Securing your Standards Based Services

Rüdiger Gartmann (con terra GmbH)

Satish Sankaran (Esri)

Agenda

- What are your security goals?
- Access control
- Standards and interoperability
- User management and authentication
- Enabling security for the ArcGIS Platform
- OGC and security standards – the missing link

Security Goals – Privacy

- Access to your information shall be restricted
- Communication shall be private
- You want to decide who shall access which information

Technical means:

- Access control
- Encryption

Security Goals - Integrity

- Data shall not be falsly modified
- Receiver of a massge shall be safe that it was not changed after it was sent

Technical means:

- Digital signatures

Security Goals - Authenticity

- The origin of information shall be proven
- The receiver of information shall be proven

Technical means:

- Digital signatures
- Public key encryption
- Certificates

Security Goals – Non Repudiation

- No party shall be able to deny a previous communication
- Make communication auditable

Technical means:

- Digital signatures

So what is your security toolset?

- Encryption → use HTTPS
- Public key infrastructure → use HTTPS with trusted SSL certificates
- Digital signatures → use HTTPS with trusted certificates
- Authentication → many different ways to do this
- Access control → Inside of the service

Interoperability Challenge

Access Control

What is Access Control?

Access control enforces

who (subject) → Alice

shall be able to perform

what (action) → view

on which

resource → service ‘SampleWorldCities’

Policy1:

Subject:

Alice

Action:

view

Resource:

service ‘SampleWorldCities’

Policy2:

Subject:

Group ‘Customer A’

Action:

*

Resource:

service ‘SampleWorldCities’

Defining Policies in ArcGIS

Policy2:

Subject:

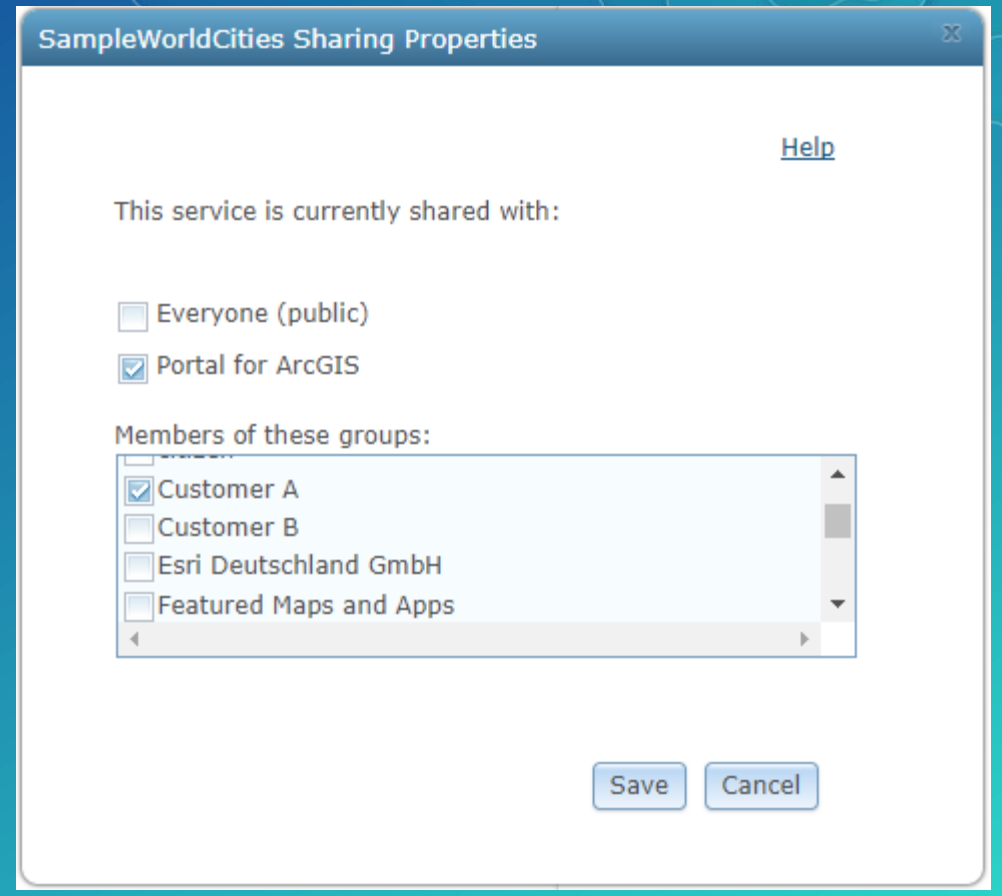
Group ‘Customer A’

