Securing Your ArcGIS Server Services
An Introduction

David Cordes & Derek Law
Esri – Redlands, CA

Technical Workshop

Agenda

- Security in the context of ArcGIS for Server
- Background concepts
- Access
- Authentication
- Authorization: securing web services
- ArcGIS for Server + Portal for ArcGIS
- Encryption and certificates
- Security architectures
- Summary

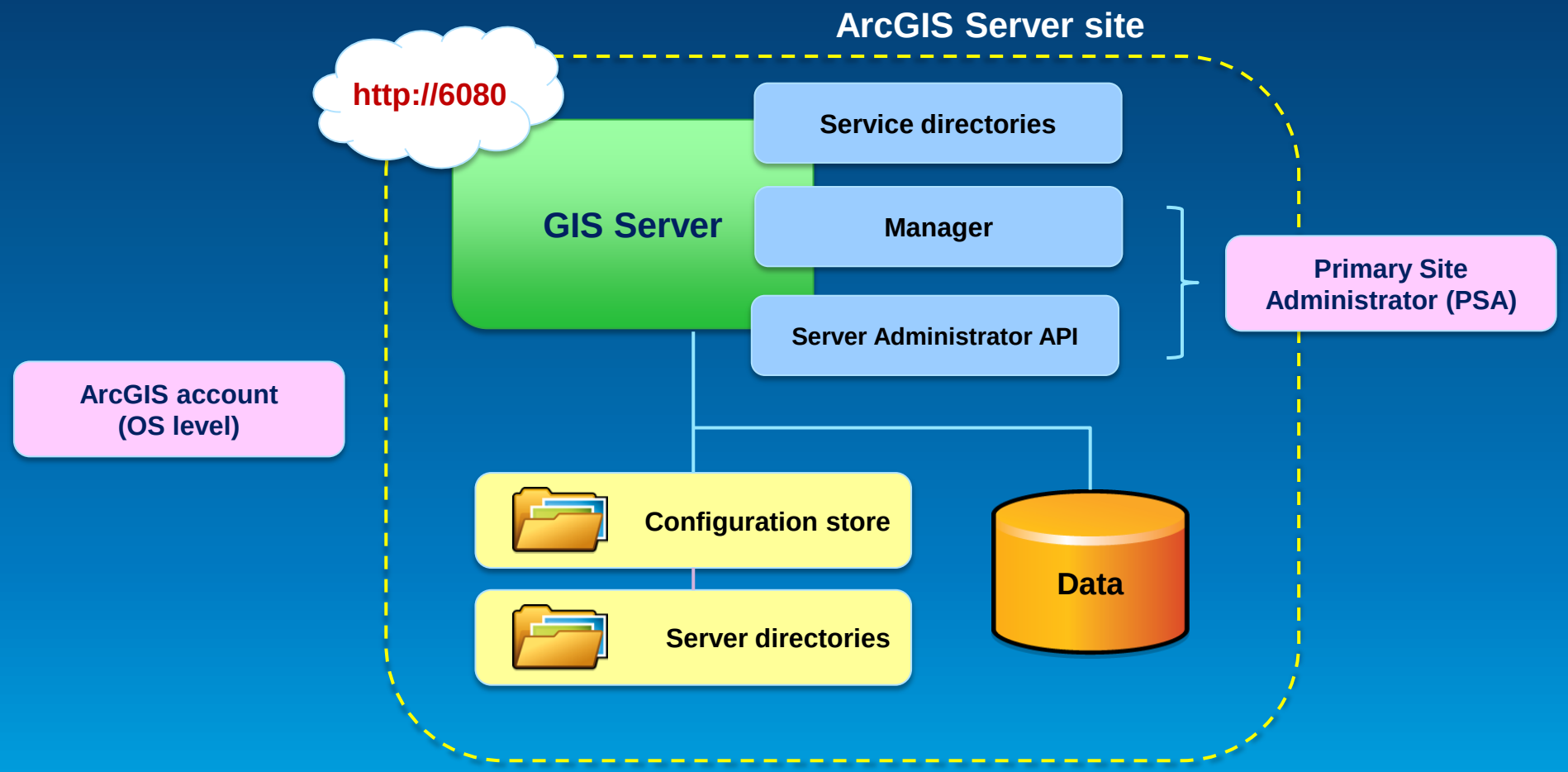
How to configure

ArcGIS for Server Security

Protect your assets
Control access and set permissions

Review: ArcGIS for Server Architecture

10.1 and later releases



Access

Who can login ArcGIS for Server?

ArcGIS for Server Access

- **User** → Valid login to access
- **Role** → Grouping of users
  - 3 types
  1. **Administrators** – Full admin control
  2. **Publishers** – Publish web services
  3. **Users** – View web services

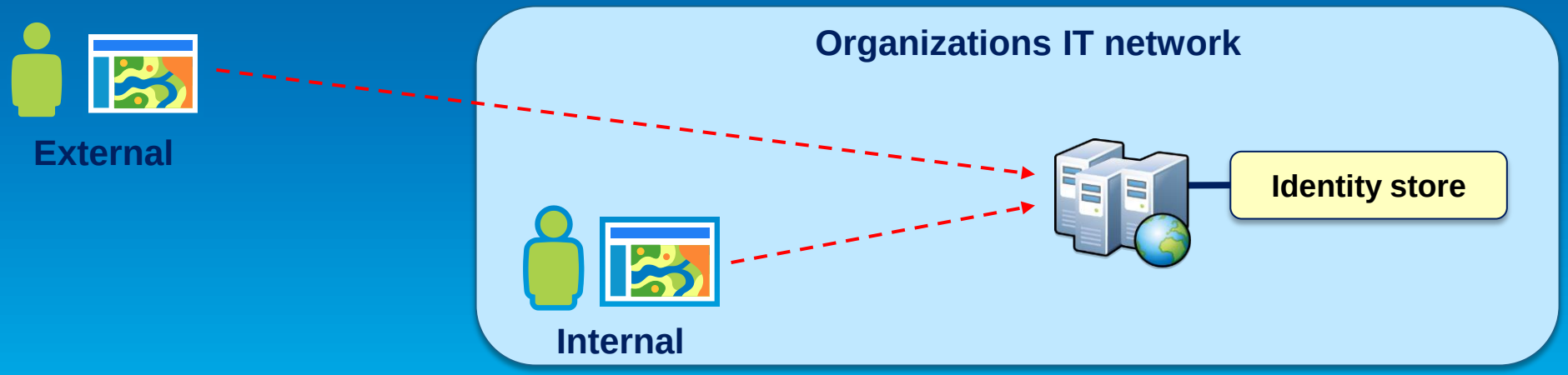
- **Identity store** → Defines your users and roles
  - User store + Role store

