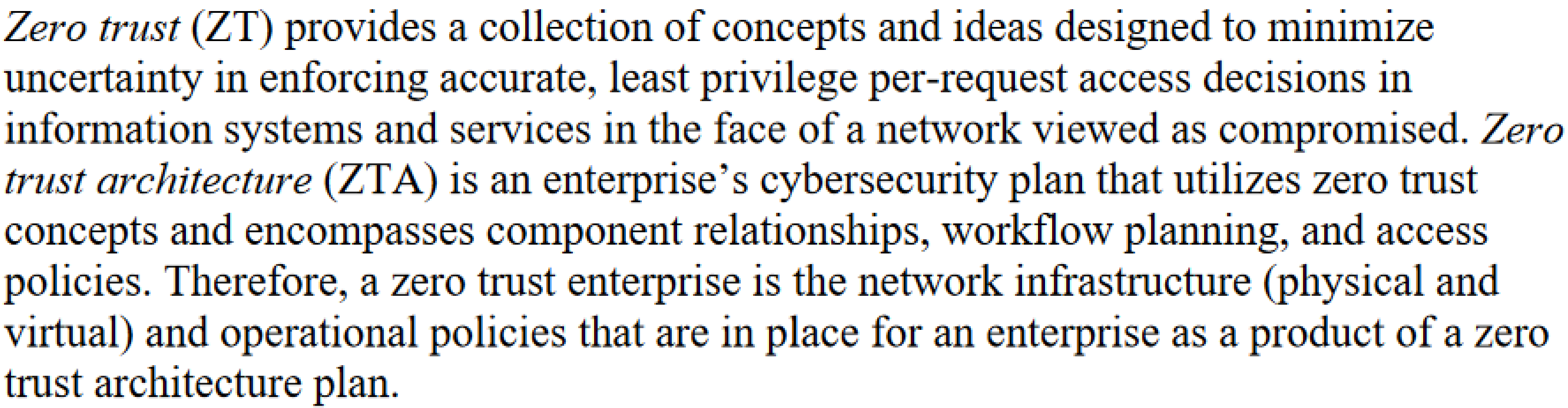
GFZ Helmholtz Centre POTSDAM

Avio Aero A GE Aviation Business



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825532.

ZERO TRUST DEFINITION FROM NIST



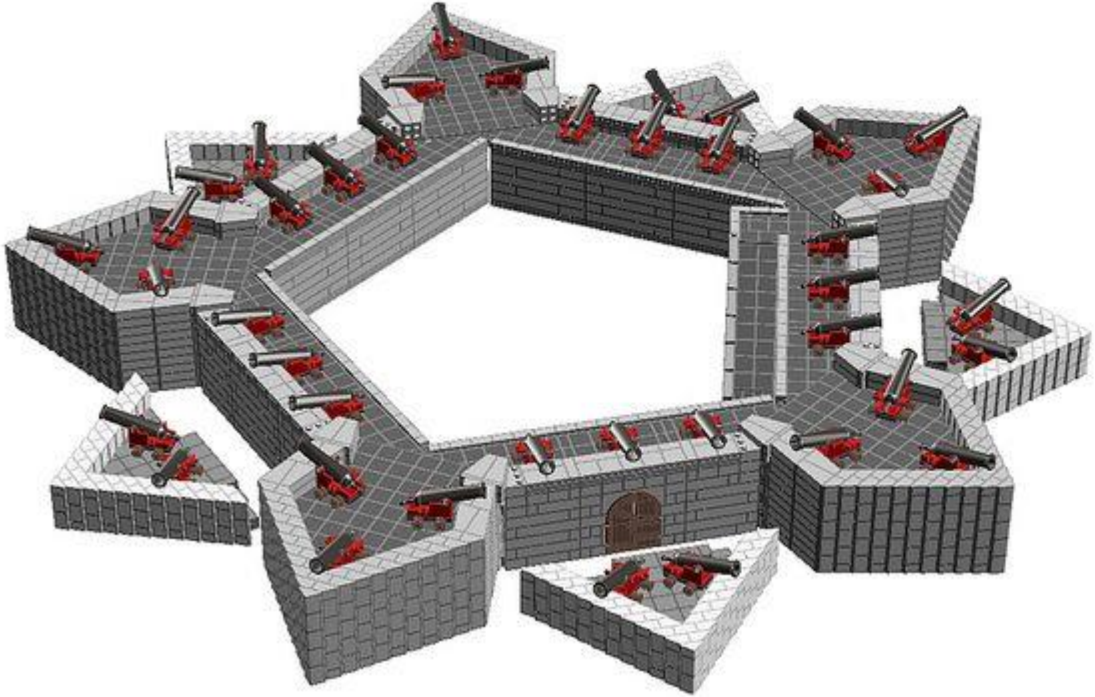
Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. *Zero trust architecture* (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

