



Implementing Security for ArcGIS Server Java Solutions

Shreyas Shinde



Introductions

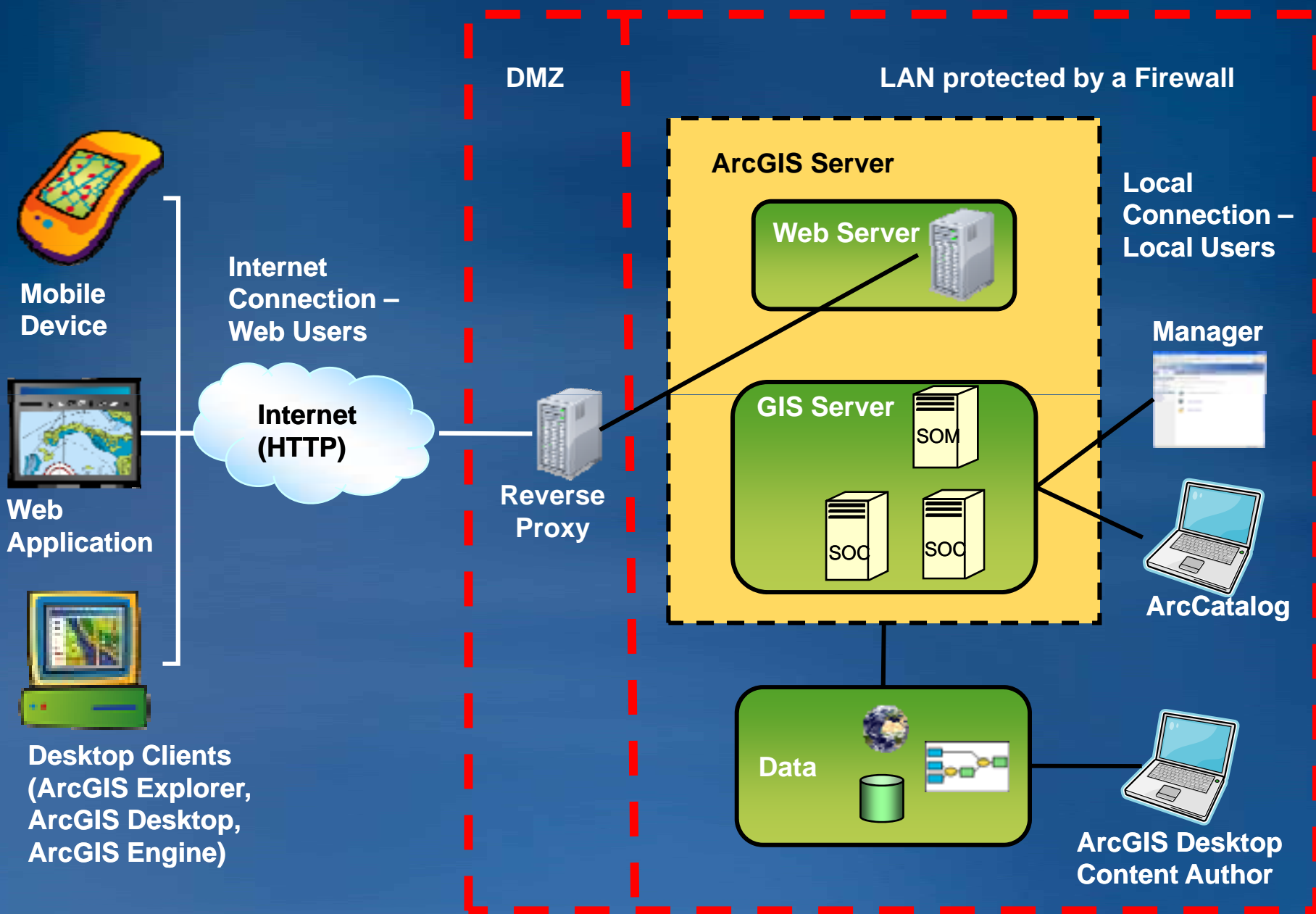
- **Who are we?**
 - **Developers for ArcGIS Server – Java**

- **Who are you?**
 - **ArcGIS Server developers**
 - **Web developers**
 - **GIS Administrators for ArcGIS Server**
 - **IT/System Architects**

Agenda

- **9.3 Security model**
 - Introduction
 - Configuration
 - Use
- **Extending & advanced configurations**
 - FileStore
 - LDAP over SSL
- **Securing your site**
 - Using reverse proxies
 - Tips & troubleshooting

A Secure ArcGIS Server Site



Introduction

- **Securing your GIS services and Web applications**
 - Java EE (provided by application servers)
 - ArcGIS managed (introduced at 9.3)
- **Java EE security**
 - UI driven through Manager
 - No more opening/editing contents of WAR file
- **ArcGIS managed**
 - UI driven through Manager
 - Role based access control
 - Works seamlessly with JavaScript /Flex clients

Terms and Concepts

- **Principal (User)**
 - Individual consuming published functionality
- **Role**
 - Group of individuals with some privilege
- **Permission**
 - Privilege to access certain resource
- **Authentication**
 - Validating credentials of the individual and establishing identity
- **Authorization**
 - Evaluating privileges of an individual based on permission

ArcGIS Managed Security - Components

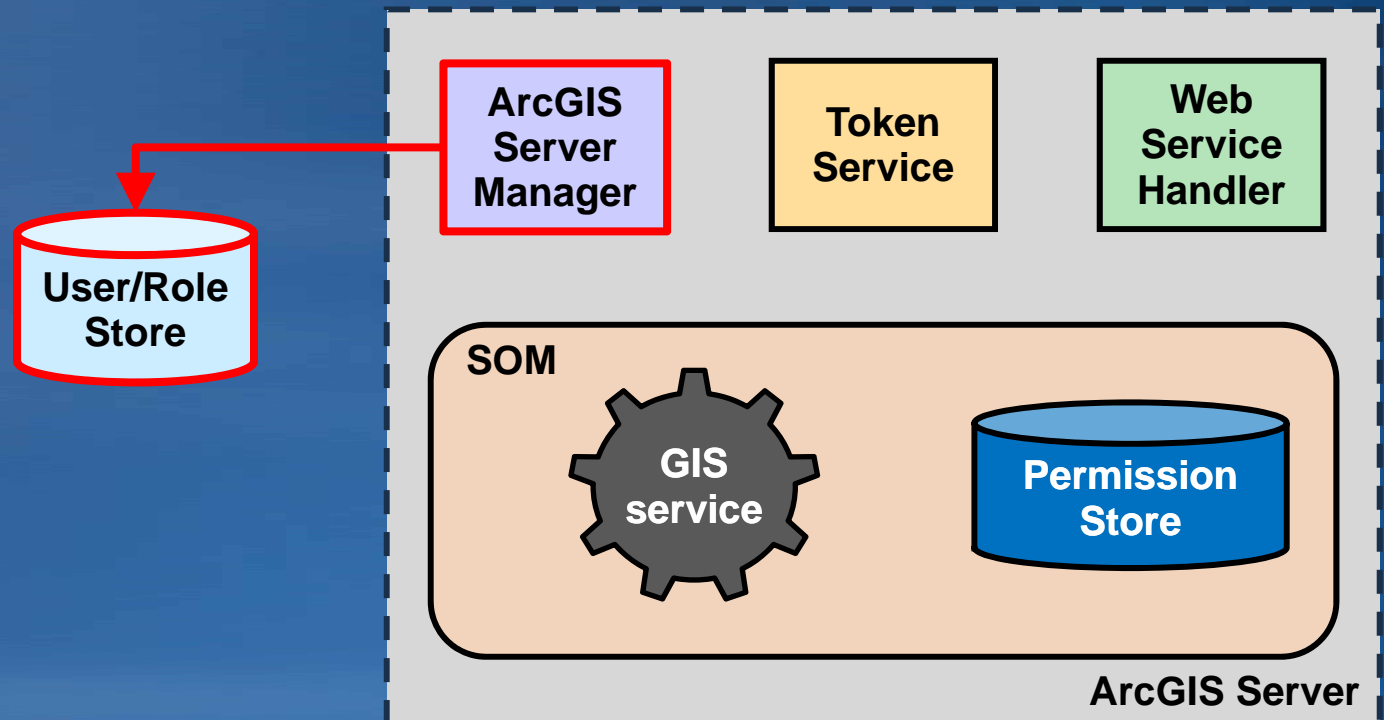
- **User and Role Store (Principal Store)**
 - Data store of user and role information (example: username, password, roles, etc)
 - APIs to access this information
- **Permission Store (engine)**
 - Data store of permissions assigned to a role
 - APIs to access this information
- **ArcGIS Token Service**
 - Web service that issues a token

ArcGIS Managed Security for GIS Services

- **Access is role based**
 - Permissions are assigned to roles
 - Authorization based on the roles a user plays
- **Requires tokens**
 - A token needs to be appended to the URL when accessing a secured GIS Service
 - Tokens are acquired from a ArcGIS Token Service by providing 'username' and 'password'
 - Desktop clients and Web Mapping Application (built using Manager) can automatically fetch tokens and use them
- **Administration through Manager**

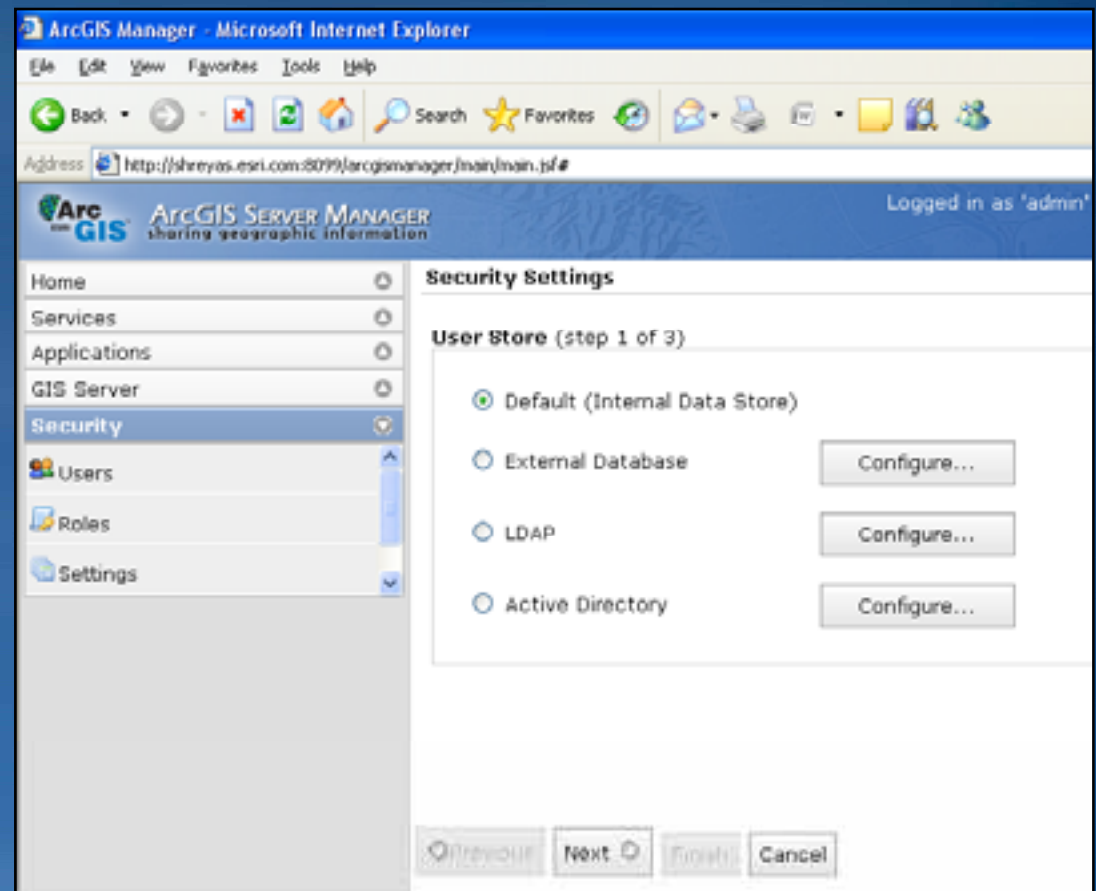
Managing User and Roles for ArcGIS Security