A

ArcGIS for Server: User considerations

- Where are your users coming from?
  - Determines which type of identity store you should use

- Intranet → Windows Active Directory or LDAP
- Internet → Built-in or custom



A

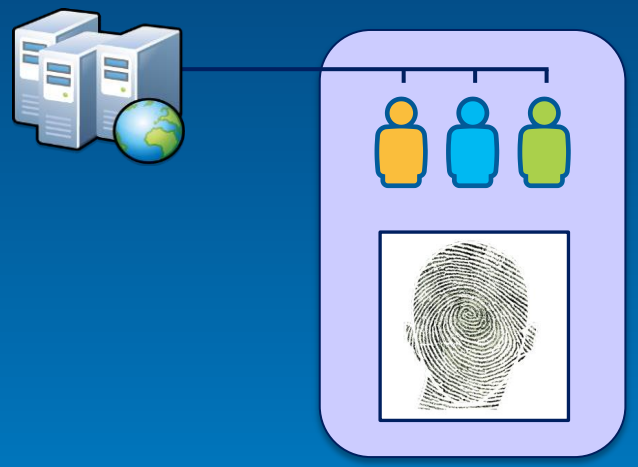
ArcGIS for Server: Role considerations

- How much control do I have on my ArcGIS Server site?
  - Managed by me, within my Dept? or
  - Managed by my organization's IT Dept
- May affect where you define your roles

A

ArcGIS for Server: Identity Store

- Identity Store → Defines your users and roles
- 3 different options
  1. Built-in (default)
  2. Register with an enterprise identity store
     - Windows Active Directory
     - LDAP
  3. "Mixed mode"
     - Users from enterprise identity store
     - Roles from built-in store



A

Demo

ArcGIS Server Manager

Show users and roles

Authentication | Check and verify user identity

Authentication Tier/Method

- **Authentication** → Check and verify user identity

- 2 options

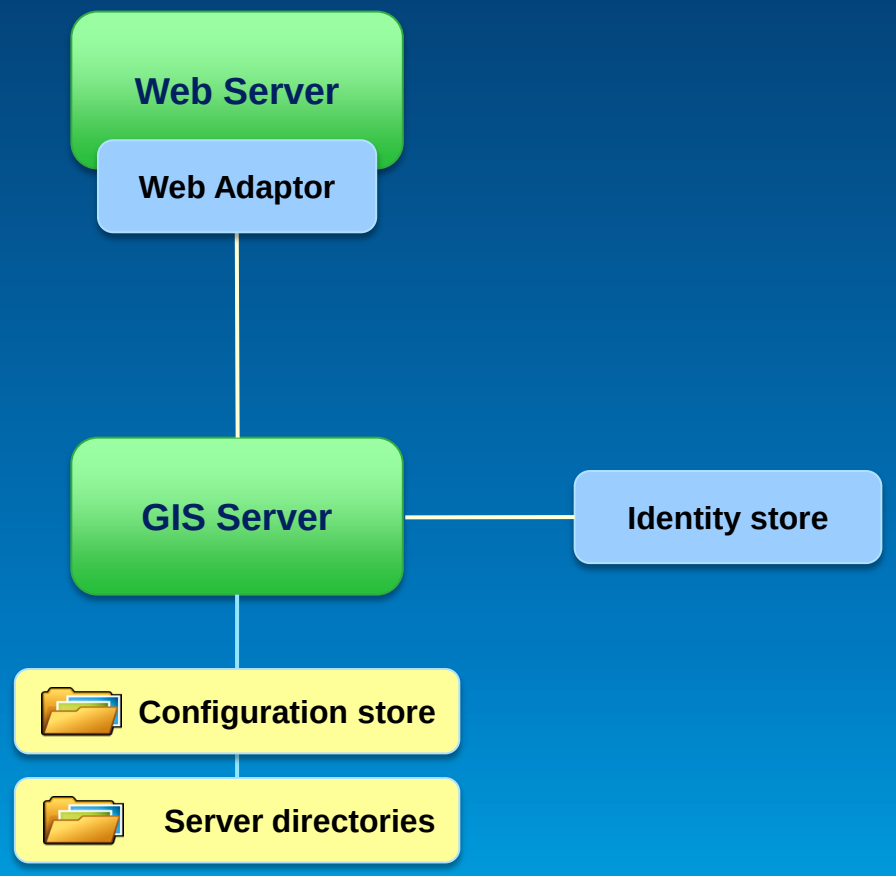
1. **GIS Tier**
   - Uses tokens to authenticate
2. **Web Tier**
   - Uses HTTP authentication
     - E.g., Basic, Digest, Integrated Windows, Client certificates, and Custom

A

Review 2: ArcGIS Server Architecture

Other components of a Server site

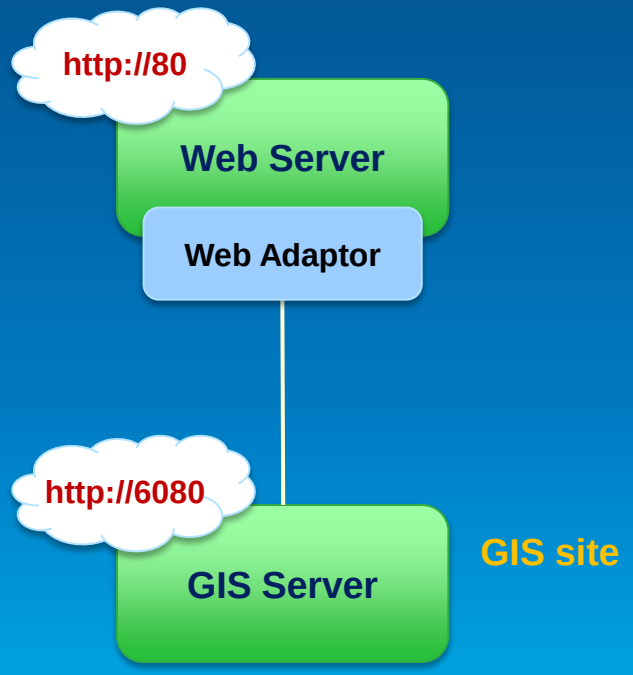
- ArcGIS Server site
- + Identity store
- + 3rd party web server
- + Web Adaptor