Zero Trust concepts

- Threats exists both outside and inside the perimeter
- Follow least privileges principles
- No implicit trust granted, continuously authenticate and authorize

ZERO TRUST CONCEPT

Do NOT rely on network perimeter, Assume breach



ZERO TRUST CONCEPT

Never Trust, Continuously Verify

ZERO TRUST CONCEPT

Use least privileges principles, verify Explicitly

ZERO TRUST PRINCIPLES

NIST Tenets:

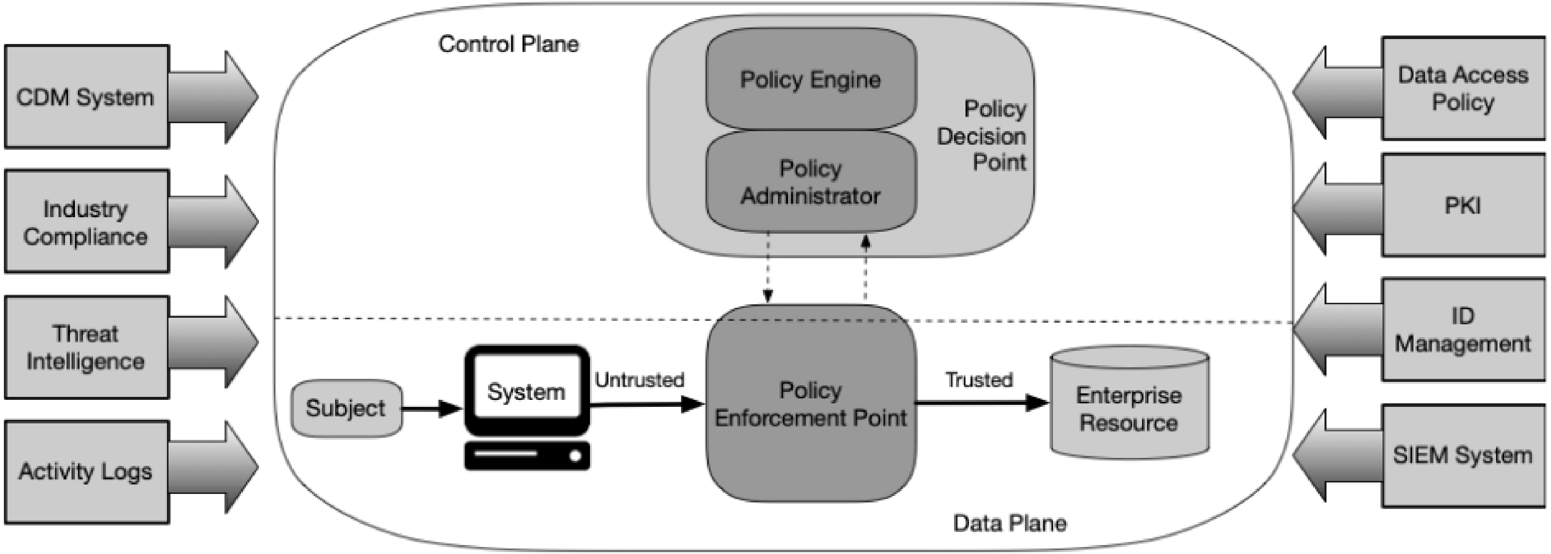
- ✓ All data sources and computing services are considered resources
- ✓ All communication is secured regardless of network location
- ✓ Access to individual enterprise resources is granted on a per-session basis
- ✓ Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes
- ✓ The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- ✓ All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- ✓ The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

ZERO TRUST ARCHITECTURE PRINCIPLES

NIST Tenets:

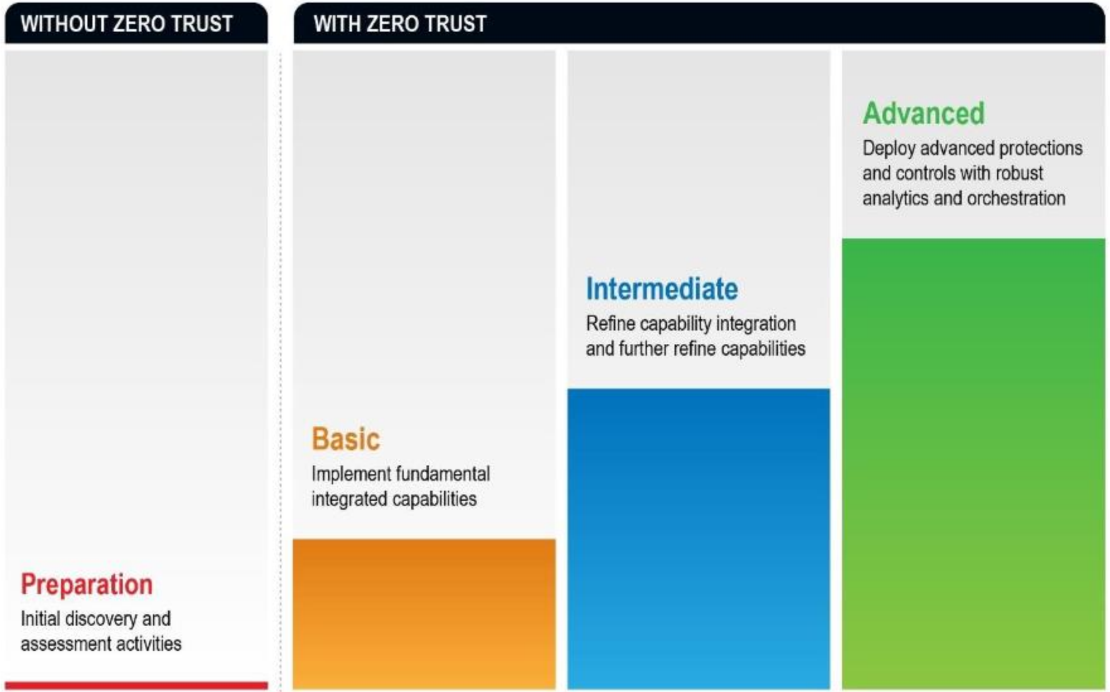
- ✓ The entire enterprise private network is not considered an implicit trust zone
- ✓ Devices on the network may not be owned or configurable by the enterprise
- ✓ No resource is inherently trusted
- ✓ Not all enterprise resources are on enterprise-owned infrastructure
- ✓ Remote enterprise subjects and assets cannot fully trust their local network connection
- ✓ Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture

ZERO TRUST COMPONENTS



ZERO TRUST MATURITY MODEL

- Zero trust takes time and effort: Build a plan and continously improve



WITHOUT ZERO TRUST

WITH ZERO TRUST

Preparation
Initial discovery and assessment activities

Basic
Implement fundamental integrated capabilities

Intermediate
Refine capability integration and further refine capabilities

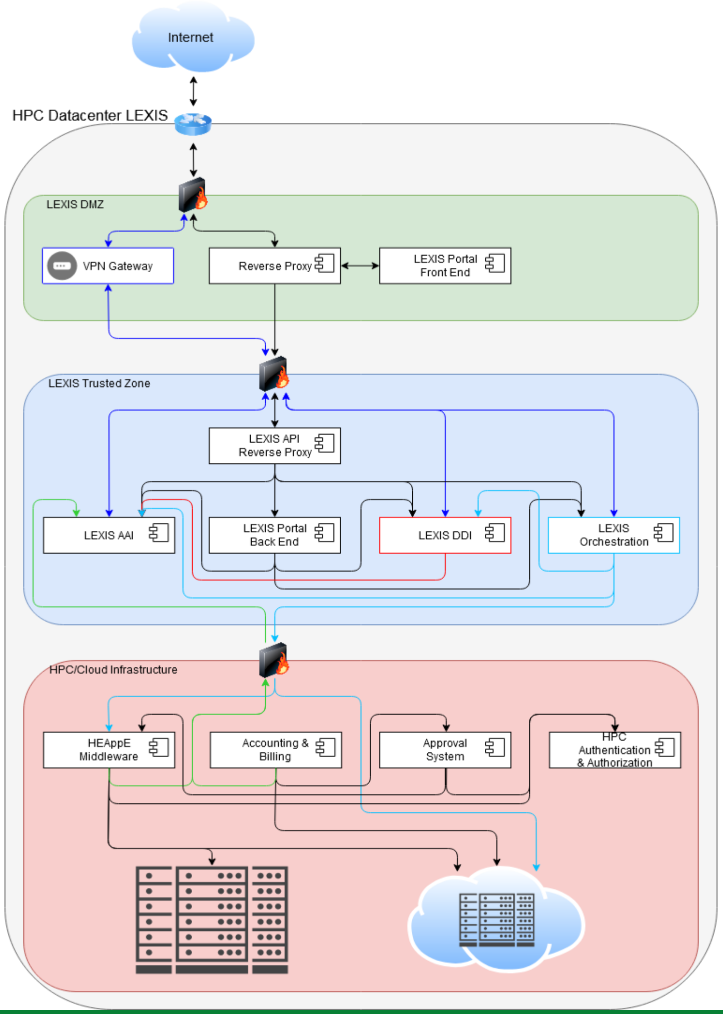
Advanced
Deploy advanced protections and controls with robust analytics and orchestration