- Administrator can configure the storage of user and roles using ArcGIS Manager
 - Manage user and role information



Demo

- Configure store
- Manage users and roles



User and Role Store – Out of the box

		R O L E S T O R A G E			
U S E R S T O R A G E	R/W = read & write R = read only	Default Apache Derby (R/W)	External DB (R/W)	LDAP (R)	MS-Active Directory (R)
	Default Apache Derby (R/W)	Allowed	X	X	X
	External DB (R/W)	X	Allowed	X	X
	LDAP (R)	Allowed	Allowed	Allowed	X
	MS-Active Directory (R)	Allowed	Allowed	X	Allowed

Also see the section: Extending and Customization

ArcGIS Token Service

- **A Web service that grants tokens (part of ArcGIS Managed security)**
 - Authenticates the user requesting a token
- **Connected to the user store**
 - Configured through Manager
- **Should be deployed on a SSL port**
- **gettoken.html page – UI for fetching tokens for JavaScript/Flex developers**

ArcGIS Managed Security for GIS Services – Internals

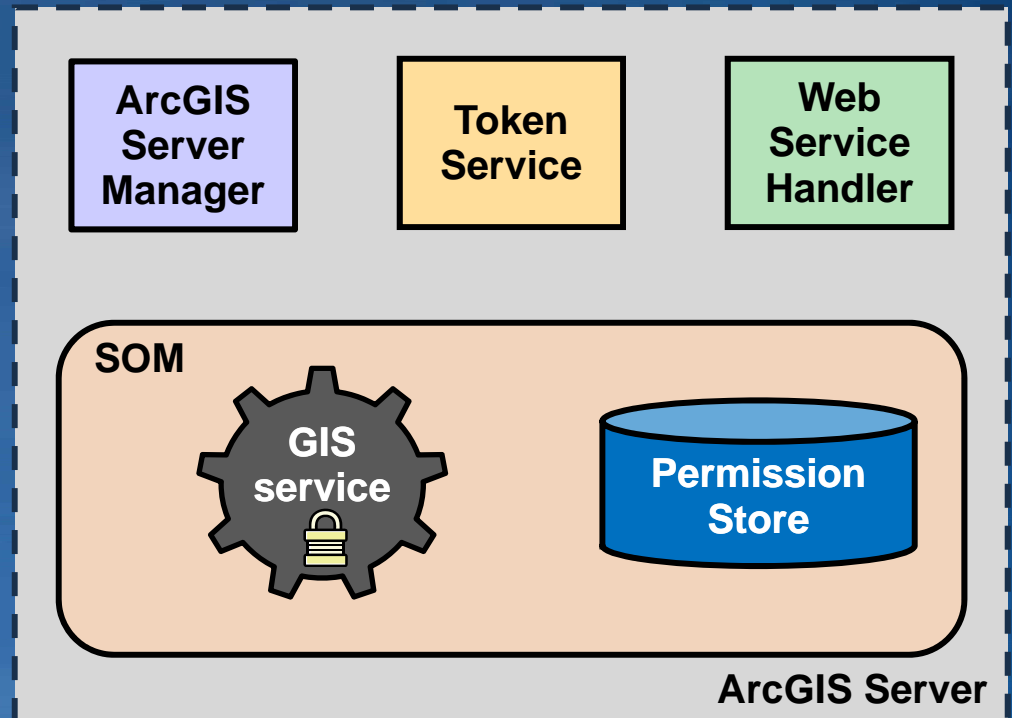
- Web applications want to consume a secured GIS service