Action:

*

Resource:

service ‘SampleWorldCities’

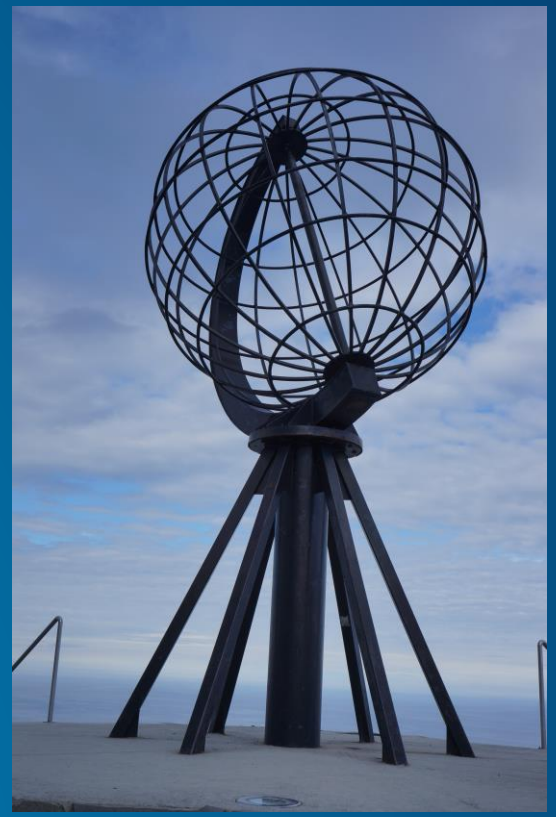


Access Control – Is Spatial Special?

- Spatial data is not impartible…

- There are
  - Layers
  - Objects
  - Geometries
  - …

→ Spatial access control is an extra challenge!



Extending Policies for Spatial Data

- Policies can be extended by obligations
- Obligations can be anything
- Access control system needs to fulfill obligation, otherwise policy cannot become effective
- If obligations are used, the access control system needs to be aligned with the obligation semantics

Policy2:

Subject:

Group ‘Customer A’

Action:

*

Resource:

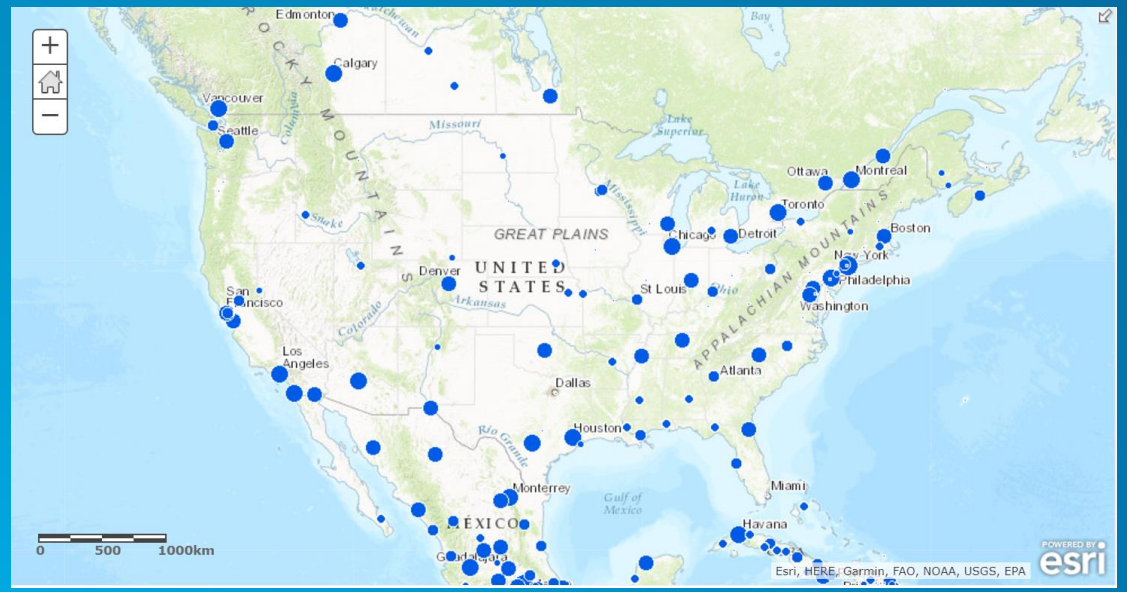
service ‘SampleWorldCities’