LEXIS ARCHITECTURE

“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

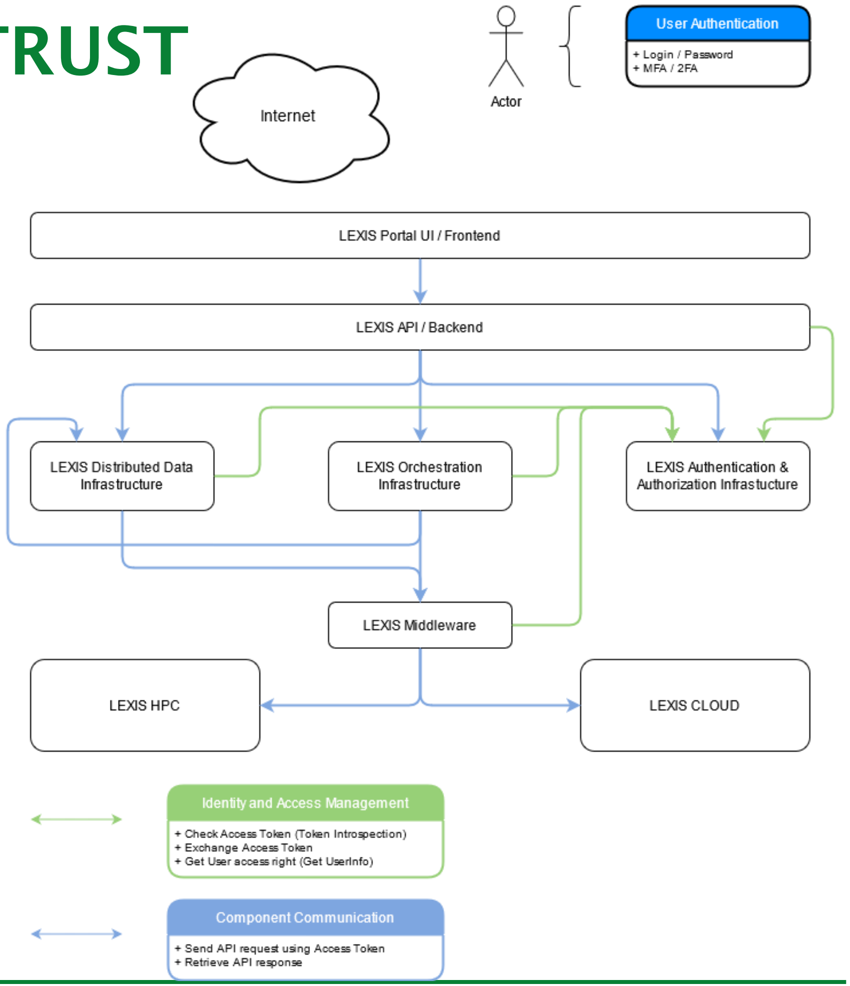


LEXIS APPROACH TO ZERO TRUST

"Zero Trust Architecture"