A

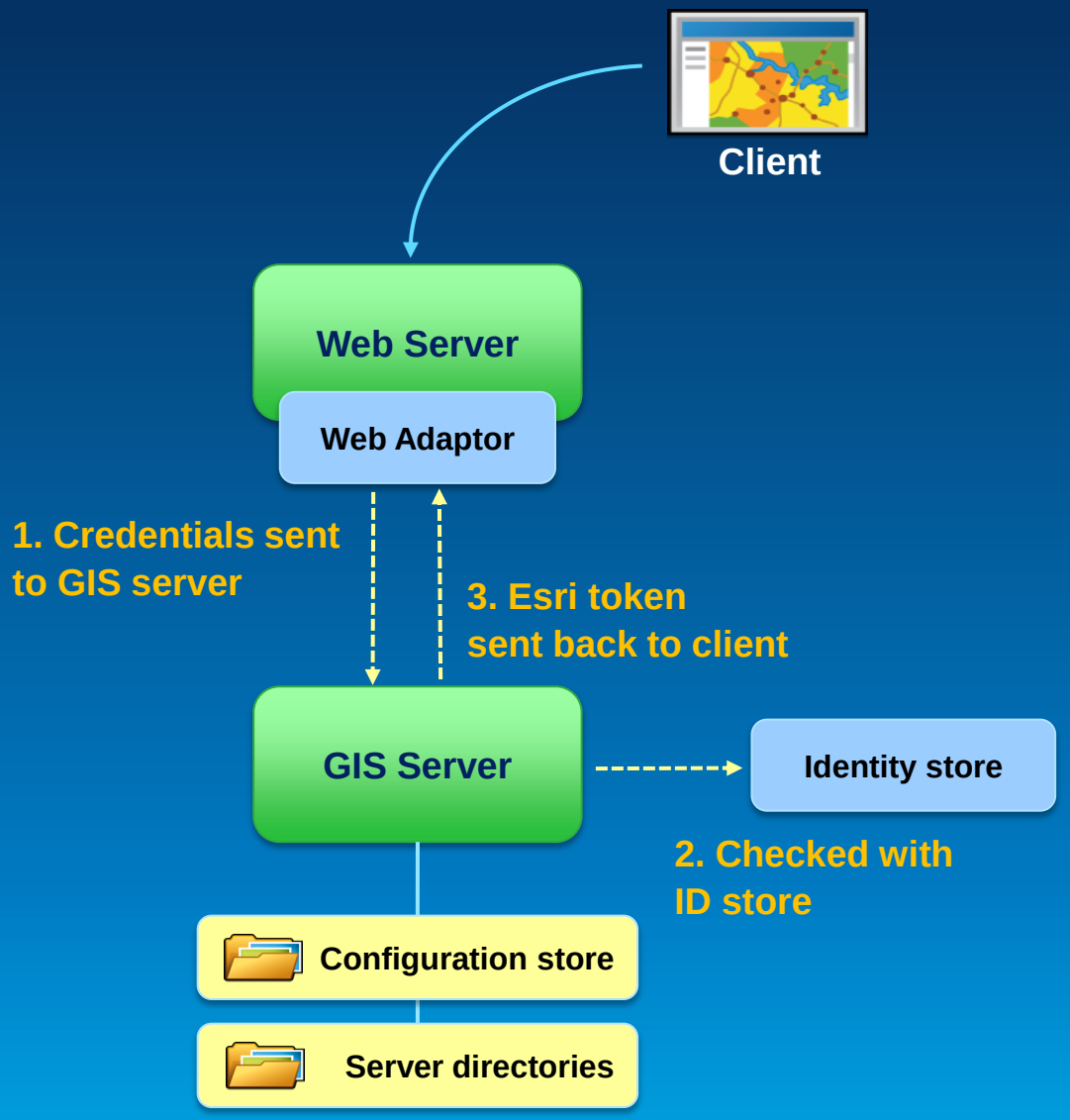
ArcGIS for Server – Web Adaptor

- Enables ArcGIS Server to work with 3rd party web server
  - E.g., IIS, Web Sphere, etc.
- Leverage web server features
- Provides more flexibility to control site access
- Conceptually like a reverse proxy