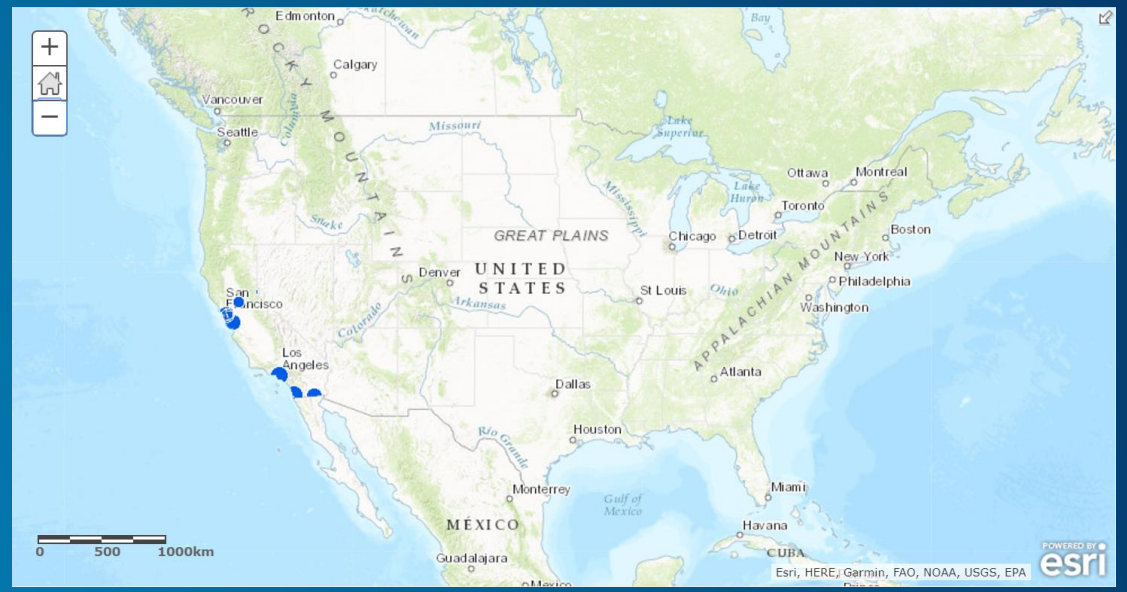
Obligation:

‘Restrict access to the area of California’