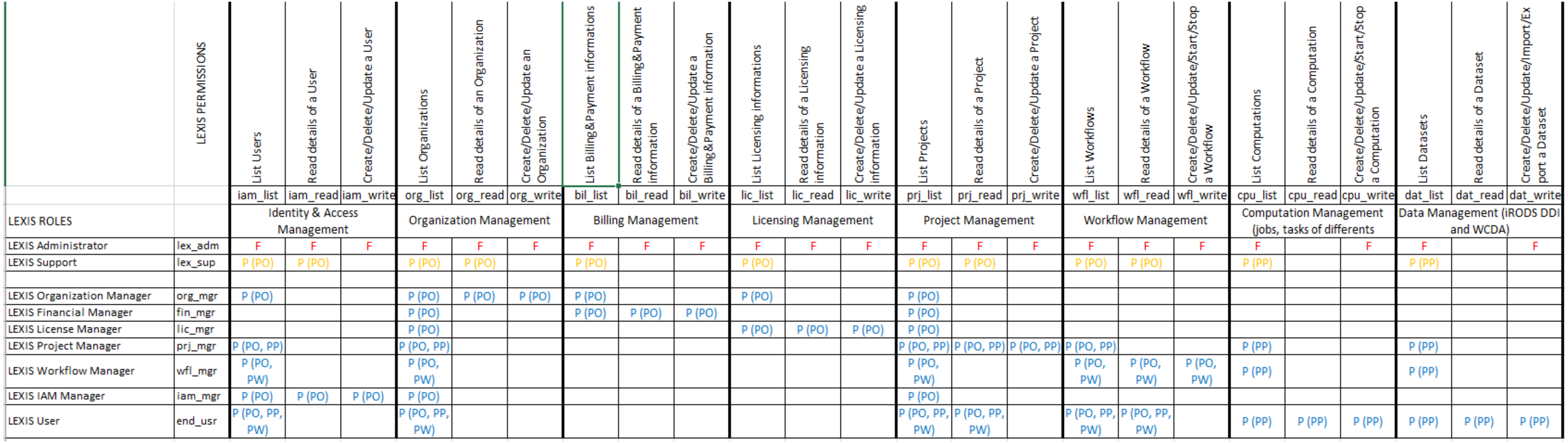
- ◦ Do NOT rely on perimeter-based network security
- ◦ Minimize access to resources
- ◦ Enforce Authentication and Authorization

- Do "NOT TRUST" anything inside the perimeter
- Use secure communication channel
- Always check Identity and Access


Internet
Actor
User Authentication
+ Login / Password
+ MFA / 2FA
LEXIS Portal UI / Frontend
LEXIS API / Backend
LEXIS Distributed Data Infrastructure
LEXIS Orchestration Infrastructure
LEXIS Authentication & Authorization Infrastucture
LEXIS Middleware
LEXIS HPC
LEXIS CLOUD
Identity and Access Management
+ Check Access Token (Token Introspection)
+ Exchange Access Token
+ Get User access right (Get UserInfo)
Component Communication
+ Send API request using Access Token
+ Retrieve API response