Web Application

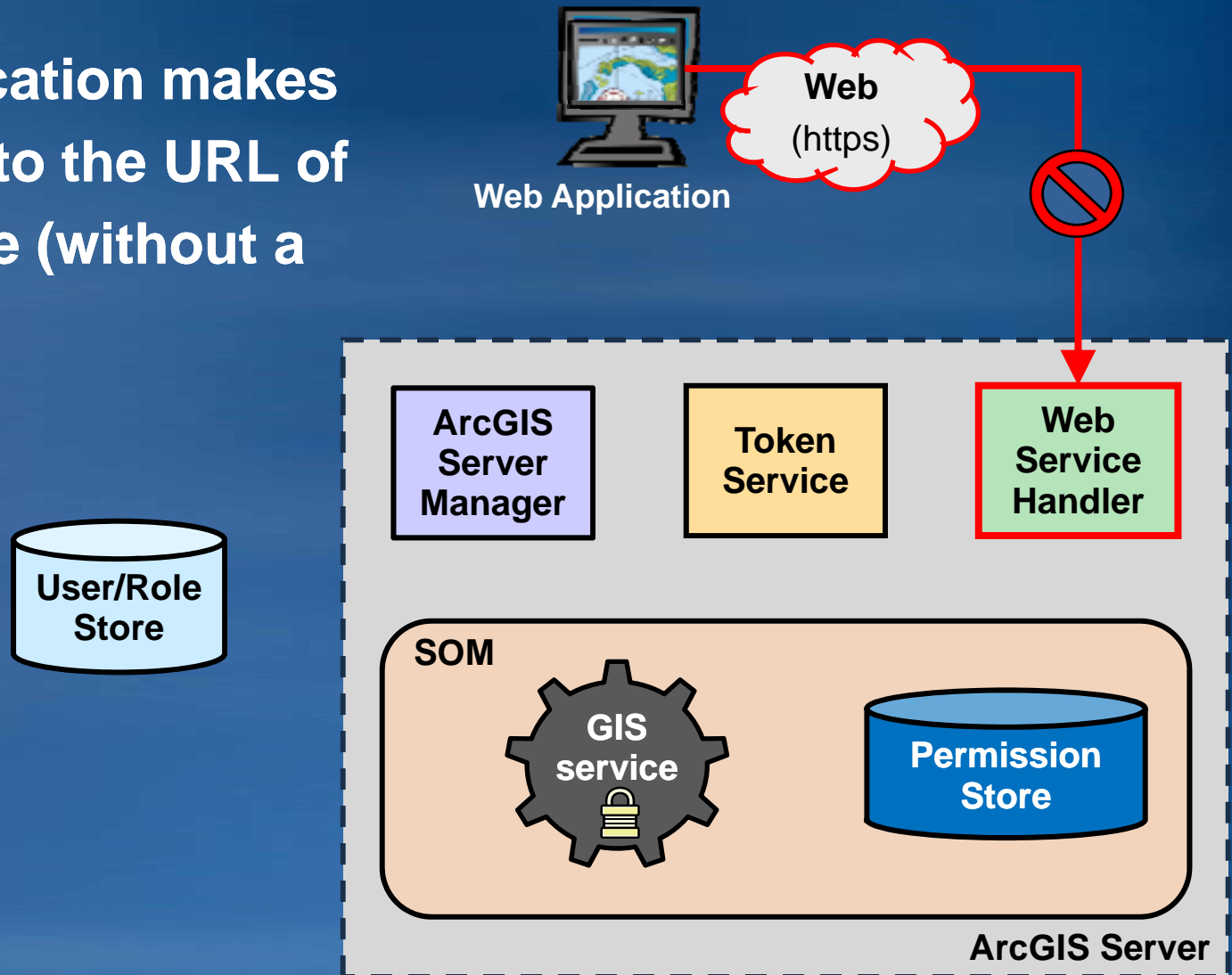


User/Role Store



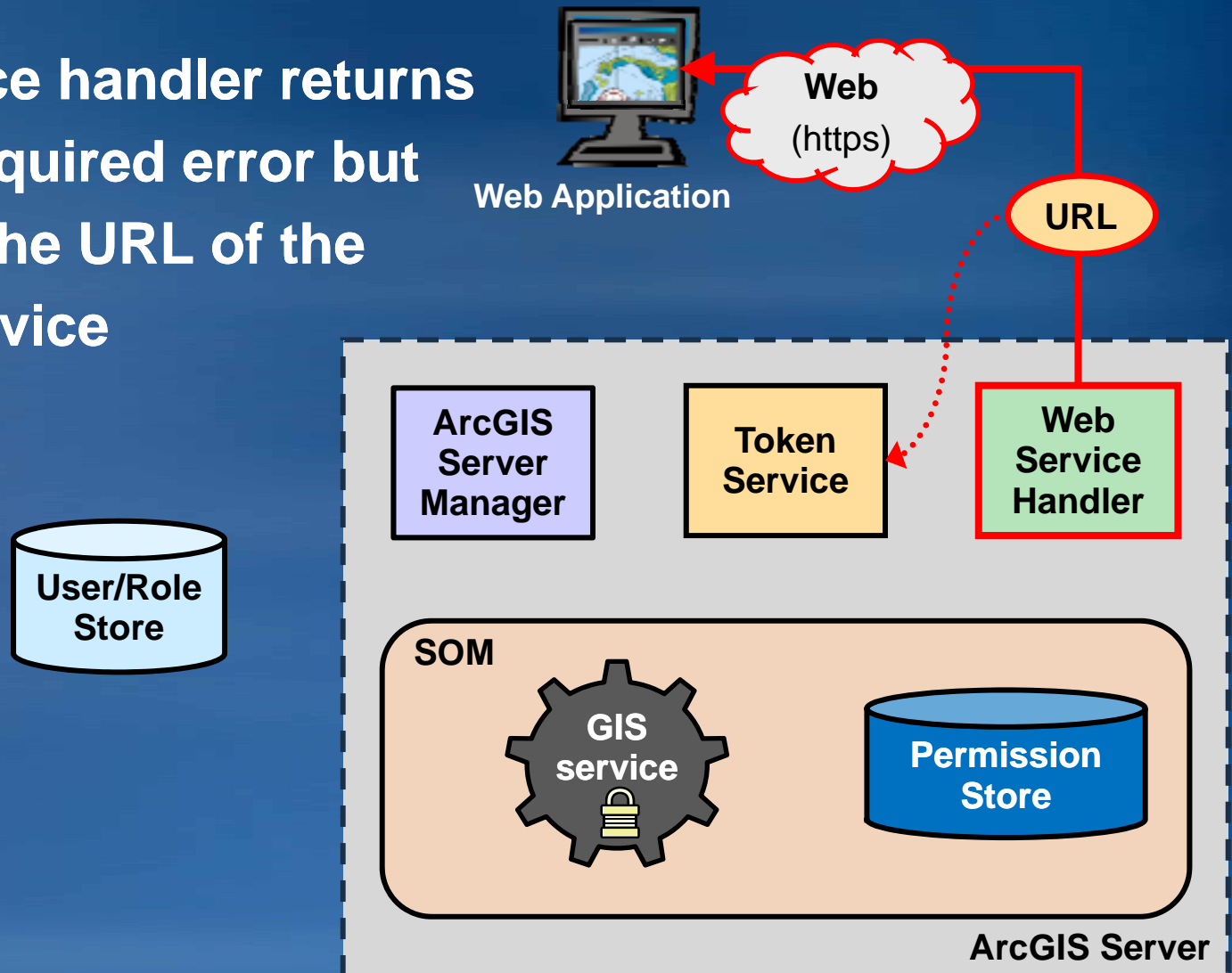
ArcGIS Managed Security for GIS Services – Internals

- Web application makes a request to the URL of the service (without a token)



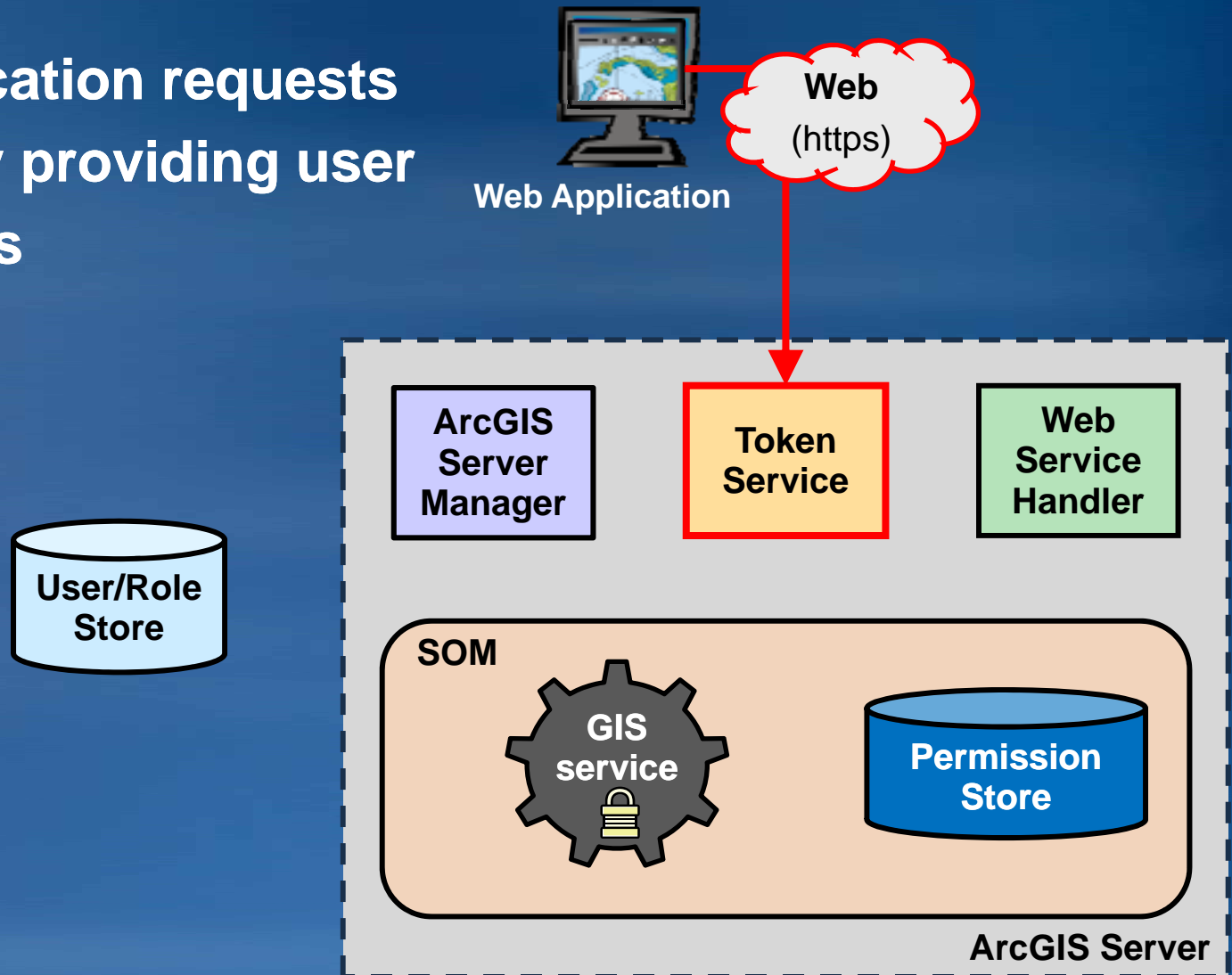
ArcGIS Managed Security for GIS Services – Internals

- Web service handler returns a token required error but provides the URL of the Token Service



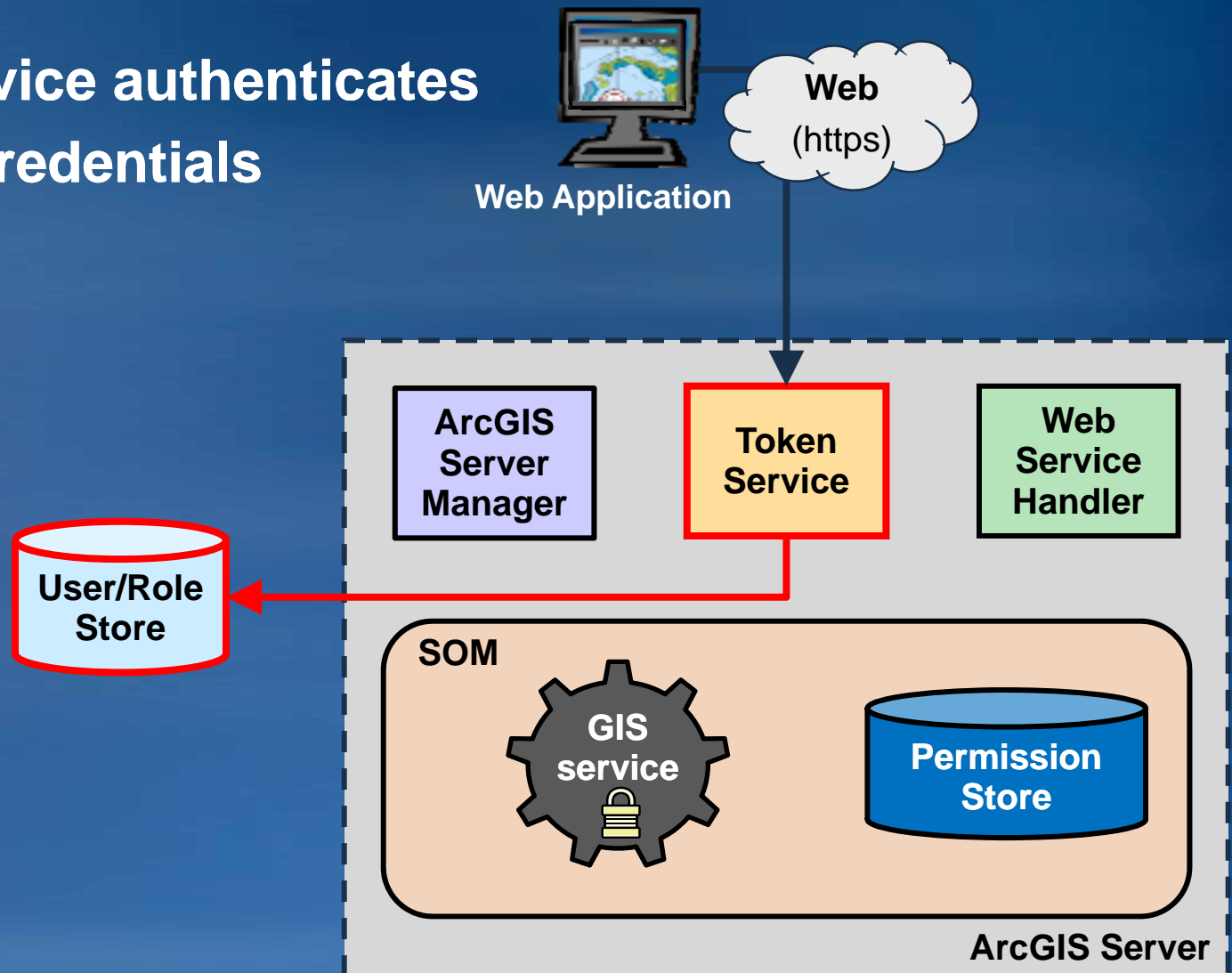
ArcGIS Managed Security for GIS Services – Internals