GIS Tier Authentication

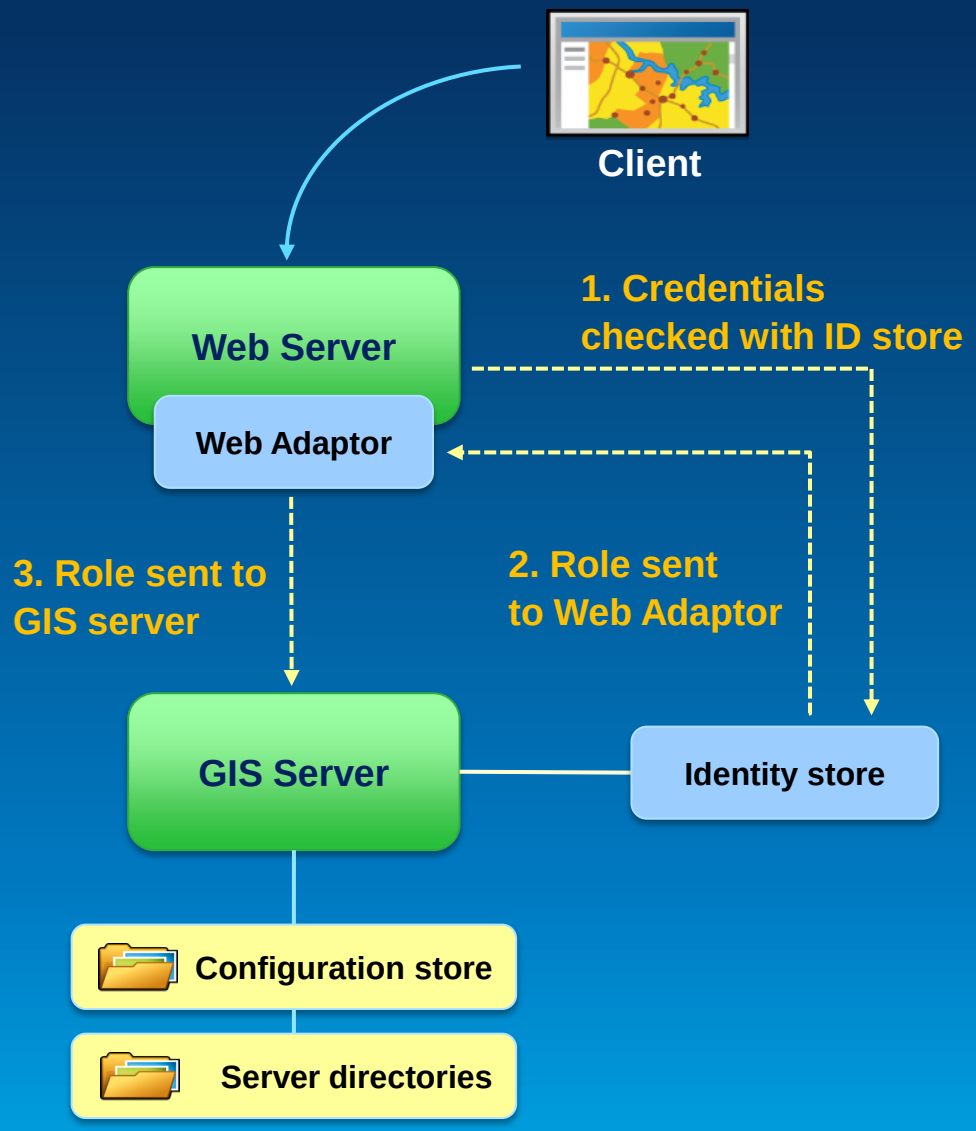
- GIS Server checks credentials
- **Token** → Unique identifier sent from Server to client to identify an interaction session



A

Web Tier Authentication

- Web server checks credentials
- Must use Web Adaptor
- HTTP authentication



A

GIS Tier vs. Web Tier Authentication

	GIS Tier / Token	Web Tier / HTTP Auth
Default	Yes	No
Public / anonymous possible	Yes	Yes
Clients Supporting	Esri	All, including OGC
Requirements	Enable SSL	Web Adaptor(s) required Basic – require SSL Digest – special setup IWA – Windows only

Demo

ArcGIS Server Manager

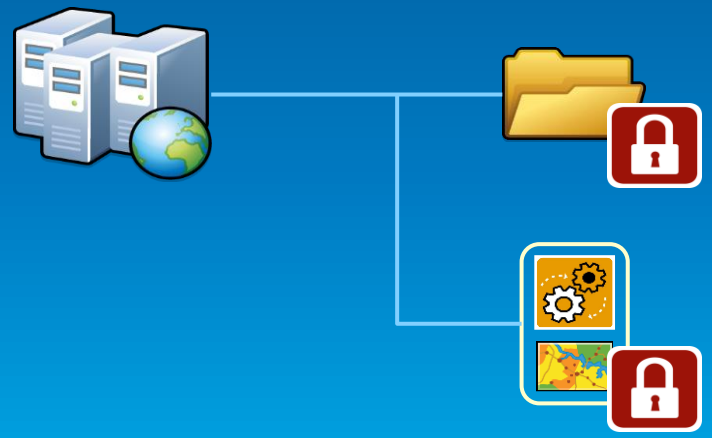
Show how to set-up authentication in wizard

Show IIS configuration of Web Adaptor

Authorization | What you are allowed to do

Securing GIS Web Services

- Set permissions for roles on folders and services
  - Administrators/Publishers grant permissions
- All new services are public by default
  - Anonymous access
- Can specify whether folders require HTTPS