Examples for Obligations

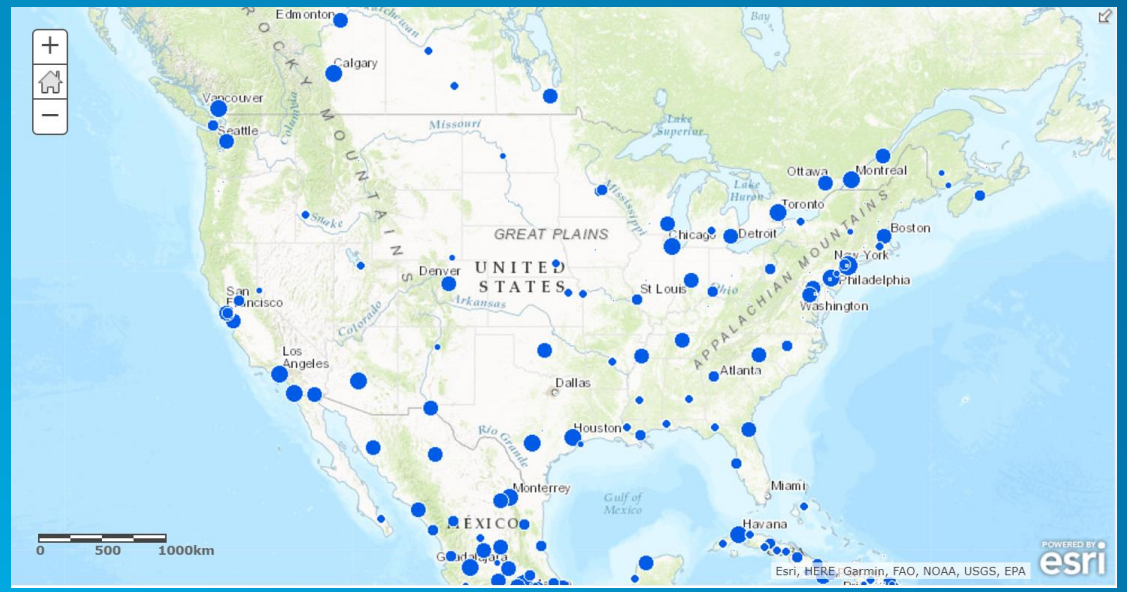
- Restrict to California

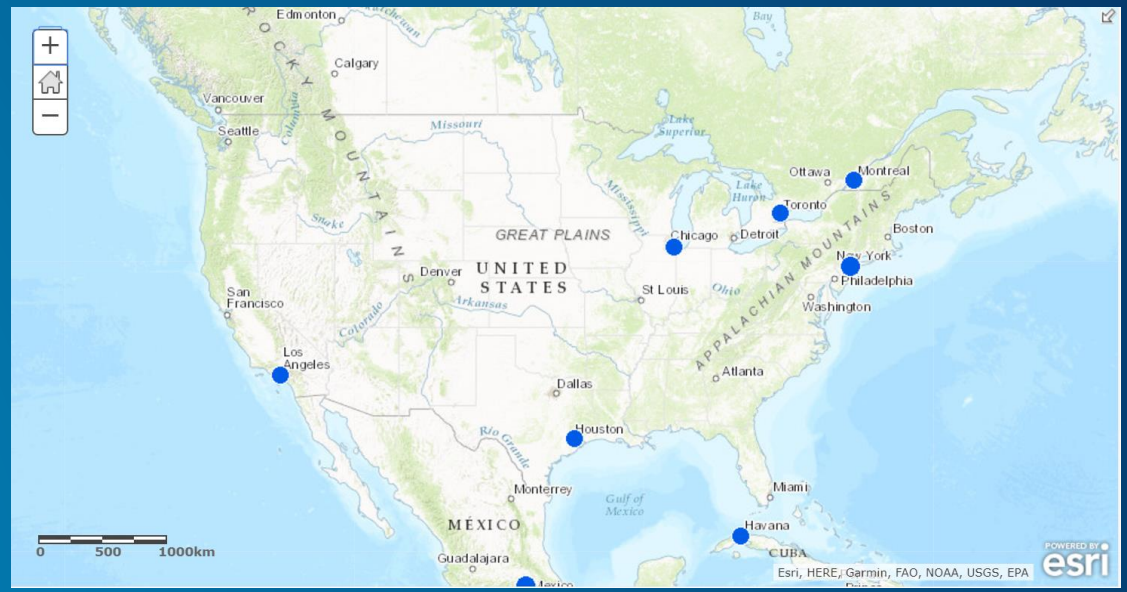




Examples for Obligations

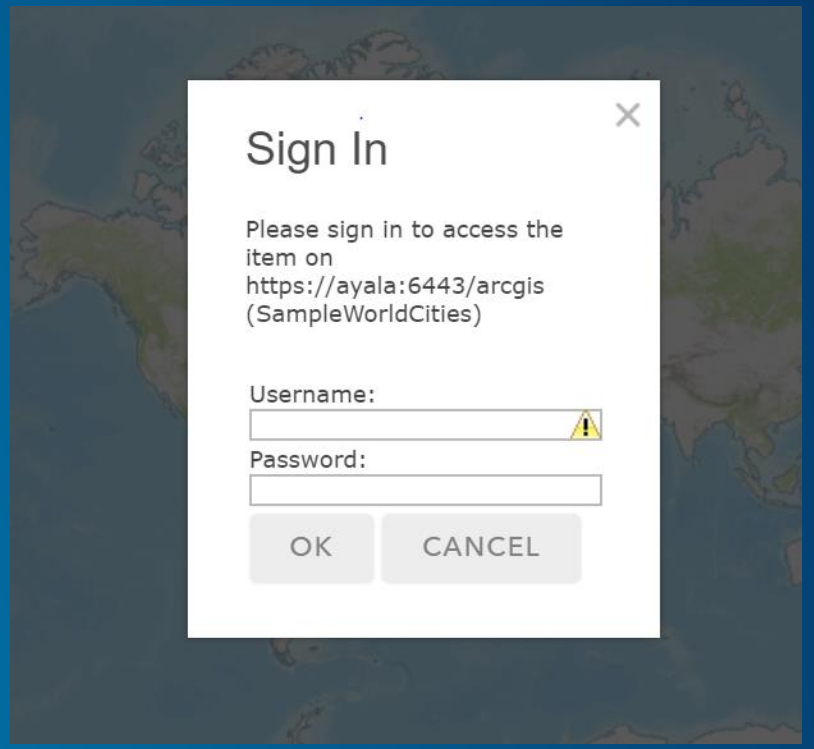
- Restrict to Cities with pop > 2,000,000