- Web application requests a token by providing user credentials



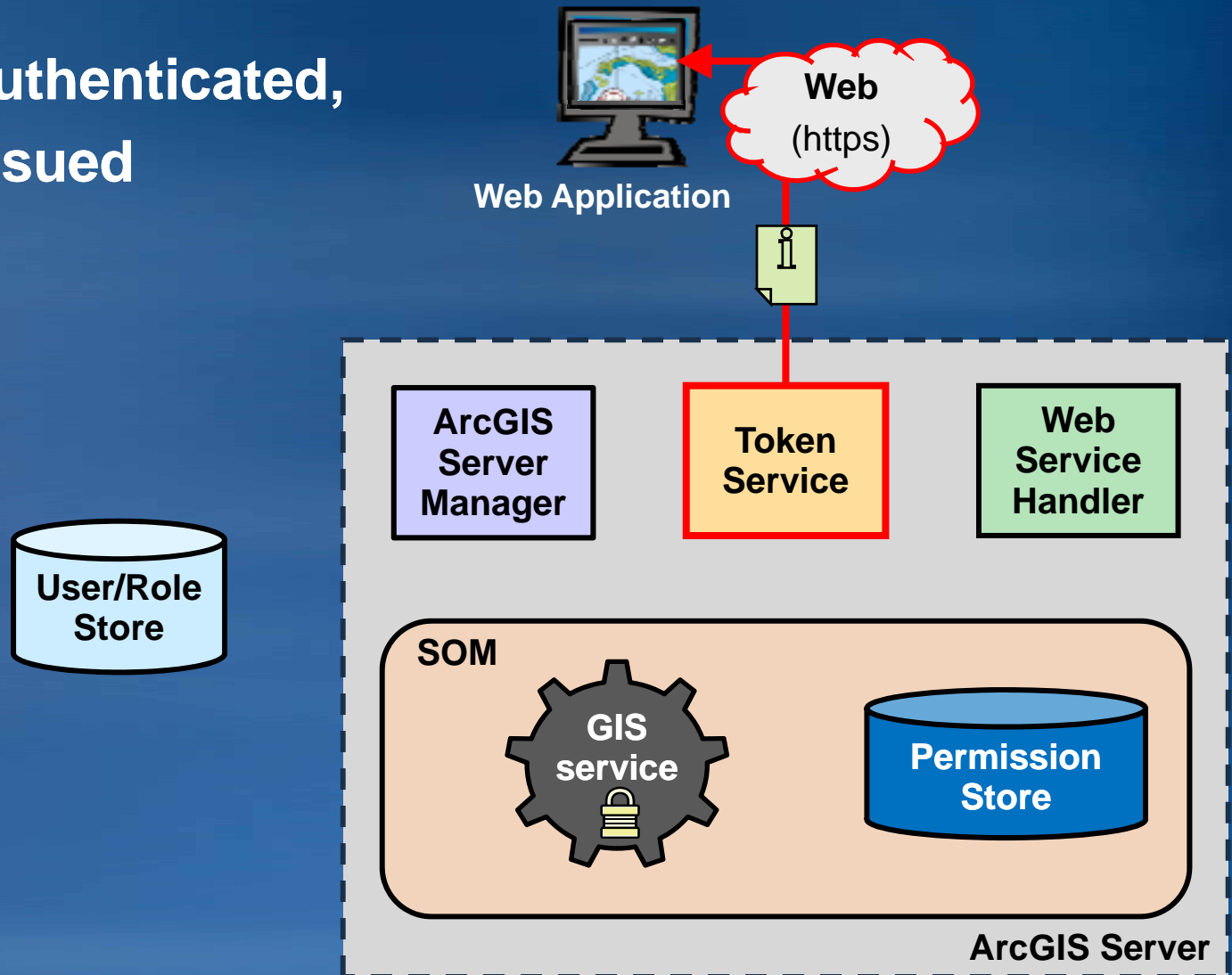
ArcGIS Managed Security for GIS Services – Internals

- **Token Service authenticates the user credentials**



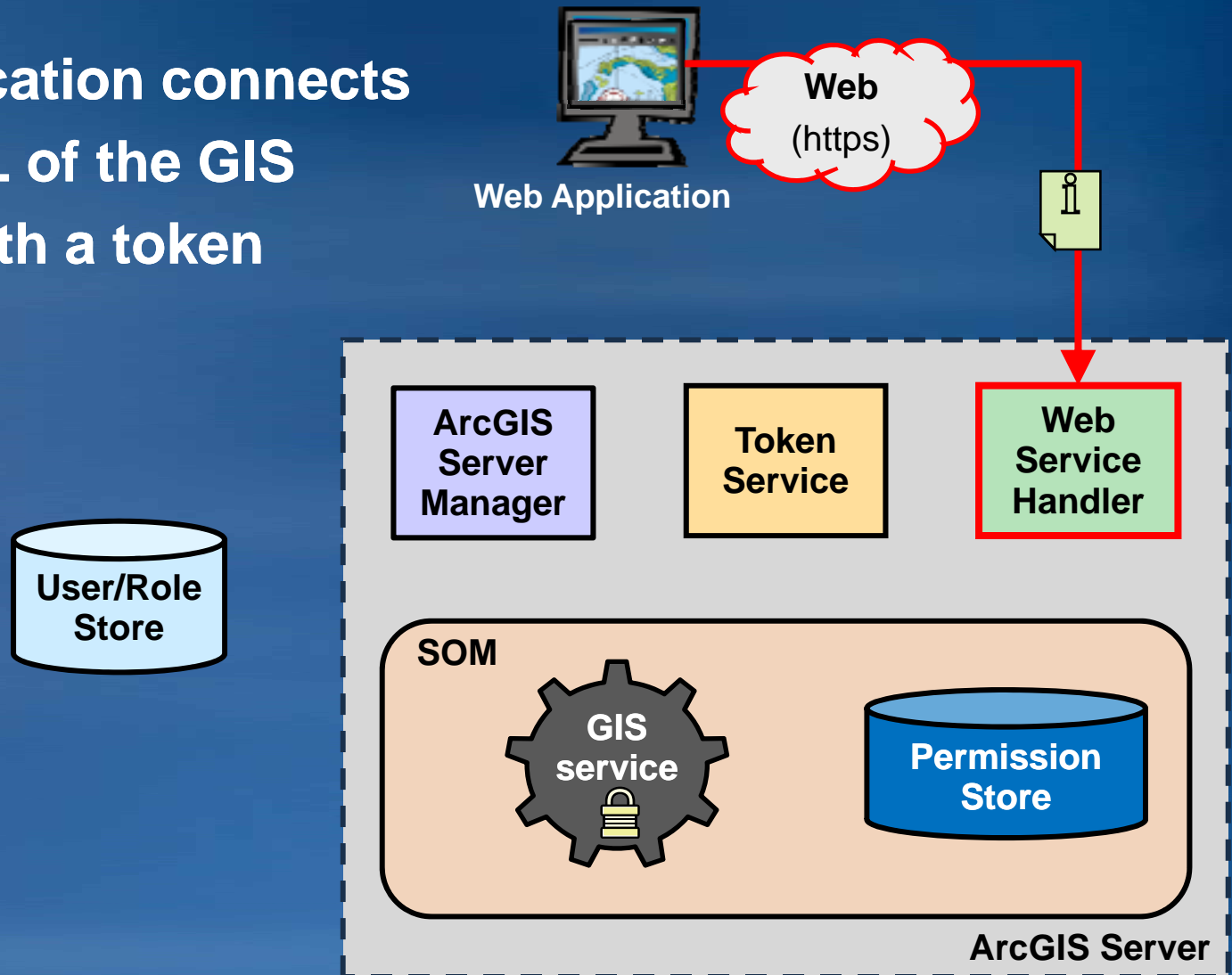
ArcGIS Managed Security for GIS Services – Internals

- If user is authenticated, token is issued



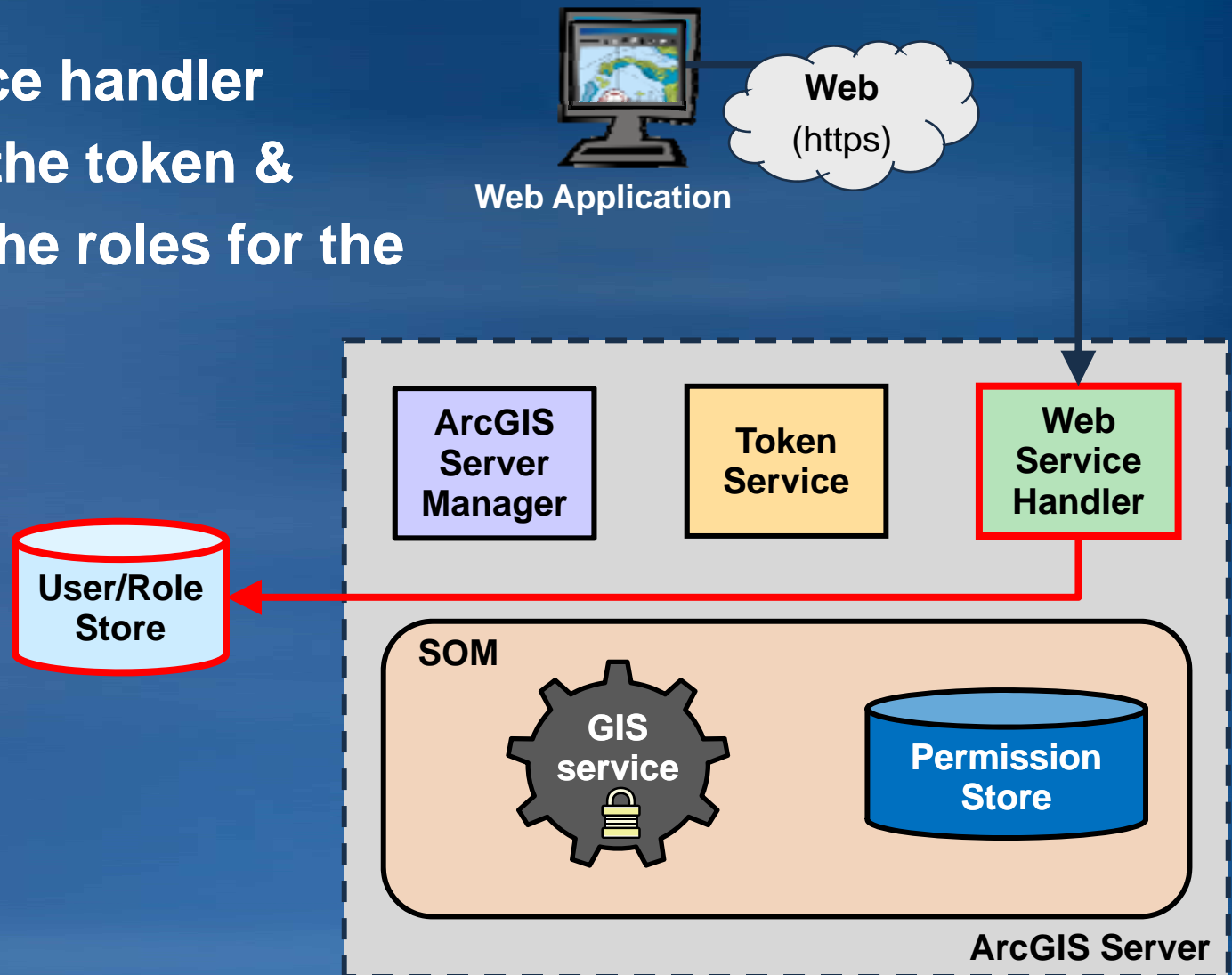
ArcGIS Managed Security for GIS Services – Internals