Demo

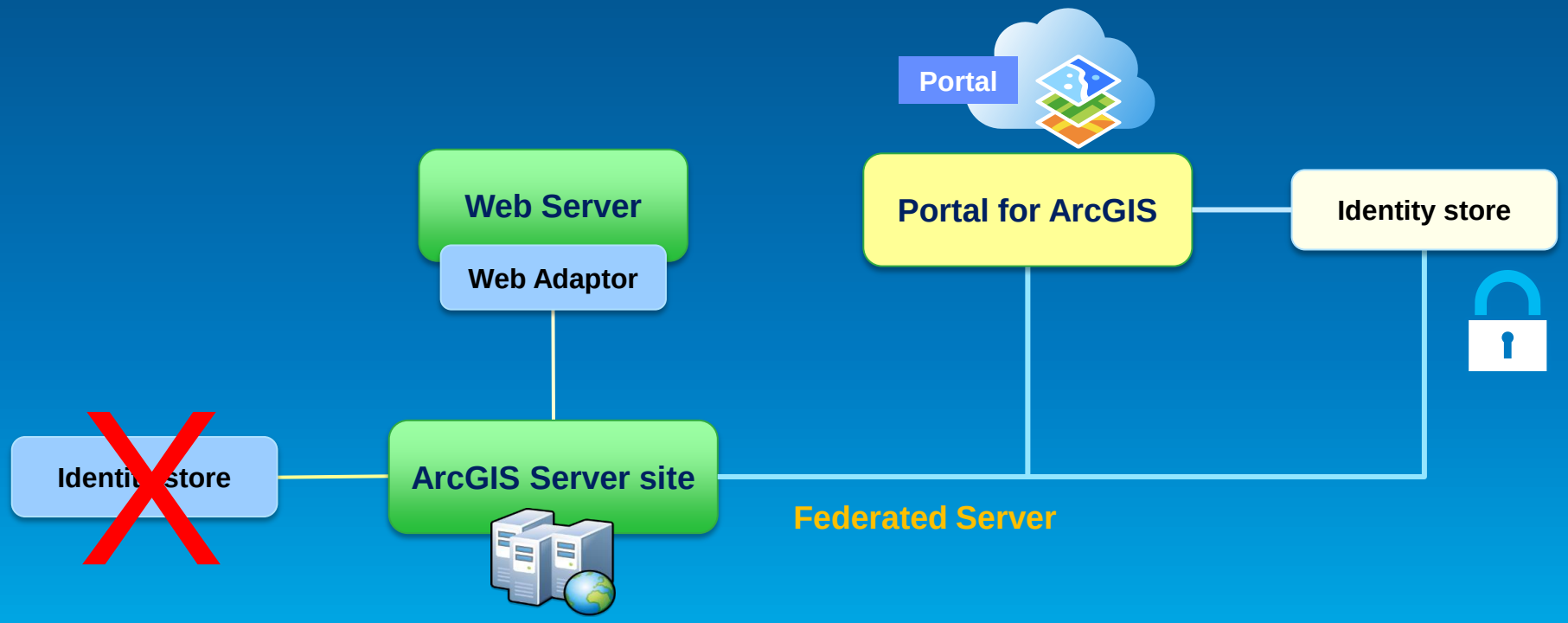
ArcGIS Server Manager

Show securing a web service

Show accessing a secured service in a client application

ArcGIS for Server + Portal for ArcGIS

- You can federate an ArcGIS Server site with Portal for ArcGIS
- Federated server → Server site uses Portal's identity store



A

Encryption and HTTPS

Securing communication protocols

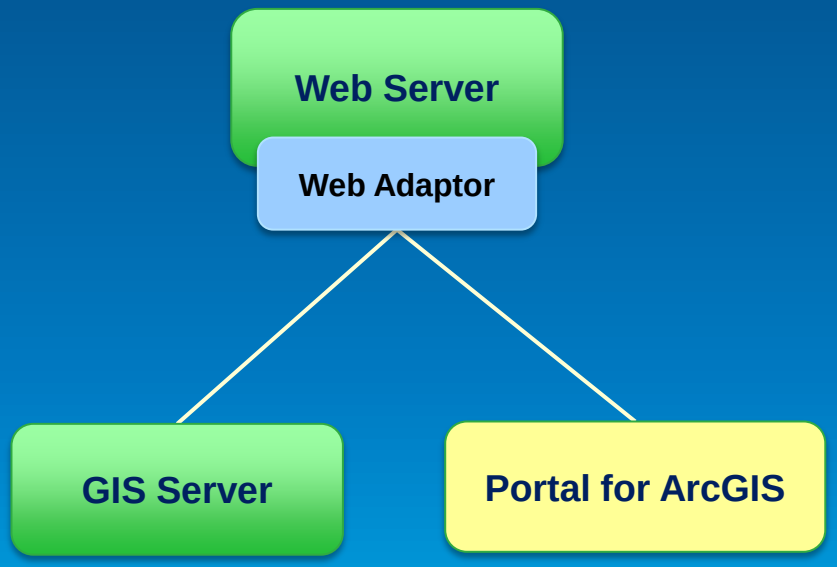
Should you be using HTTPS?

Hypertext Transfer Protocol Secure (HTTPS)

Yes!

Do I need to get a CA signed certificate for ArcGIS Server or Portal?

No, just for your reverse proxy or Web Adaptor.



What do you need to do if you need a certificate?

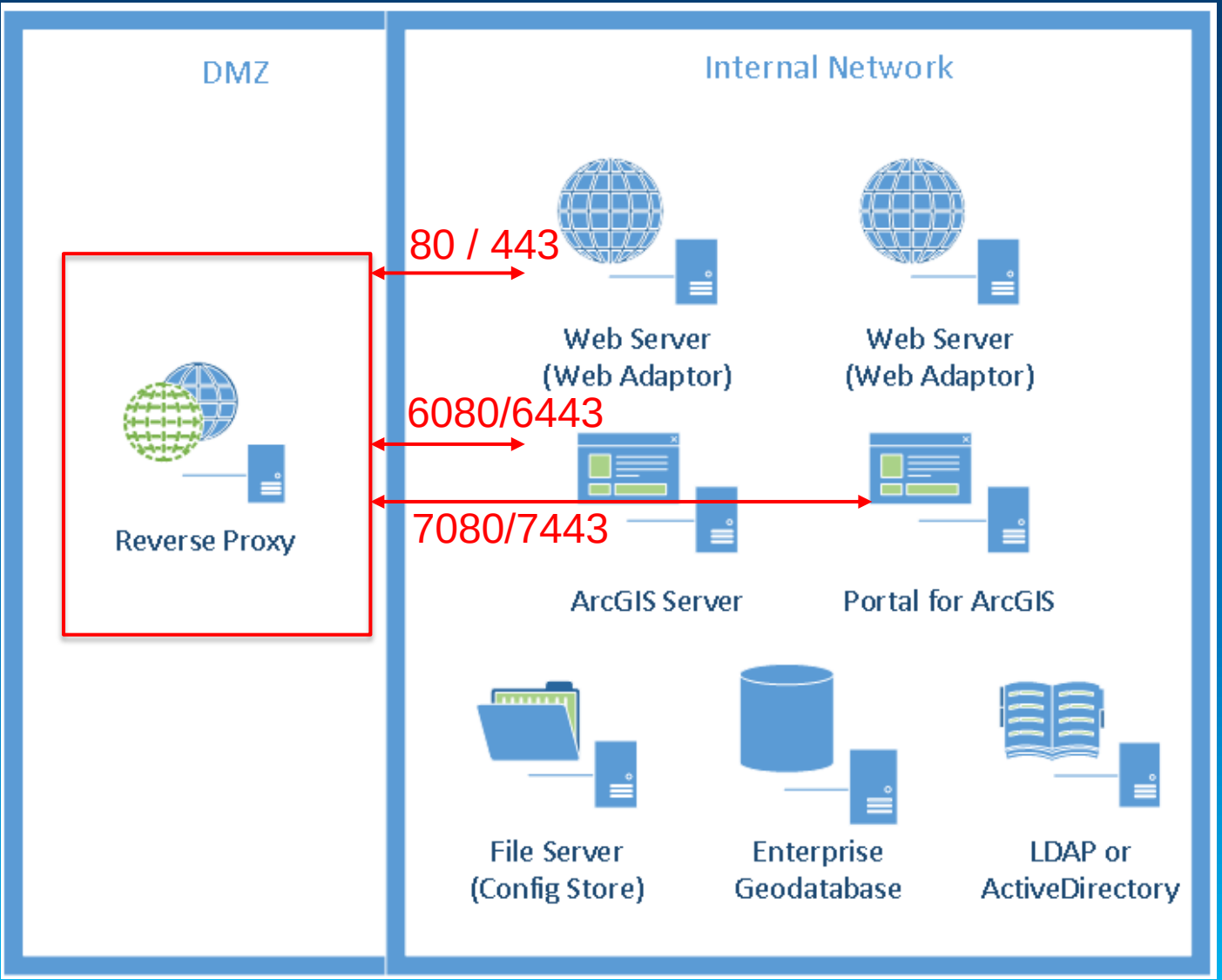
1. Generate a CSR
2. Send CSR for signing
3. Import signed certificate

