Land Registers Interconnected

LRI User Authorisation. Findings and Solutions

Dietmar Gombotz

Federal Computing Center / Bundesrechenzentrum
Austria

09.-10.05.2019
LRI MS Connection / lri-ms.eu

This presentation was funded by the European Union's Justice Programme (2014-2020).

RIK
Centre of Registers and Information Systems

Federal Ministry
Republic of Austria
Constitutional Affairs, Reforms, Deregulation and Justice

BRZ

Funded by the Justice Programme of the European Union

THE MISSION

Creating a standardised, extensible, maintainable and lasting authentication & authorisation solution for the
Land Register Interconnected
that serves as Best Practice for future projects

Development-Process

- Analysis of the authentication & authorization solutions in in both member countries (EE, AT)
- Definition of Requirements
- Compilation of Design Document
- Setup of Prototype Implementation

Requirements

- Land-Register Services shall not need to do authentication and authorization

- Allowing access of multiple User Groups
- Decentralise authorisation Management
  - Integrate into the Member States own IAM process
- Standardised for future extension
- Extendable to incorporate future partners
- Best Practice for follow up projects
- Long Term Solution

Comparing Countries

- Austria:
  - heavily federated country with three layers + agencies + self-governing bodies
  - since 2001 developed inter-governmental federation
  - eID just one authentication method within government
- Estonia:
  - centralised administrative structure
  - highly advanced data sharing platform which allows objects to be transferred into digital working environment
  - eID used widely (ID-card, Mobile-ID, Digital Id)
- European Commission
  - mediates between the Member States different needs

Components

Identity Provider

eIDAS

LRI

e-JUSTICE EUROPEAN

Land Register Service Layer

eRIK

Audience

- Citizen & Business Access
  - Anonymous Access
  - Service Account for Repetitive Access
- Administration Access
  - Access for Cross-Border Queries from within the administrative domain
  - Integration with existing infrastructures
  - Includes also Notaries, Legal Professionals, Self Governing bodies,… dependent on country legislation

SOLUTION

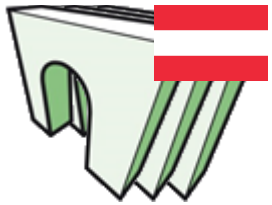
Two Solutions

- Proposed Solution by European Commission
  - Professional Authentication System (PAS)
  - Proprietary self developed Solution
  - Token based system
- Concerns:
  - Maintainability
  - Security Constraints
  - Products & Services
  - No Standardised Description

- LRI-Federation
  - Based on Standard Technology
  - Strategically aligned with eID.AS
  - Easy Extensible
  - Splitting into three Areas
    - Authentication
    - Authorisation
    - Accounting
  - Standardised Description of Metadata and URLs

Components

Identity Provider
(incl. Authorization)



eIDAS

LRI
(User Interface
& Auth Verification)

LRI

e-JUSTICE

Service Layer

eRIK

Functions assigned to Components

Identity Provider

Provides the Identification Information for principals including organisational information and the local assigned rights

The assignment of rights is done inside the IDP

- Identity Information
- Access-Rights for LRI
- Accounting Information

Land Registers Interconnected

The LRI Application provides a unified User Interface to query all members Land Registers