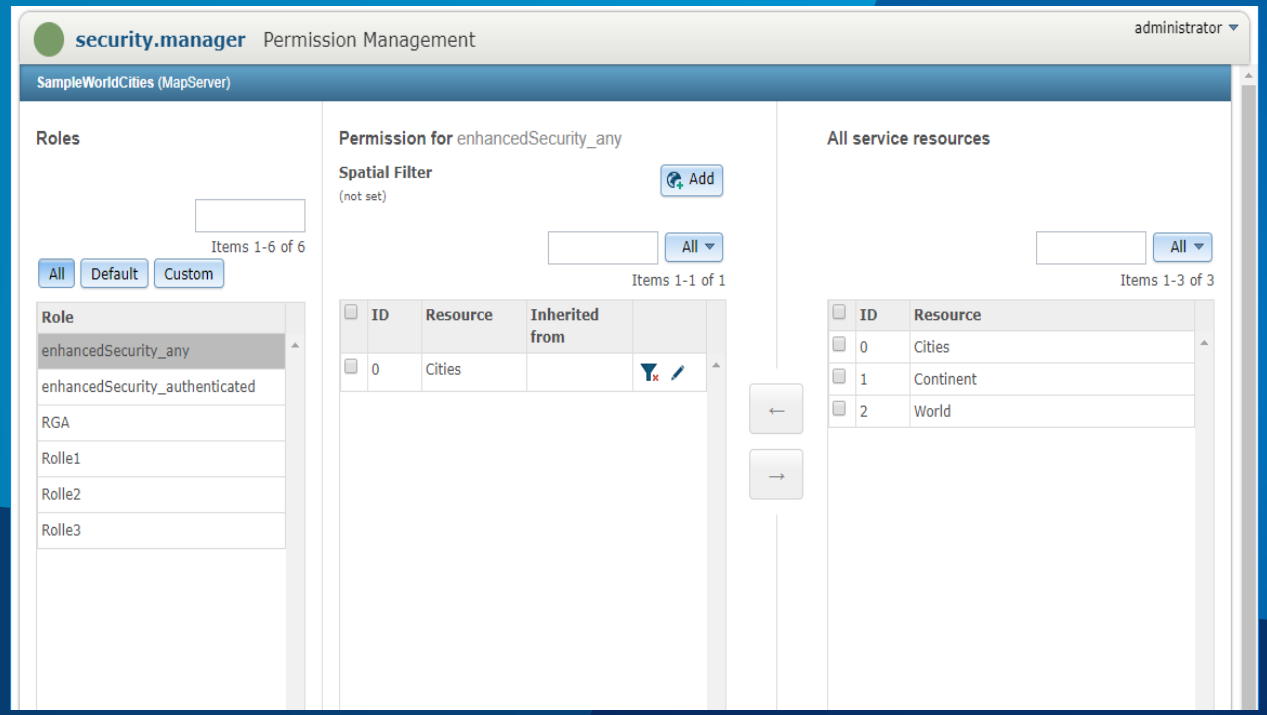




Requirements for Access Control

- Users need to be identified
- User identity needs to be verified (authentication)





Access Control

Demo

Standards and Interoperability

What is Interoperability?

If two or more systems are capable of communicating with each other, they exhibit syntactic interoperability when using specified data formats and communication protocols.

Wikipedia

Where is the Interoperability Challenge?