- Web application connects to the URL of the GIS service with a token



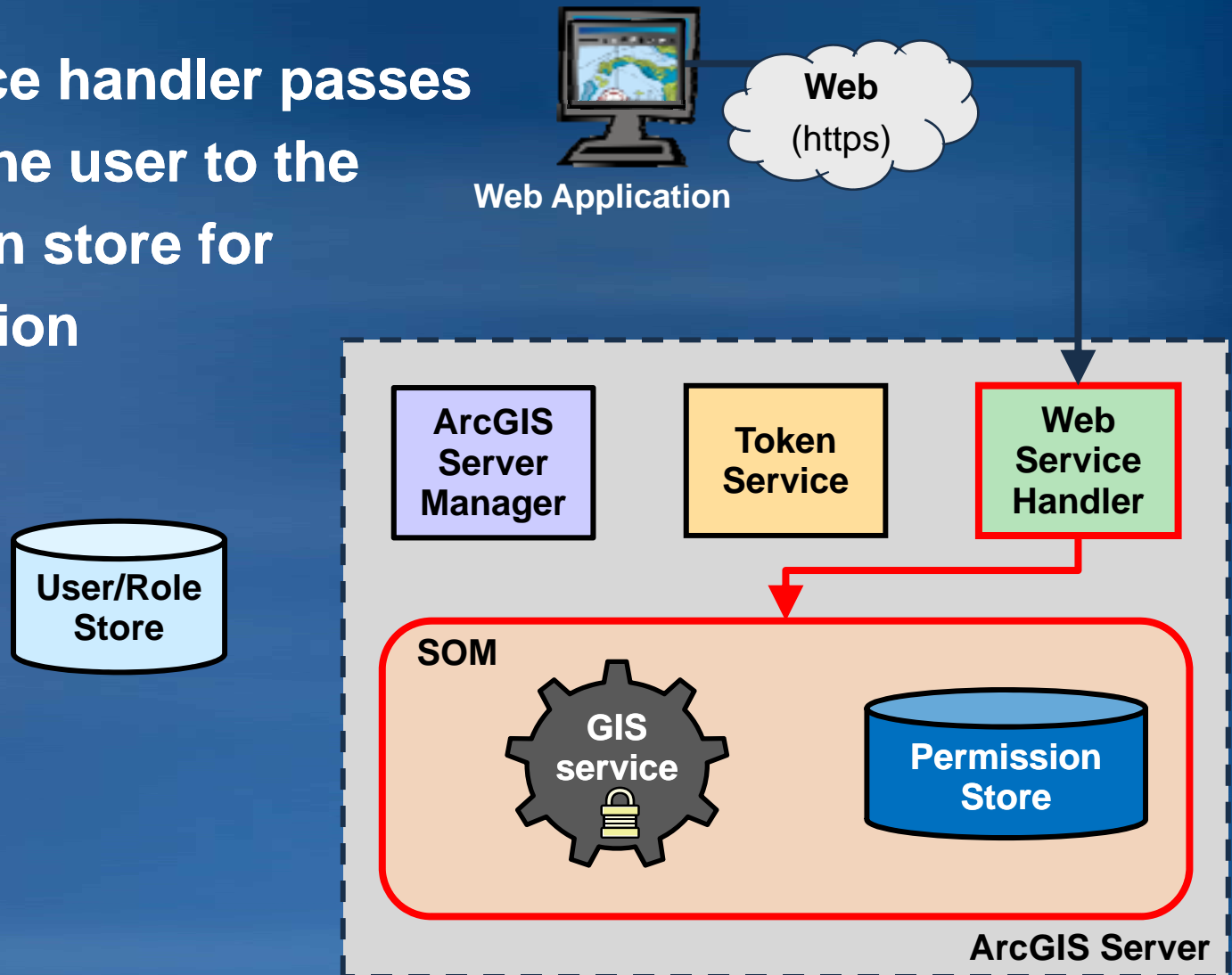
ArcGIS Managed Security for GIS Services – Internals

- Web service handler validates the token & looks up the roles for the user



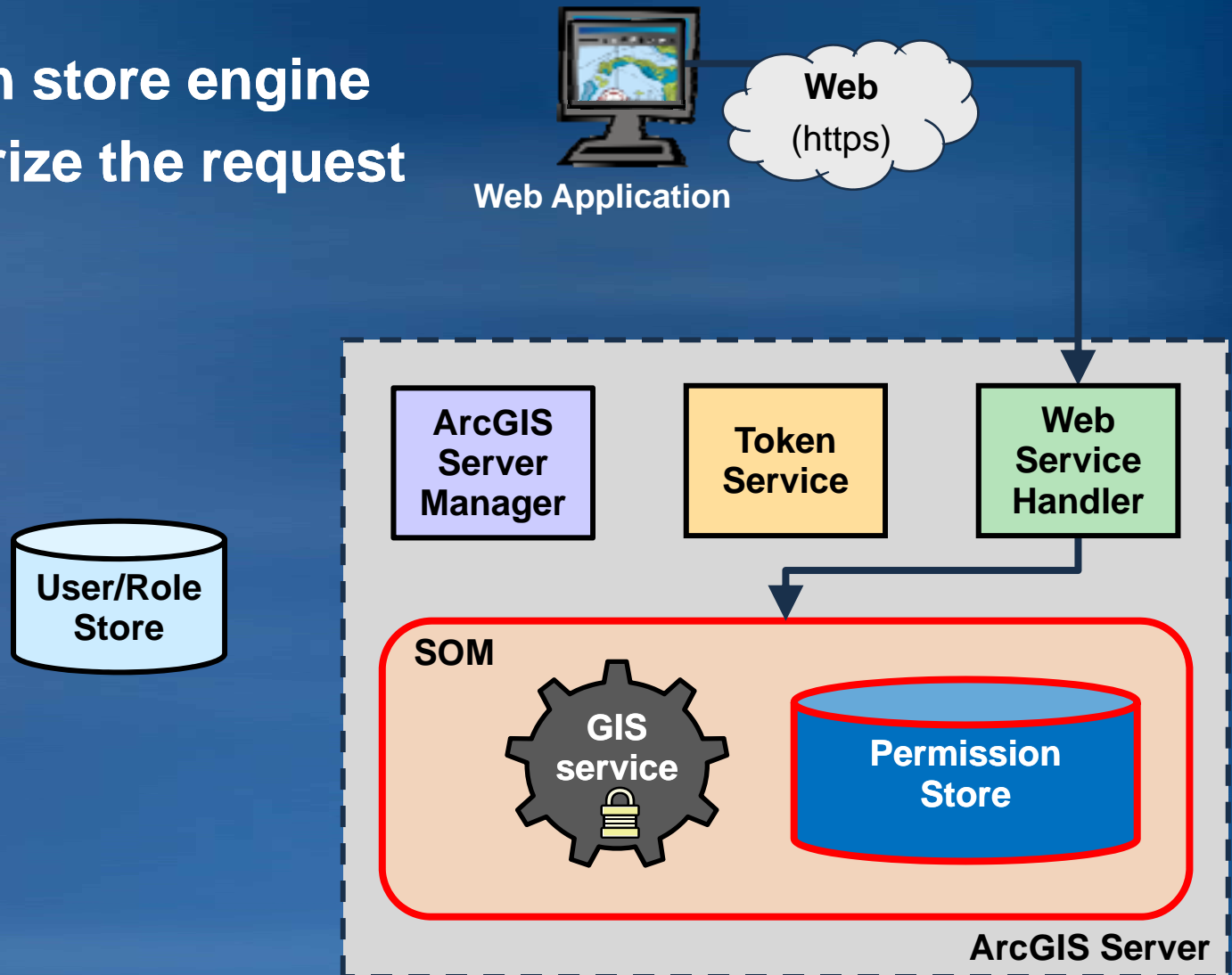
ArcGIS Managed Security for GIS Services – Internals

- Web service handler passes roles for the user to the permission store for authorization



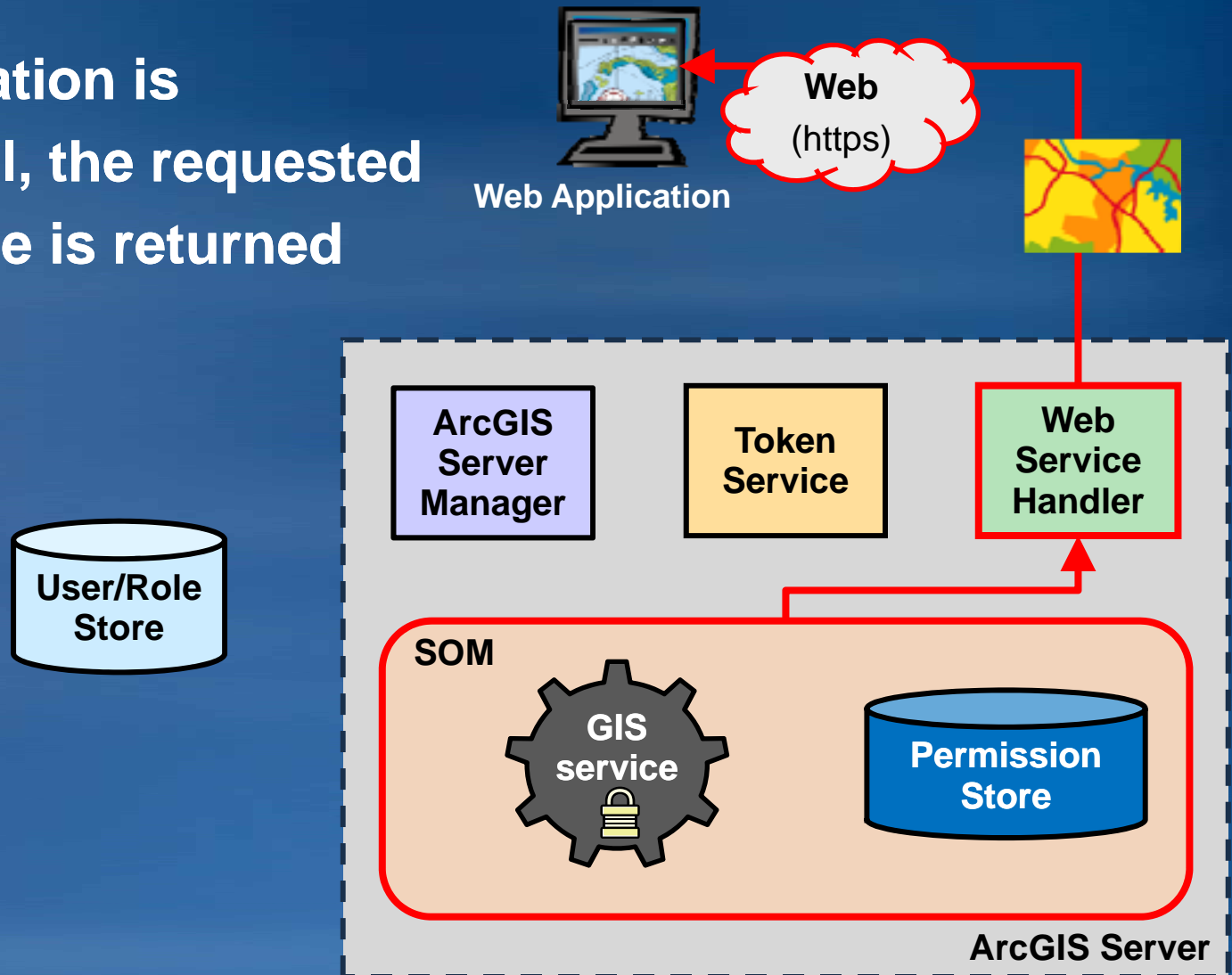
ArcGIS Managed Security for GIS Services – Internals