It removes rights which a specific IDP is not allowed to use

- Structure of Access Rights
- Rules for checking assigned rights

Service Layer

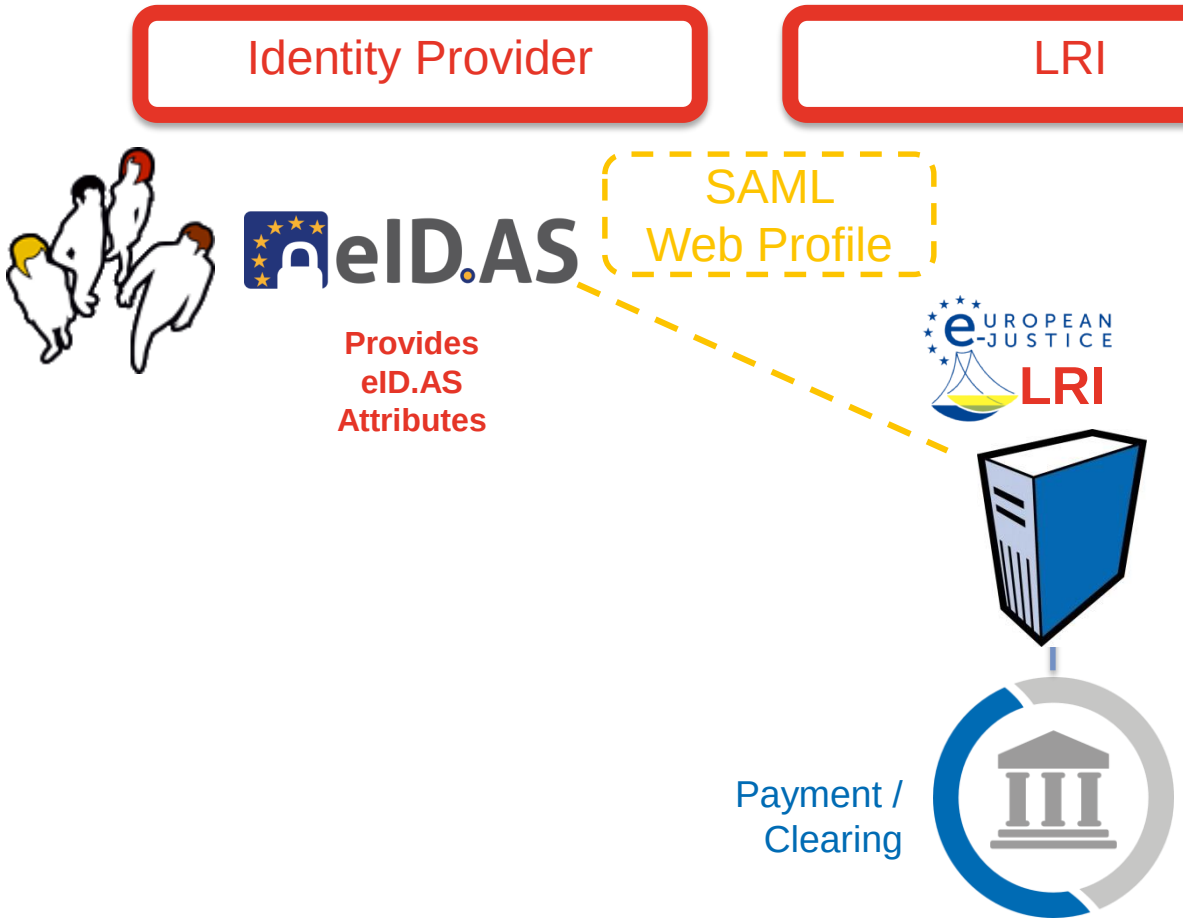
Each land register provides web services which allow LRI the access and provide the data to the consumer