- Network protocols and encryption are standardized (HTTPS)
- Geospatial protocols are standardized (OGC)
- Policies and policy decisions are standardized
  - But: This remains internal
  - Not crucial for interoperability
- Authentication and identities are standardized
  - But: there are so many different standards!

Interoperability Challenge

User Management and Authentication

Key Requirement: Identify the User!

How can a system do that?

- Authenticate a user
  - OAuth 2.0
  - Token-based
  - PKI
  - HTTP Basic / Digest
  - Windows Authentication
- Trust a remote authentication
  - SAML 2.0 (Enterprise Login)

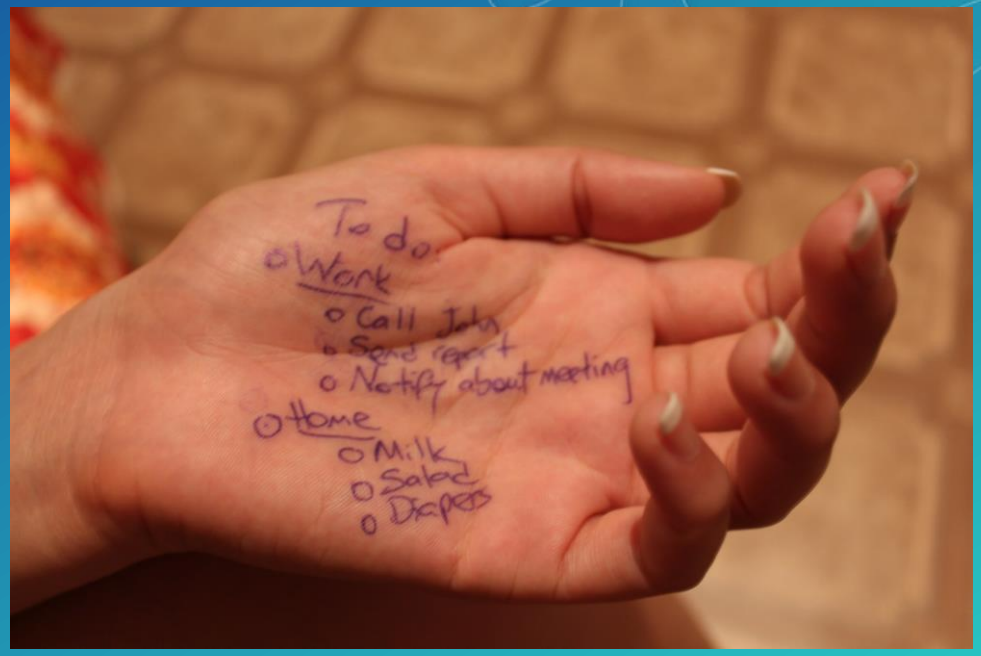
User Management

Who is in charge?

- ArcGIS Platform
  - Built-in user store
- Active Directory
  - Portal connecting to Active Directory
  - Enterprise Login
  - Windows Authentication
- Remote
  - Enterprise Login

Guidelines

- Use HTTPS (only)
- Use trusted certificates
- Provide user repository
- Lock down non-public services
- Create permissions



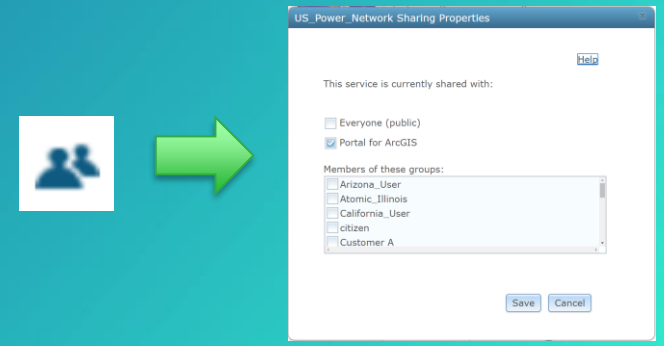
Access Control in ArcGIS – Service Level