- Permission store engine will authorize the request



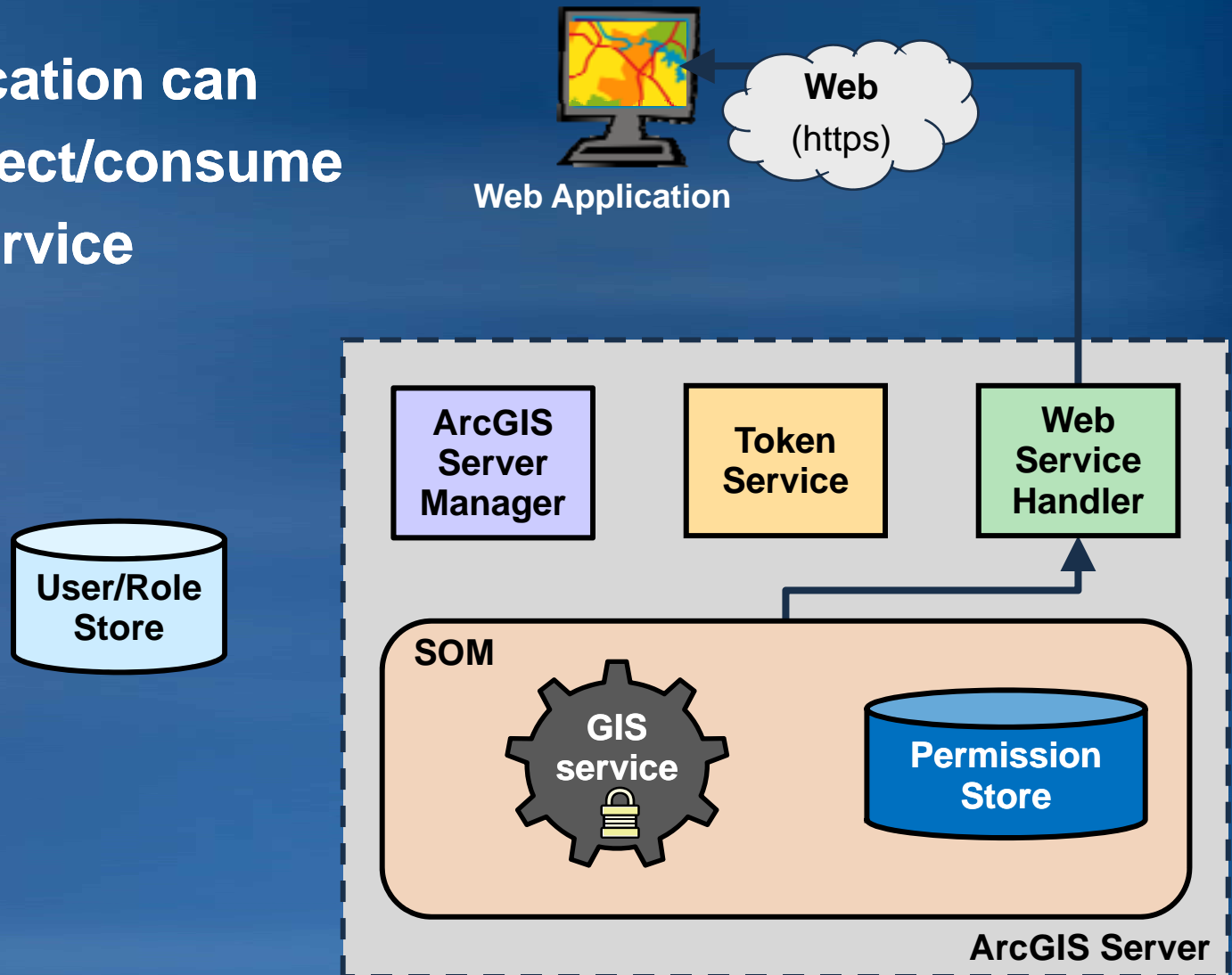
ArcGIS Managed Security for GIS Services – Internals

- If authorization is successful, the requested GIS service is returned



ArcGIS Managed Security for GIS Services – Internals

- Web application can then connect/consume the GIS service



Demo

- Assigning permissions

The screenshot displays the ArcGIS Server Manager web interface in Mozilla Firefox. The browser address bar shows the URL <http://stefanle-009@arcgismanager.hs-niederrhein.de/>. The page is titled "ArcGIS Server Manager" and shows the user is logged in as "stefanle" on Monday, July 21, 2008, at 3:47:44 PM. The interface includes a navigation menu on the left with options like "Home", "Services", "Manage Services", "Publish GIS Resource", "Add New Service", "Configure Services Handler", "Applications", "GIS Server", and "Security". The main content area is titled "Manage Services" and shows a table of services. A "Permissions" dialog box is open, displaying the available roles and the role assigned to the service "gulf_of_st_lawrence".

Name	Type	Status	Instances (In Use/Running)	URL	Security
gulf	Map Service	Stopped	0/2		
gulf_of_st_lawrence	Map Service	Stopped	0/2		
usa	Map Service	Stopped	0/2		

Permissions
You are editing permissions for service 'gulf_of_st_lawrence'

Available Roles: Architect, Surveyor, Everyone, Authenticated, Anonymous

Allowed Roles: Engineer

Buttons: Save, Cancel

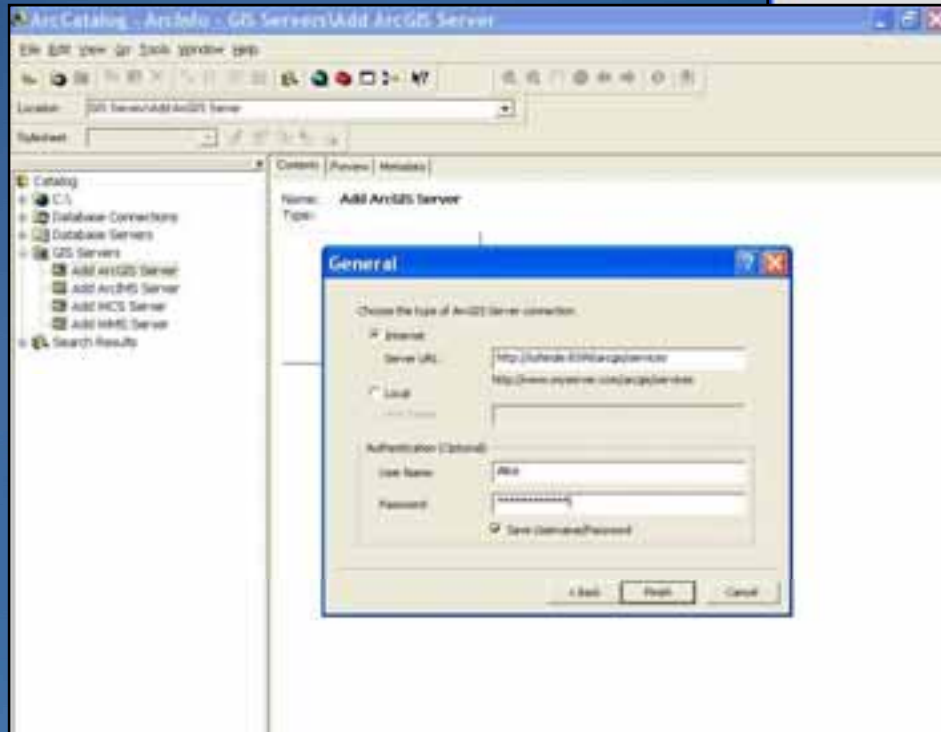
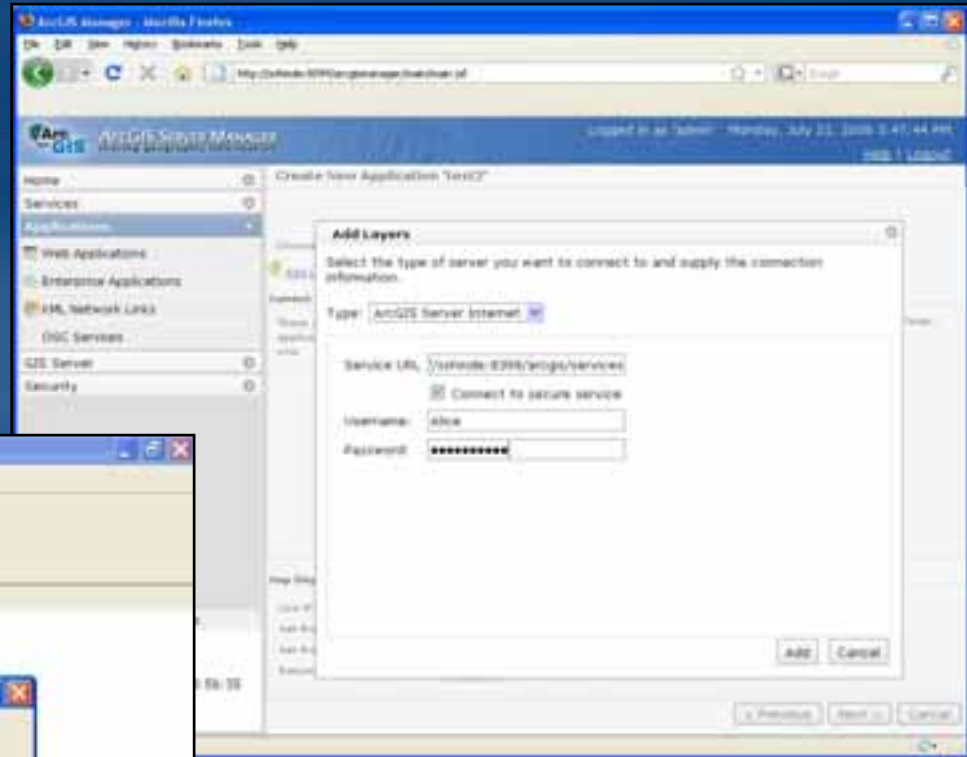
GIS Server Status
Name: SSHNDCE
Status: Online
Started: Jul 8, 2008 - 09:56:35 AM
Message: vlm_302

Demo

- Consuming secured services

through Web application

through ArcCatalog



JavaScript Applications Consuming Secured Services

- JavaScript embeds a token instead of user credentials
- Simple workflow for the developer
 - Build your application
 - Fetch a token from ArcGIS Token Service
 - Append the token to the URL

```
var map = new esri.Map("mymap");  
var layer = new  
    esri.layers.ArcGISDynamicMapServiceLayer("http://machine:83  
    99/arcgis/rest/services/usa/MapServer?token=ksdfsfsirteueim  
    lskdmcwkck");  
map.addLayer(layer);
```

Demo

- JavaScript application consuming a secured service

ArcGIS Token Service - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:8090/arcgis/tokens/gettoken.html

ArcGIS ArcGIS TOKEN SERVICE

This utility generates tokens that grant access to secured GIS services. A token is an encrypted string containing the user name, expiration time and an identifier. Client applications include the token with any requests sent to the GIS server and the server grants access to the appropriate GIS service.