- Definition of Attribute Sets as mentioned in IDP

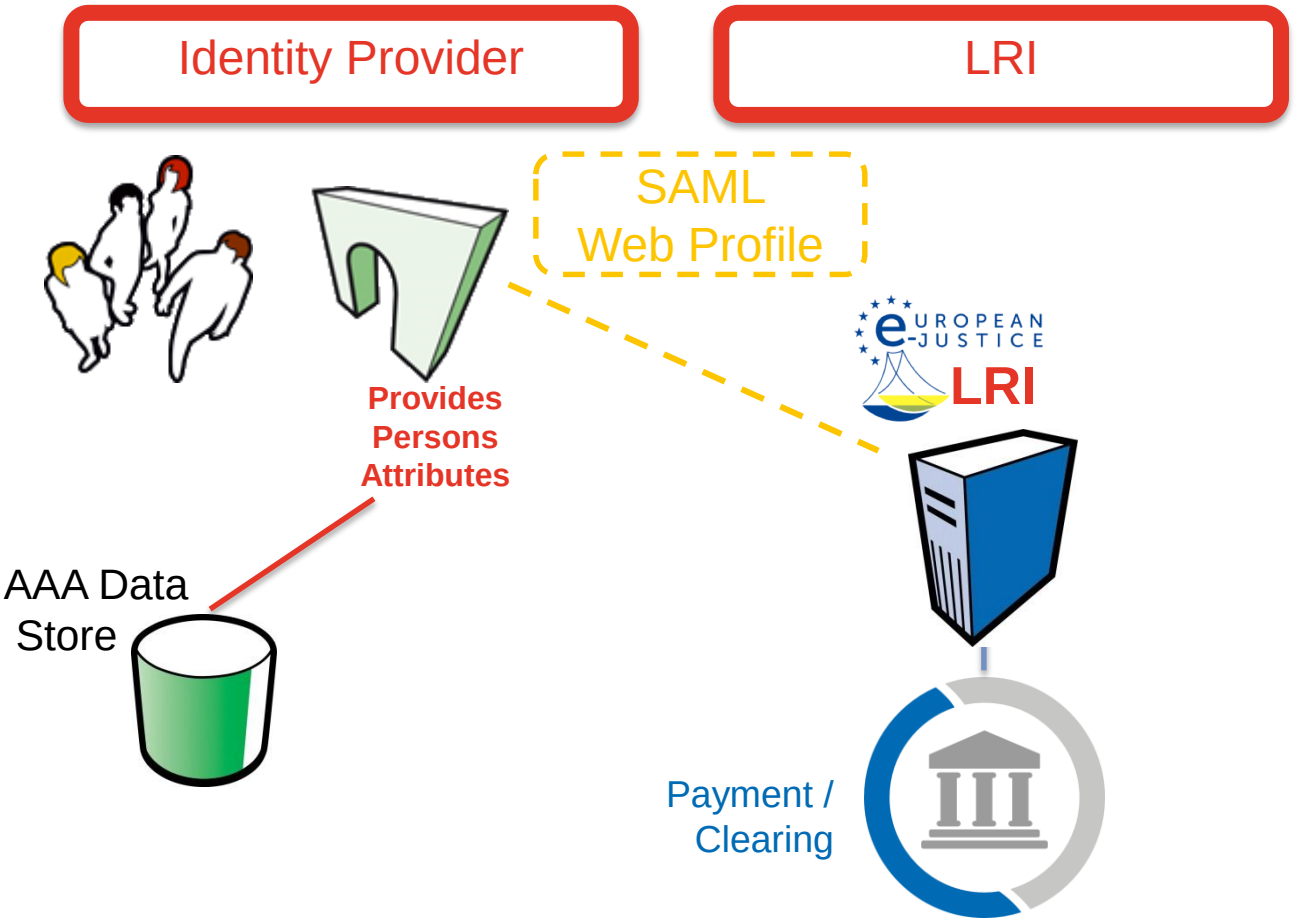
AAA Token - User Information

- Authentication - LRI Profile
  - Extension of eID.AS eID-Profile
  - eID.AS Attributes: First-Name, Surname, Identifier, DoB
- Authorisation
  - Role:
    - ANONYMOUS
    - PRIVATE
    - LEGAL_PROFESSIONAL
    - PUBLIC_OFFICIAL
- Accounting (optional)
  - Participant Organisation
  - Participant Organisational-Unit
  - Invoice Recepient Id
  - Cost-Center for Print-Outs