Desktop

Web

Device

Server



Access Control in ArcGIS – Fine-Grained Control via SOI

Desktop

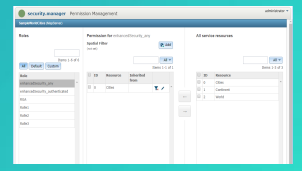
Web

Device

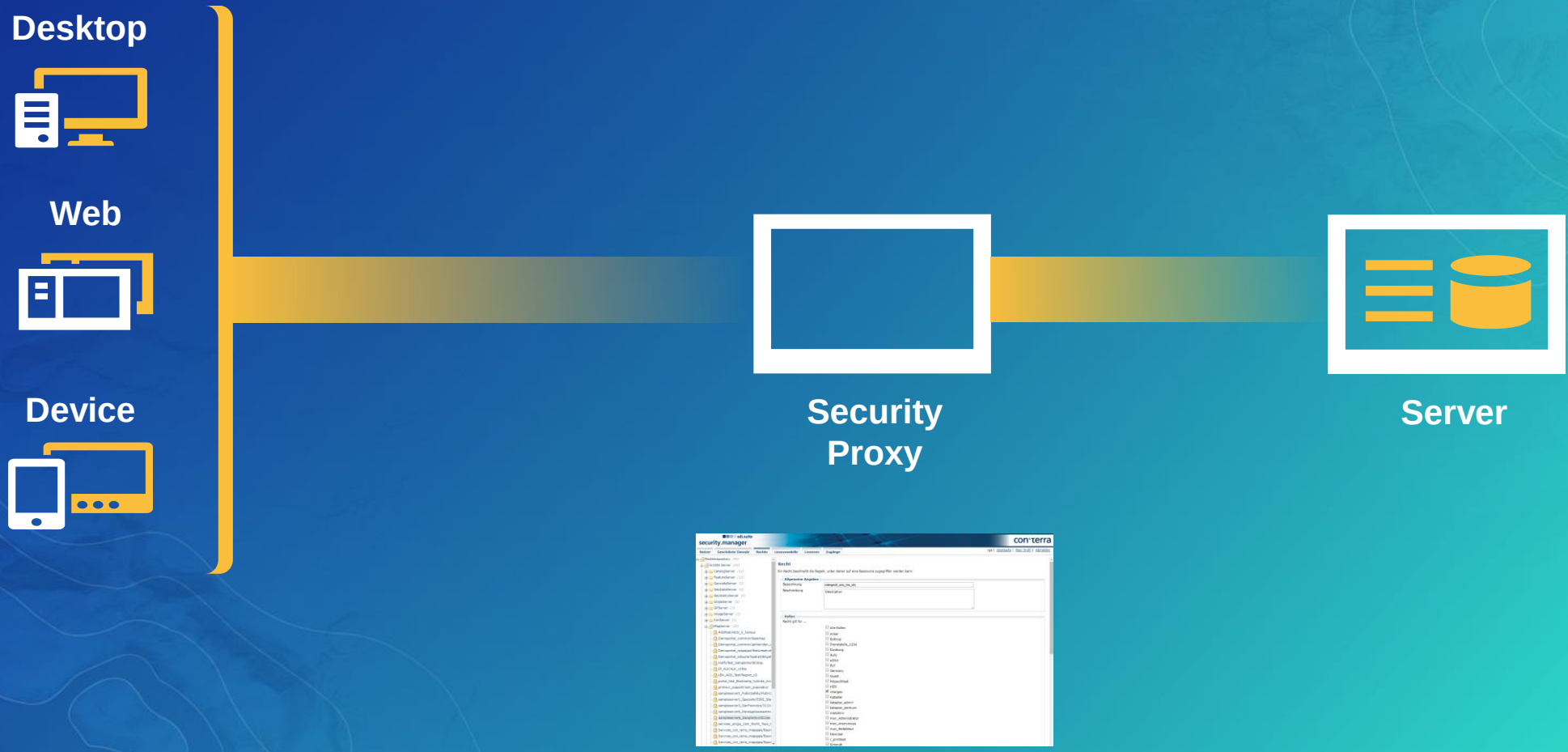
SOI

Server

Manage Permissions



Access Control in ArcGIS – Fine-Grained Control via Proxy



Security-Standardization at OGC

- GeoXACML
  - Standard to define spatial policies
  - Defined 2007
  - Based on XACML (OASIS)
  - No commercial implementation yet
- However…
  - Defining policies is not an interoperability challenge
  - Authentication *is* an interoperability challenge
  - No standardization of authentication by OGC yet

→ Secure interoperability between different software vendors is still not ensured


esri
THE
SCIENCE
OF
WHERE