User Name: Alice

Password: *****

Identifier: Web Application URL or HTTP Referrer

IP Address

192.52.40.1

Expires in: 4 minute(s)

(maximum expiration time can be 10 day(s))

Copy the following token into your application:

ctpyBnD0o1eSC7KHE7zYA0IVRbeJymnPiA1V7EDD-lmZE8GLMKgoaVusK YCW_B6

Done

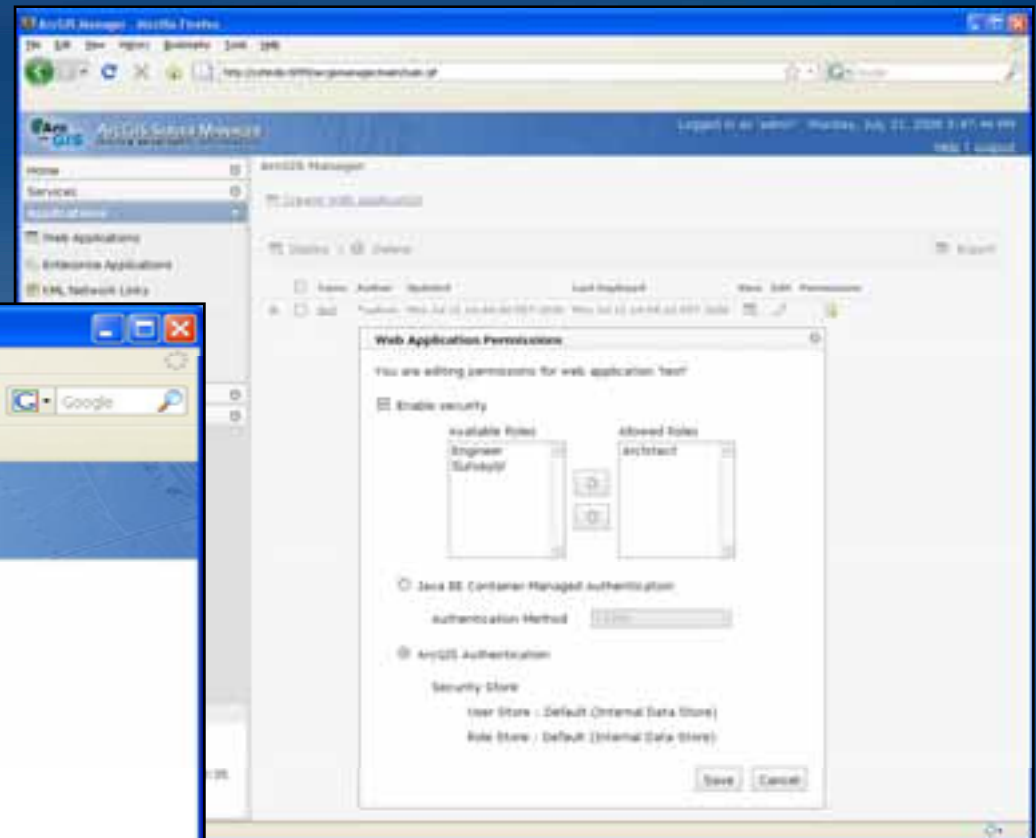
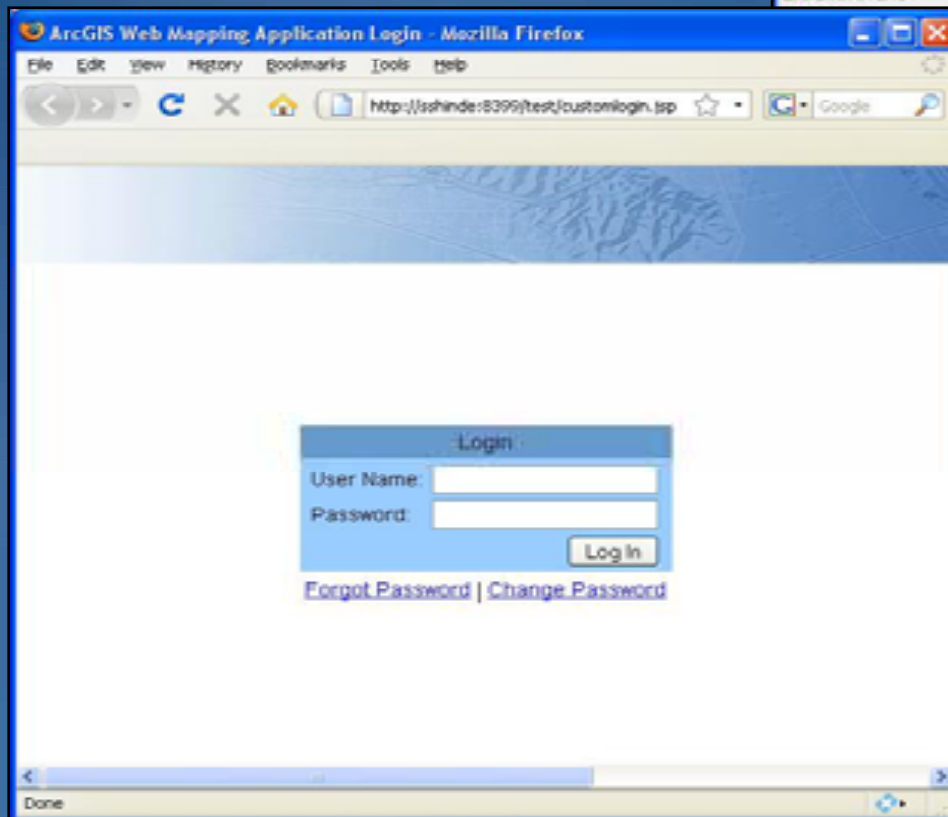
ArcGIS Managed Security for Web Applications

- **Application can be secured using ArcGIS Manager**
 - Web application creator set the permissions
 - User and role store can be configured using ArcGIS Manager
- **Web application is secured using login control**
 - The login web page can be customized

Demo

Securing the web application

Secure web application login



Extending and Customization

- **Out of the box support for:**
 - Relational Databases
 - LDAP
 - Active Directory
- **You can write custom membership providers if:**
 - None of the above schemes meet your storage needs
 - Have data in a proprietary format
 - Want to authenticate using other tools
- **You need to implement the *SecurityStore* Java interface provided by ArcGIS**

Demo

- **FileStore – user/role storage in an XML file**

User and Role Store – Advanced Configuration

- **Connecting to LDAP over SSL (ldaps)**

- **Server side**

- Enable ldaps (usually port 636) on the LDAP server
 - Generate the public & private keys
 - Get the public key signed by a CA
 - Import the signed certificate into the keystore

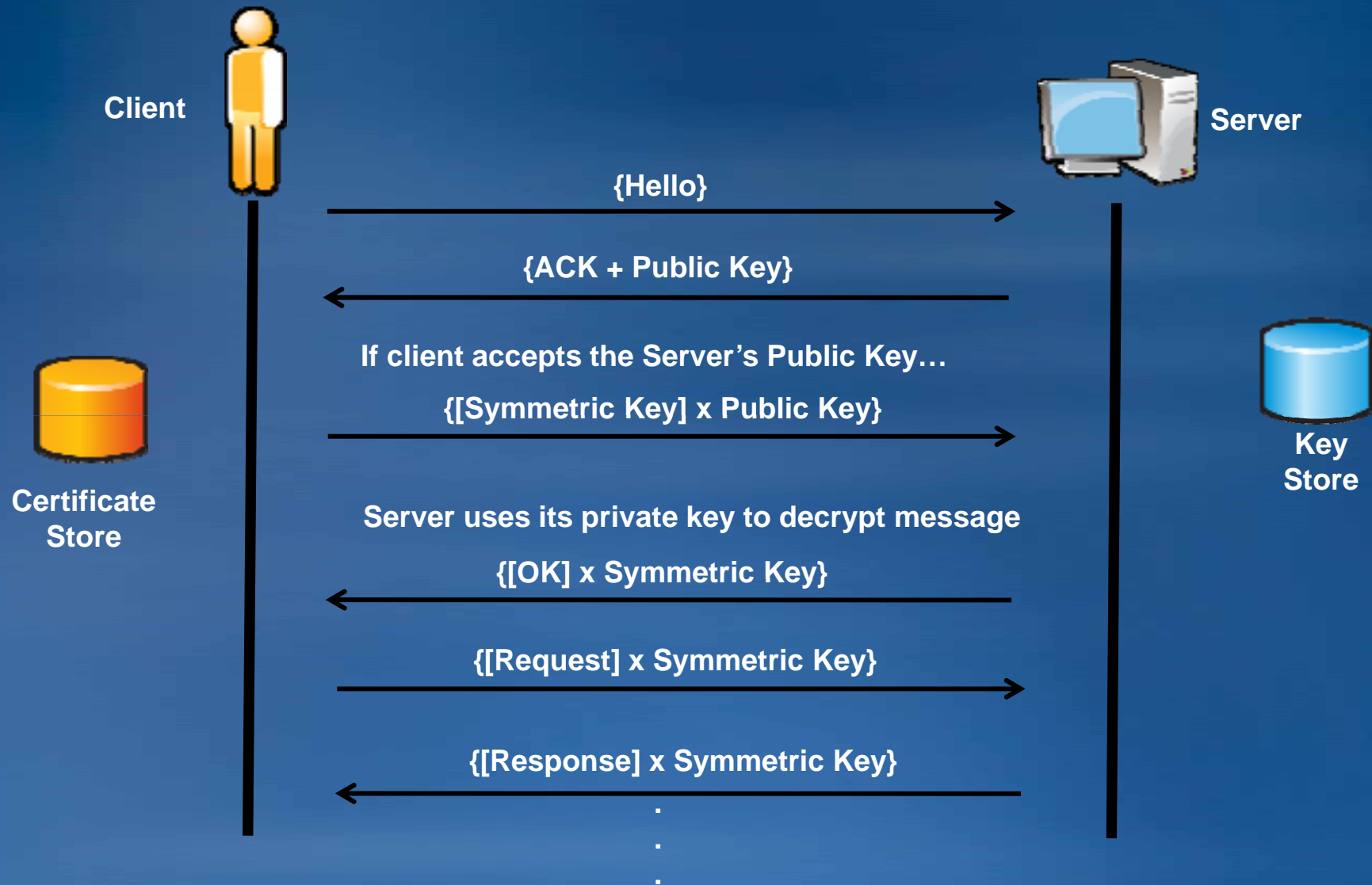
- **Client side**

- If certificates are self signed – import self-signed certificate of the Server into the JRE's certificate store
 - Restart ArcGIS components (Manager Service, Service Handlers etc)