IDP to LRI System (1/2) – eID.AS



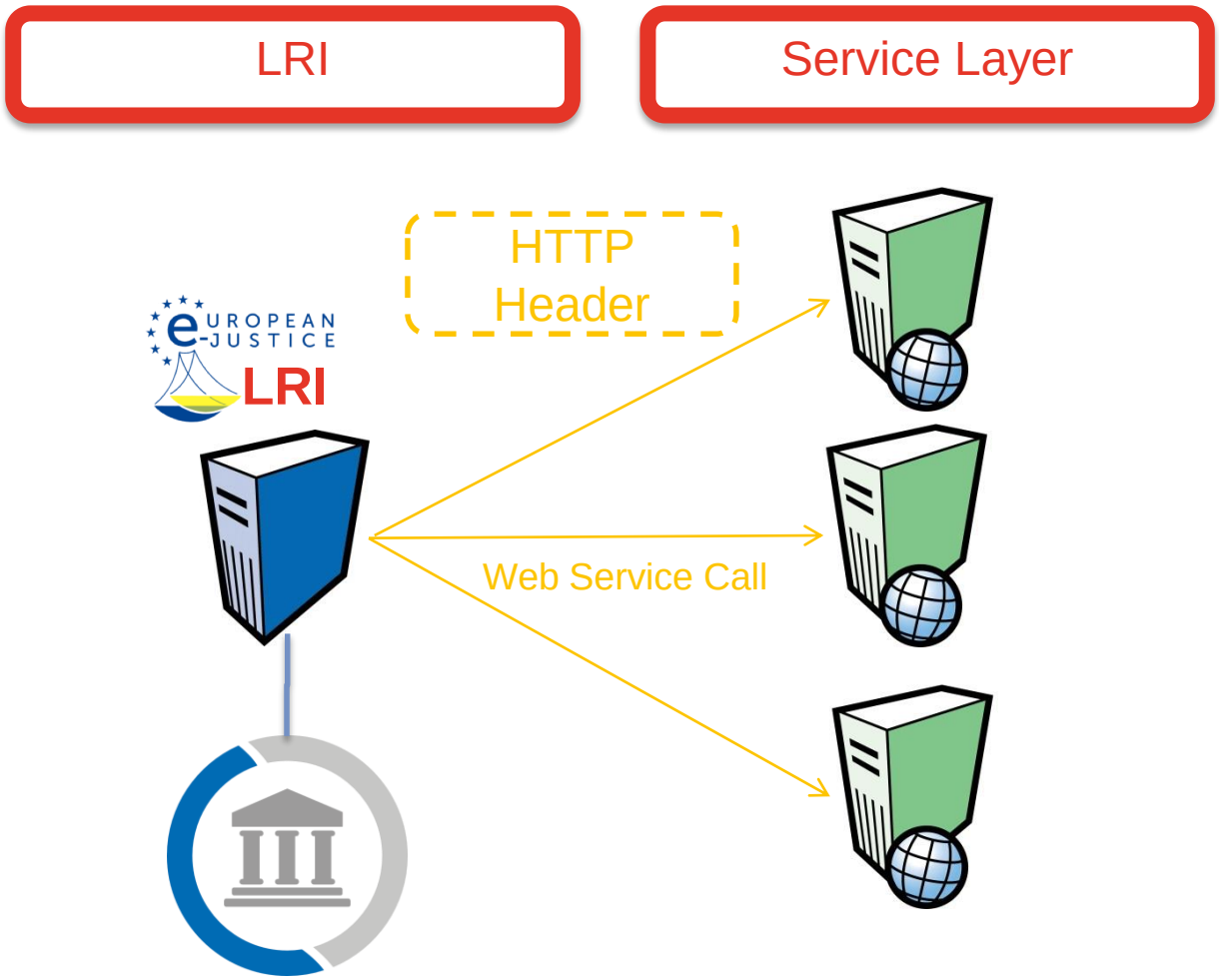
IDP to LRI System (2/2) – national IdP



IdP to LRI System

- SAML - Security Assertion Markup Language
  - XML based Security Language
  - Industry Standard
  - Integrated into all major Ecosystems
- Product Support
  - Product Support from different Vendors
  - Open-Source Solutions
- Extensible by Default
  - Attribute Sets
  - Attribute Providing by third party supported, which allows enriching of user dependent on the performing role
    - XX as Citizen
    - XX as Clerk
    - XX as part of a self governing Body