Security Architecture – Introduction

- Deployment of machines and components
- Demilitarized Zones (DMZ) → a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet
- Applies to internal-only sites or Internet-facing

Internal Oriented Security Architecture

- Pros
  - Fast to setup
  - Easy to manage
- Cons
  - Exposes internal network
  - Less controlled



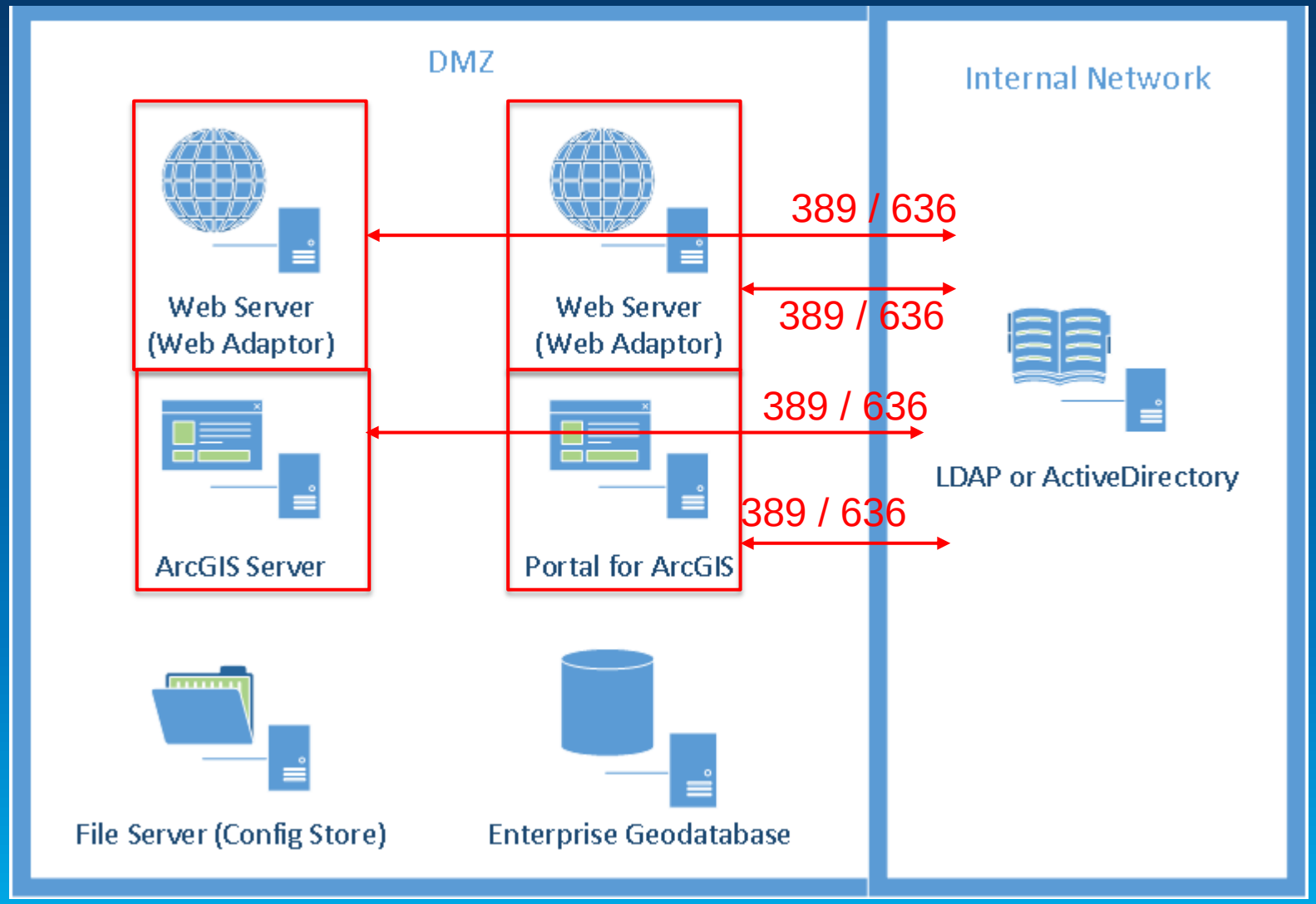
External Oriented Security Architecture

Pros

- Limited internal exposure
- Highly Controlled

Cons

- Data management issues
- Risk to LDAP/AD



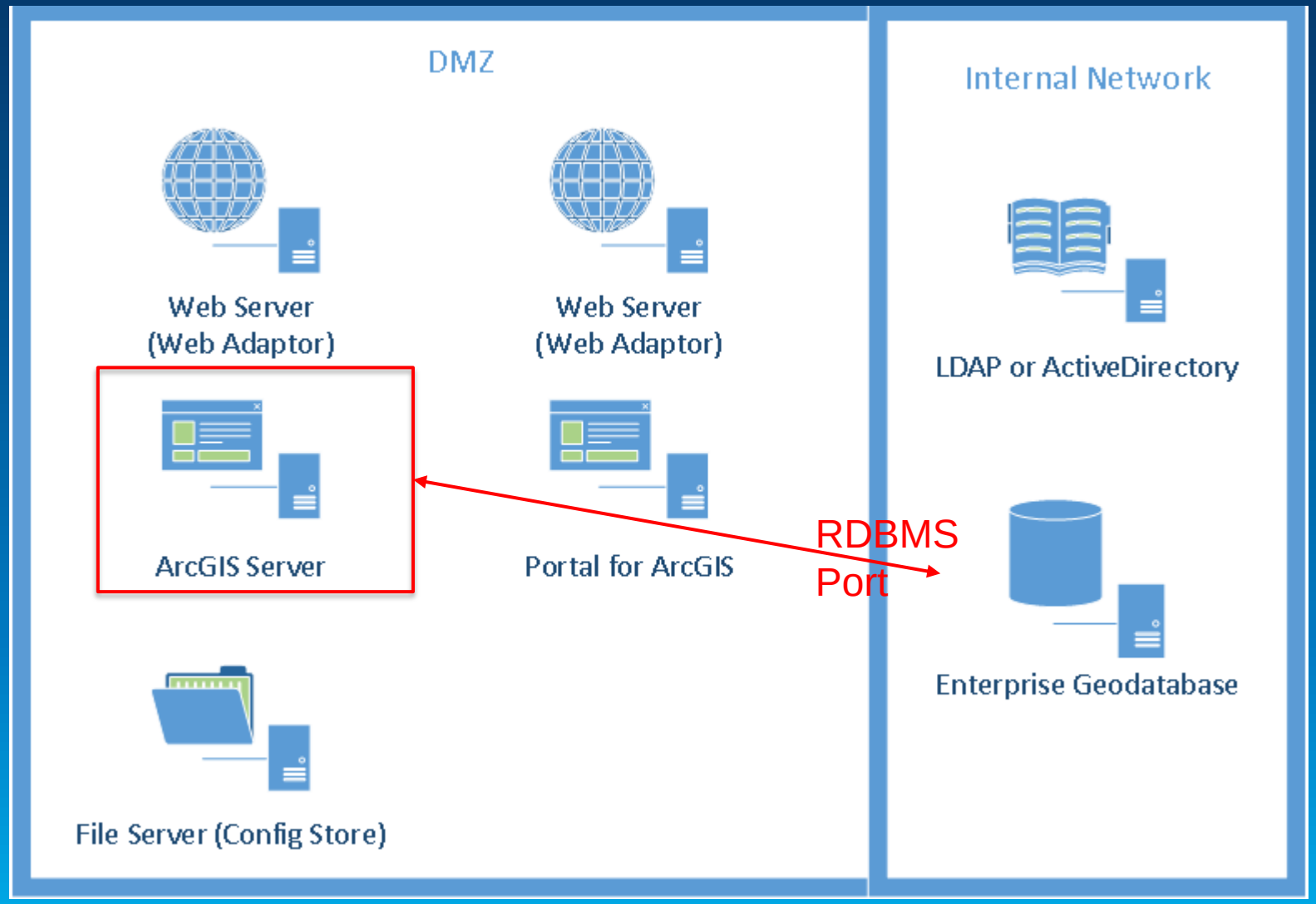
Hybrid Security Architecture

Pros

- Limited internal exposure
- Controlled
- Data easier to manage

Cons

- Risk to database