SSL Basics

- **Server proves its identity, data transfer is encrypted**
- **Uses asymmetric key cryptography for handshaking**
 - Public and private keys
 - CA signs the public keys, public keys are shared with clients
 - Encrypting data with the public key and then decrypting it is usually an expensive operation (hence the use of fast symmetric keys)
- **Uses symmetric key to encrypt the contents sent over the wire for the duration of the session**
 - More efficient way of encrypting instead of using public/private keys

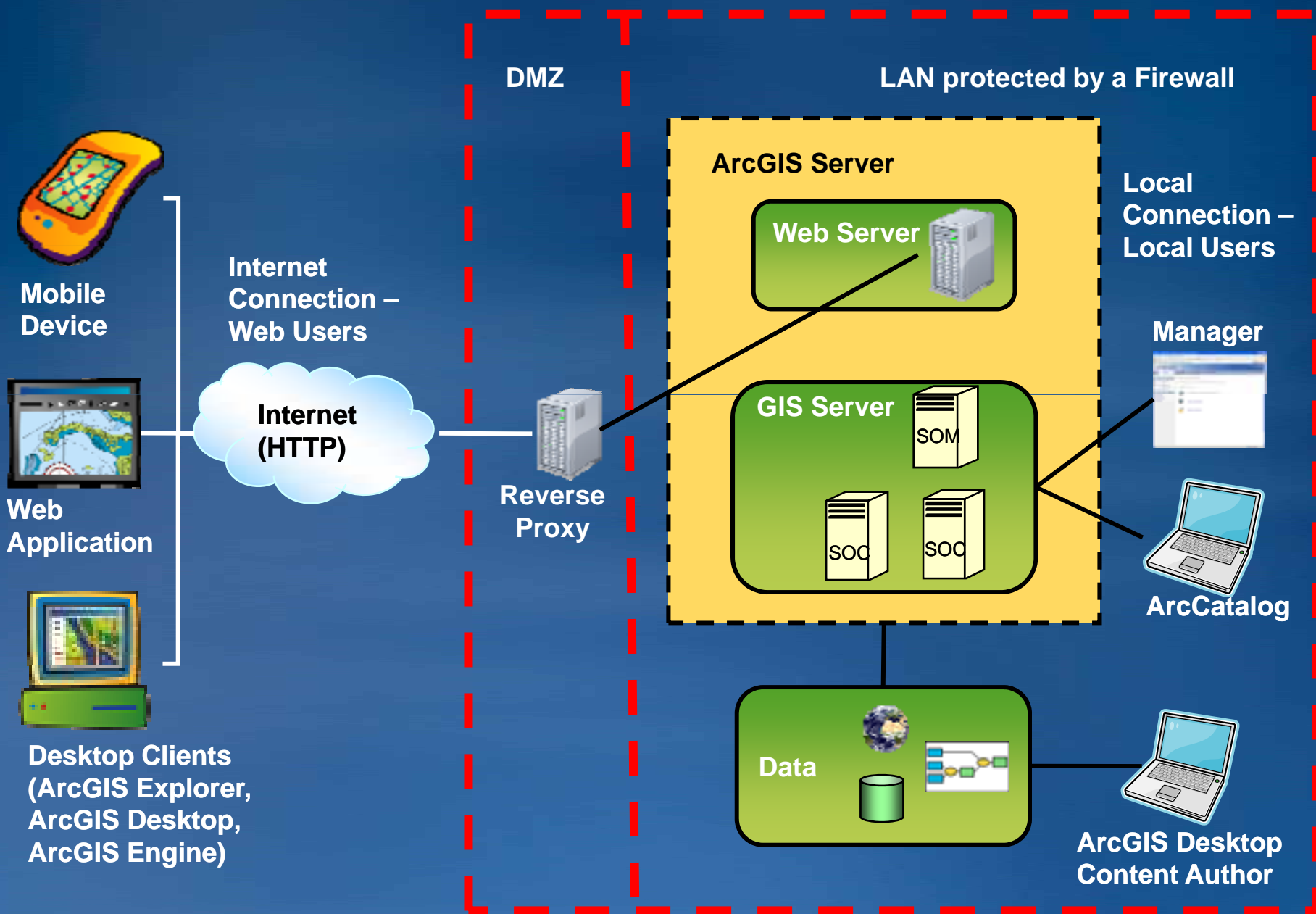
SSL Basics – The handshake



Demo

- **Connecting to LDAP over SSL**
 - ApacheDS 1.5.1
 - keytool – Java tool to manage cryptographic keys and certificates
 - ArcGIS Manager
- **Troubleshooting tip**
 - Use this JVM argument: `-Djavax.net.debug=ssl`

A Secure ArcGIS Server Site



Securing Your Site

- **Host application servers within the firewall protected LAN**
- **Use a reverse proxy server to expose functionality to the Internet**
 - **Hides app server**
 - **Client is not aware of the internal server specifics**
 - **Can do SSL instead of app server**
 - **No SSL between reverse proxy and app server**
 - **Load balancing**
 - **Can toggle requests between multiple app servers**
 - **Caching, etc.**

Demo

- **Setting up a reverse proxy server using Apache Web Server**

Reverse Proxy with Apache

- Download the Apache Web server from <http://httpd.apache.org>
- Following modules are required:
 - mod_proxy
 - mod_proxy_http
 - mod_headers
 - mod_deflate
 - mod_proxy_html (available at <http://apache.webthing.com>)
 - ...

KB: <http://support.esri.com/index.cfm?fa=knowledgebase.techarticles.articleShow&d=35948>

Reverse Proxy with Apache – Cont'd

- **Make builds**

```
./configure --enable-so --enable-mods-shared="proxy proxy_http  
proxy_connect headers deflate" --prefix=/usr/local/apache2
```

```
$make
```

```
$make install
```

```
$apxs -c -I/usr/include/libxml2 -i mod_proxy_html.c
```

- **Load the modules into Apache – httpd.conf**

```
LoadModule proxy_module modules/mod_proxy.so
```

```
LoadModule proxy_http modules/mod_proxy_http.so
```

```
LoadFile /usr/lib/libxml2.so
```

```
LoadModule proxy_html_module modules/mod_proxy_html.so
```

```
...
```

Reverse Proxy with Apache – Cont'd

- **ProxyPass & ProxyPassReverse directives – httpd.conf**

ProxyPass /arcgis/services http://internal:8399/arcgis/services

ProxyPassReverse /arcgis/services <http://internal:8399/arcgis/services>

ProxyPass /arcgis/rest http://internal:8399/arcgis/services

ProxyPassReverse /arcgis/rest <http://internal:8399/arcgis/services>

ProxyPass /arcgis/tokens http://internal:8399/arcgis/services

ProxyPassReverse /arcgis/tokens <http://internal:8399/arcgis/services>

- **References with an HTML page returned by the server will be re-written by the mod_html module**
 - Unfortunately, it does not re-write XML/WSDLs

Tips & Troubleshooting

- **User/Role store**

- LDAP, Active Directory are treated as read-only stores. Cannot use ArcGIS Manager to edit information in them
- When connecting to a database, add the JDBC driver (JAR file) into `/arcgis/java/manager/config/security/lib` directory

- **Token Service**

- Should run on an SSL port (install certificates in components that need to communicate with the service)
- Windows Vista has IPv6 enabled by default – use the correct IP version when requesting tokens (IPv4 vs IPv6)
- Set the token expiration time to something appropriate – balance between security & performance
- Store the shared key securely

Tips & Troubleshooting

- **Consuming secured GIS services**
 - ArcGIS Manager & Desktop will warn when the token service is not running on SSL port
 - Only tokens issued by ArcGIS Token Service are considered to be valid tokens – cannot use tokens from other entities
- **When using a reverse proxy**
 - JavaScript /Flex developers should not use the IP address mechanism to lock their tokens (the client IP is not visible to the server) – use HTTP referrer/URL method
 - WSDL exposed by a service has reference to the internal server's URL – need to use an XML re-writer in the reverse proxy, ability will be provided at post 9.3.1

Tips & Troubleshooting – Cont'd

- **Enabling/Disabling security for GIS Services**
 - Services will be “locked down” by default when security is enabled – access based on permissions
 - Disabling security is multiple steps – read documentation

Q&A

- **Tech Talk Area: Mesquite A**

Conclusion

- **Secure your GIS services and Web applications using ArcGIS managed or JavaEE security**
- **Seamlessly consume secured services in JavaScript/Flex application using tokens**
- **Think about all the aspects of security for your site. Don't make it an afterthought**

Resources

- **9.3 Security Model Documentation**

 - http://webhelp.esri.com/arcgisserver/9.3/java/security_concepts.htm

 - http://resources.esri.com/help/9.3/arcgisserver/apis/flex/help/index.html#whats_new.htm – Flex API

- **Setting up SSL for ApacheDS**

 - <http://directory.apache.org/apacheds/1.5/33-how-to-enable-ssl.html>

- **Sun's 'keytool' – tool to manage keys and certificates**

 - <http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html>

- **Reverse proxy using Apache**

 - <http://www.apachetutor.org/admin/reverseproxies>

Want to Learn More?

ESRI Training and Education Resources

- **Instructor-Led Training**

 - [Developing Applications with ArcGIS Server Using the Java Platform](#)

- **Free Web Training Seminars**

 - [Building Applications with ArcGIS Server Using the Java Platform](#)

 - [Implementing Security for ArcGIS Server 9.3 Java Solutions](#)

<http://www.esri.com/training>