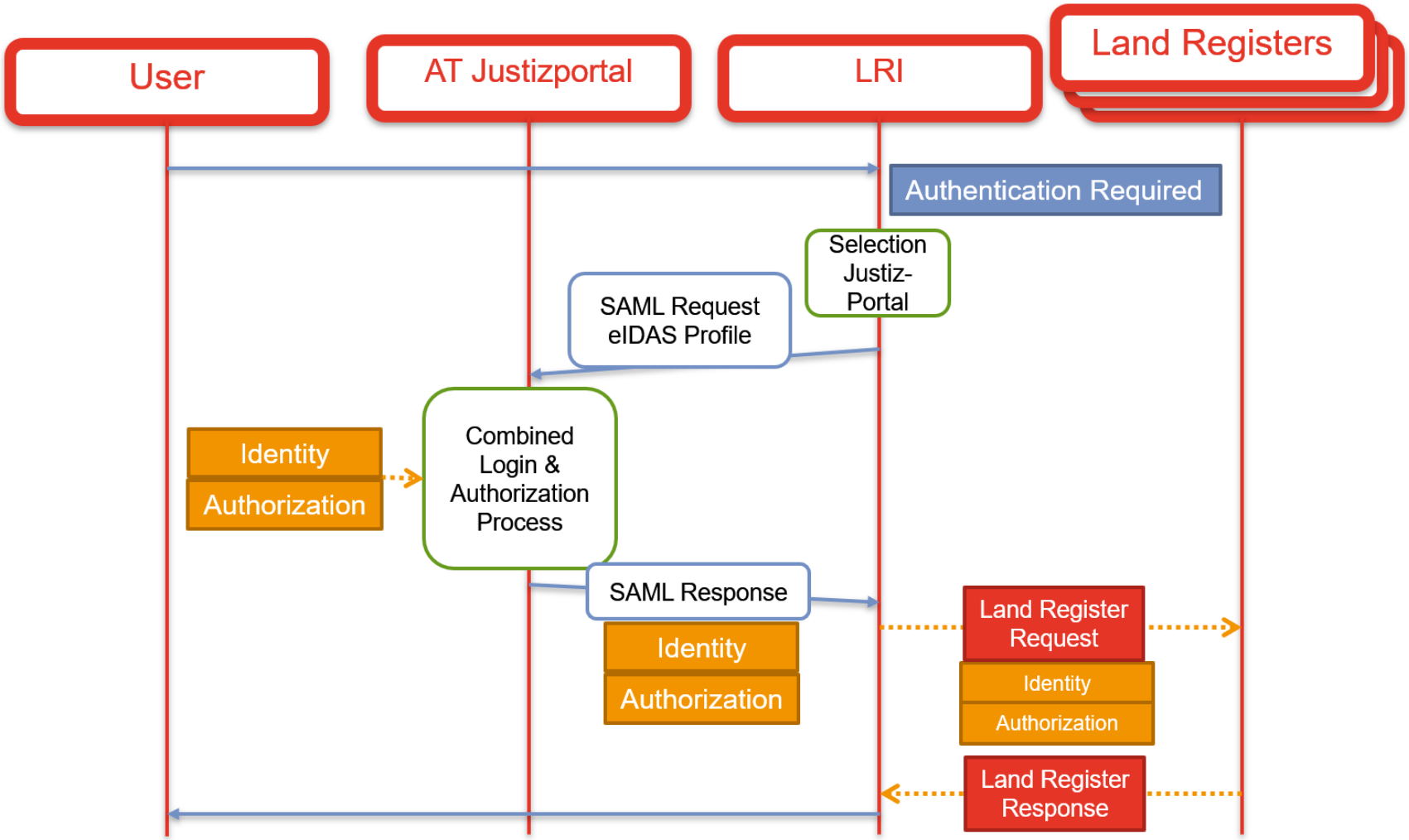
LRI to LR Service Providers



LRI to LR Service Providers

- General thoughts
  - Make AAA not part of the Request-Message
  - Would limit extensibility & maintainability
  - To retrieve AAA parsing of the Message would be needed
  - Trusted Authentication of LRI to Land Registers needed
- AAA Token sent via HTTP Hader
  - Can easily be read and used in application
- Implementation:
  - LRI System authenticates itself via client certificate at the national Land Register (1 certificate needed only)
  - The AAA Token is added to the request via custom HTTP-Header (X-LRI-*)
  - Additionally a transaction-id has to be provided by the eJustice system to make revision and issue tracking easy

Full Picture



How to Integrate your System

- Design Document available
  - Sets out Organisation and Rules applied to Federation
- Austria has a Test-Infrastructure
  - Via the Justice Portal of the ministry of Constitutional Affairs, Reforms, Deregulation and Justice
  - Identity Provider for technical integration test of your Land Register Site
  - Test Service Site for testing your Identity Provider
  - Integrated with eID.AS for Citizen
- To be done:
  - Productive Integration with eJustice Portal
  - Put up Design Document as an online technical Specification

Q&A

Dietmar Gombotz
LFRZ GmbH – a subsidiary of BRZ GmbH
dietmar.gombotz@lfrz.gv.at
+ 43 1 33176 428
+43 664 513 08 71

Learnings of LRI project

- Very different internal structures did lead to discussions about minor points
- Common Language took time to develop
- PAS System was big discussion
  - Missing is a general approach on how to deal with federated Identity Management between MS

Attribute	SAML ID (Idp2LRI)	HTTP (LRI2NLR)
Unique Personal ID	http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	X-LRI-PersonIdentifier
Family Name	http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName	X-LRI-CurrentFamilyName
Given Name	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName	X-LRI-CurrentGivenName
Date of Birth	http://eidas.europa.eu/attributes/naturalperson/DateOfBirth	X-LRI-DateOfBirth
Role	http://e-justice.europa.eu/lri/attributes/authentication/Role	X-LRI-Role
Participant	http://e-justice.europa.eu/lri/attributes/accounting/Participant	X-LRI-Participant
Organisational Unit	http://e-justice.europa.eu/lri/attributes/accounting/OrganisationalUnit	X-LRI-OrganisationalUnit
Invoice Recipient Id	http://e-justice.europa.eu/lri/attributes/accounting/InvoiceRecipientId	X-LRI-InvoiceRecipientId
Cost Center Id	http://e-justice.europa.eu/lri/attributes/accounting/CostCenter	X-LRI-InvoiceRecipientId
Transaction Id	- - - NONE - - -	X-LRI-TransactionId

All Use-Cases: Long Term View