- Risk to LDAP/AD



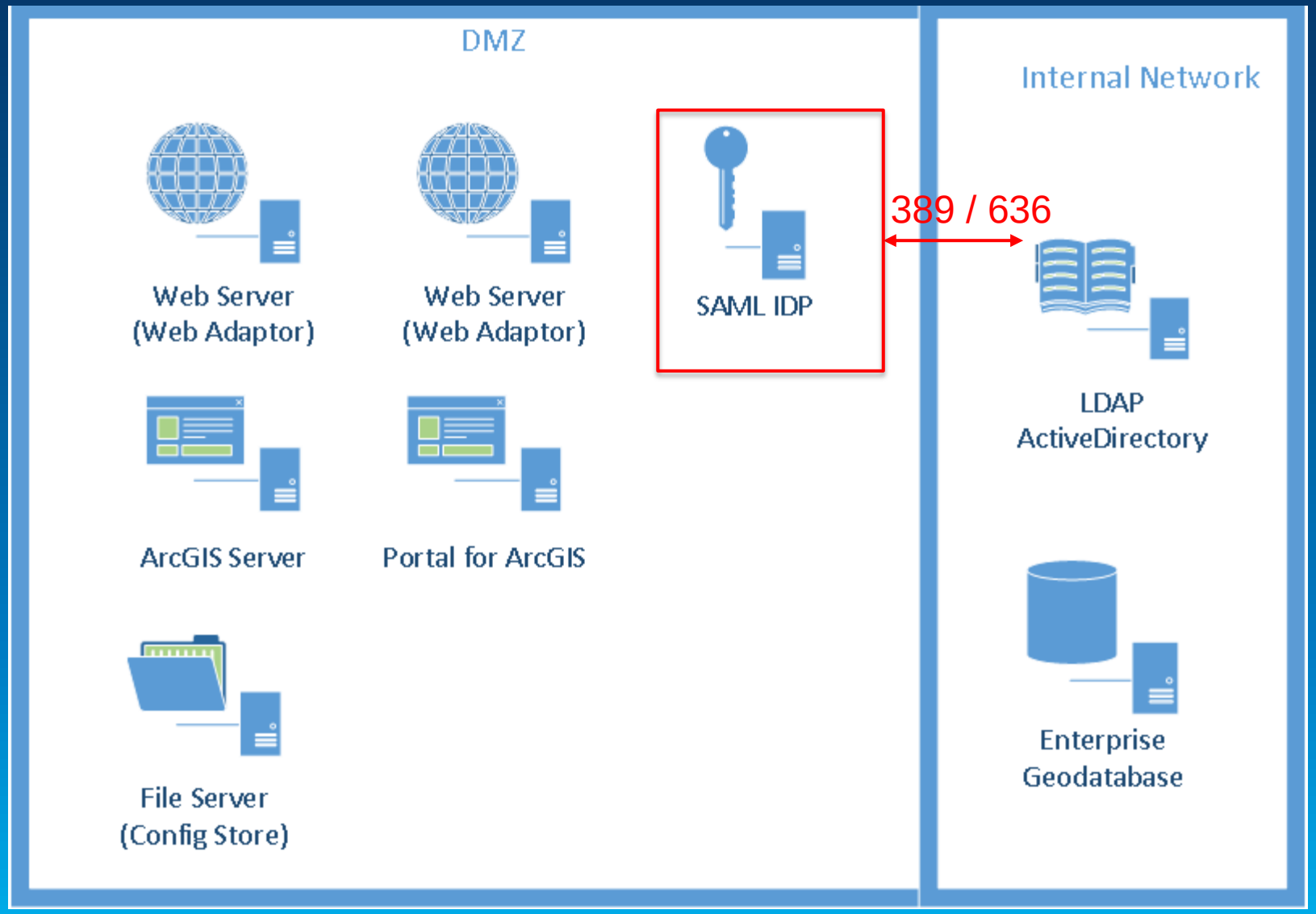
10.3 Hybrid Security Architecture

Pros

- Limited internal exposure
- Highly Controlled
- Single point into your LDAP or ActiveDirectory
- Easy data management

Cons

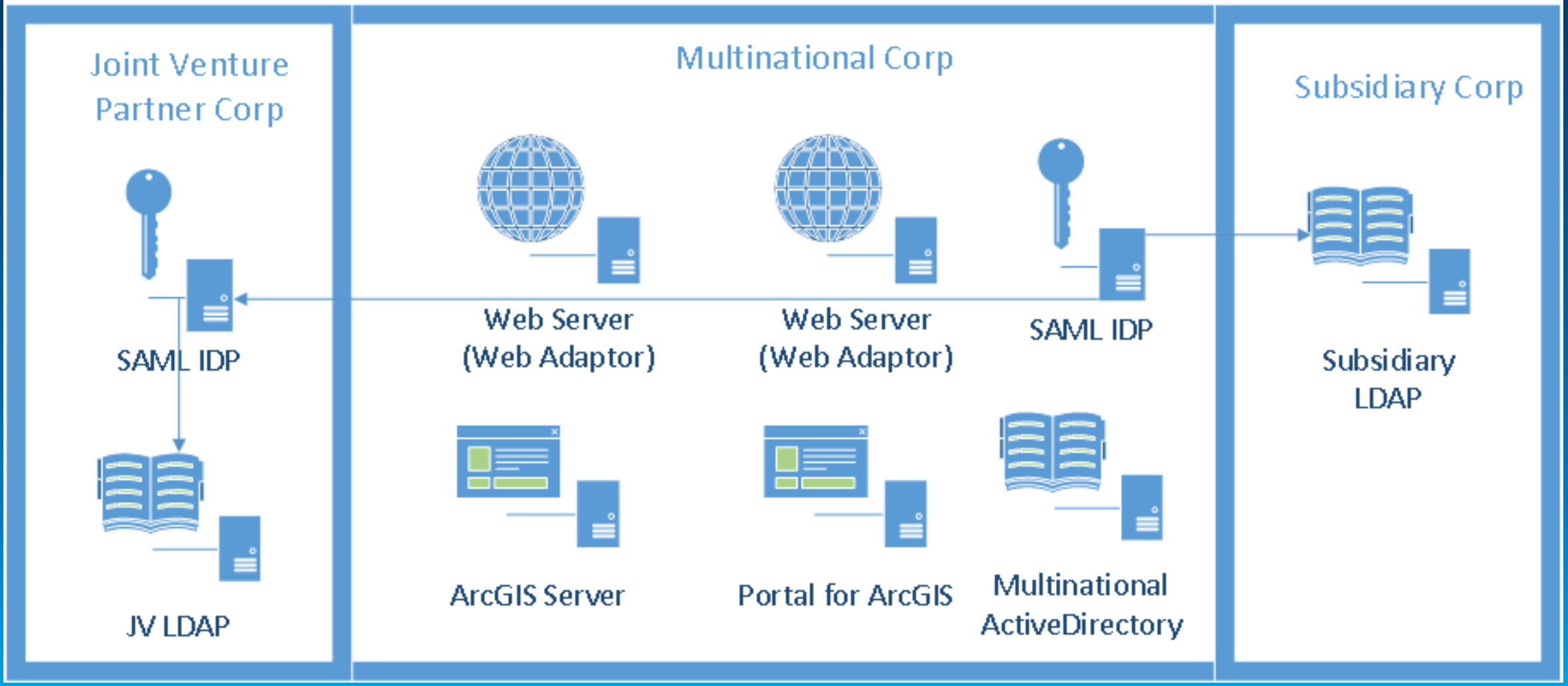
- Some database risk
- Requires 10.3
- Requires Portal



Security Architecture for Multiple Organizations

- **Scenario:**
  - **You are a multinational**
  - **You work closely with another company that you own, a subsidiary**
  - **You work closely with a competitor through a joint venture**
  - **People from the subsidiary and joint venture need access**

10.3 Multiple Federated Organizations



Summary

- Security in the context of ArcGIS for Server
- Background concepts
- Access
- Authentication
- Authorization: securing web services
- ArcGIS for Server + Portal for ArcGIS
- Encryption and certificates
- Security architectures
- Summary

Thank you…

- **Please fill out the session survey:**

First Offering ID: 658

Second Offering ID: 1129

Online – www.esri.com/ucsessionsurveys

Paper – pick up and put in drop box

Other Security sessions

- **Designing an Enterprise GIS Security Strategy**
  - **Thurs July 15, 8:30 – 9:45 am, Room 31C**
- **Securing Your ArcGIS Server Services: Advanced**
  - **Thurs July 15, 1:30 – 2:45 pm, Ballroom 6E**
- **Please complete survey: www.esri.com/ucsessionsurveys**
  - **Session ID: 1129**

Understanding our world.