RBAC MATRIX WITH KEYCLOAK

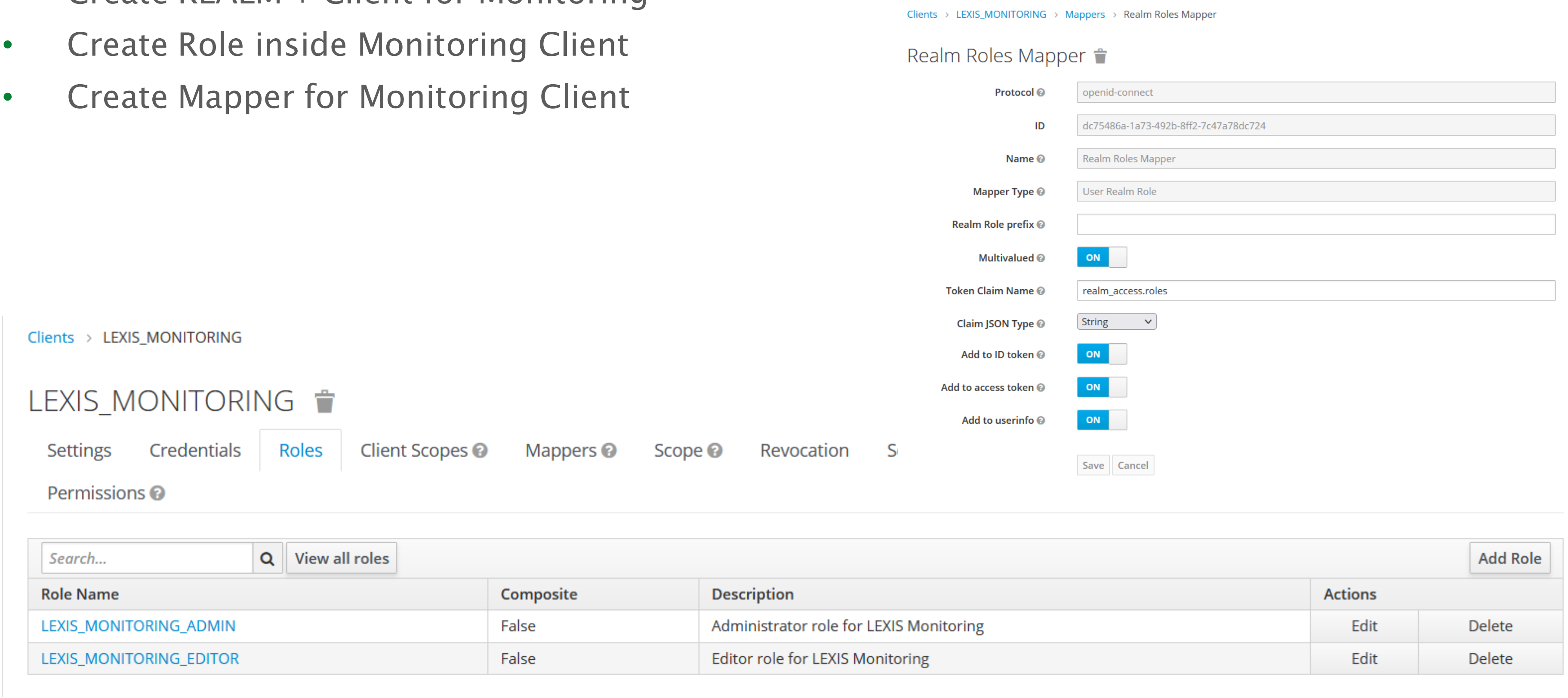
- Basic concept with 3 permissions
  - **List**: Users, processes or devices are able to list a resource and get its details; e.g., name, creation date, etc. We can refer to such details as the meta-data of the resource;
  - **Read**: Users, processes or devices can access the resource in read-only mode;
  - **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 of differents			Data Management (iRODS DDI and WCDA)		
LEXIS Administrator	lex_adm	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 CONFIGURATION PER COMPONENT

- Create REALM + Client for Monitoring
- Create Role inside Monitoring Client
- Create Mapper for Monitoring Client



Clients › LEXIS_MONITORING › Mappers › Realm Roles Mapper

Realm Roles Mapper

Protocol	openid-connect
ID	dc75486a-1a73-492b-8ff2-7c47a78dc724
Name	Realm Roles Mapper
Mapper Type	User Realm Role
Realm Role prefix	
Multivalued	ON
Token Claim Name	realm_access.roles
Claim JSON Type	String
Add to ID token	ON
Add to access token	ON
Add to userinfo	ON

Clients › LEXIS_MONITORING

LEXIS_MONITORING

Role Name	Composite	Description	Actions	
LEXIS_MONITORING_ADMIN	False	Administrator role for LEXIS Monitoring	Edit	Delete
LEXIS_MONITORING_EDITOR	False	Editor role for LEXIS Monitoring	Edit	Delete

DOCUMENTATION & LINKS

- Zero Trust and Zero Trust Architecture
  - NIST: https://csrc.nist.gov/publications/detail/sp/800-207/final
  - NSA: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

- Keycloak
  - https://www.keycloak.org/
  - https://www.keycloak.org/extensions.html

CONTACT

Frédéric Donnat
Cloud technical Security Architect
fdo@outpost24.com

Large-scale EXecution for Industry & Society

LEXIS

CONSORTIUM

VSB TECHNICAL UNIVERSITY OF OSTRAVA | IT4INNOVATIONS NATIONAL SUPERCOMPUTING CENTER

Avio Aero
A GE Aviation Business

Outpost24

EURAXENT

Atos

lrz Leibniz Supercomputing Centre
of the Bavarian Academy of Sciences and Humanities

ICHEC
Irish Centre for High-end Computing

cima RESEARCH FOUNDATION

ITHACA INFORMATION TECHNOLOGY FOR HUMANITARIAN ASSISTANCE, COOPERATION AND ACTION

FROM RESEARCH TO INDUSTRY
cea

EIFFAGE TESEO

GFZ
Helmholtz Centre
Potsdam

numtech
INTELLIGENCE ENVIRONNEMENTALE

ECMWF

FONDAZIONE links
PASSION FOR INNOVATION

AWI

CYCLOPS

BAYNCORE LABS