

2011 Esri Developer Summit

Palm Springs, CA

Building Secure Applications with ArcGIS Server

Tom Brenneman

Gregory Ponto



Schedule

- Security overview
- Setup and configuration
- **Securing GIS Web services**
- **Using the token service**
 - Using a proxy page
- **Securing Web applications**
- **Security pass through**

Please!
Turn **OFF** cell phones
and paging devices



Please complete the session survey!

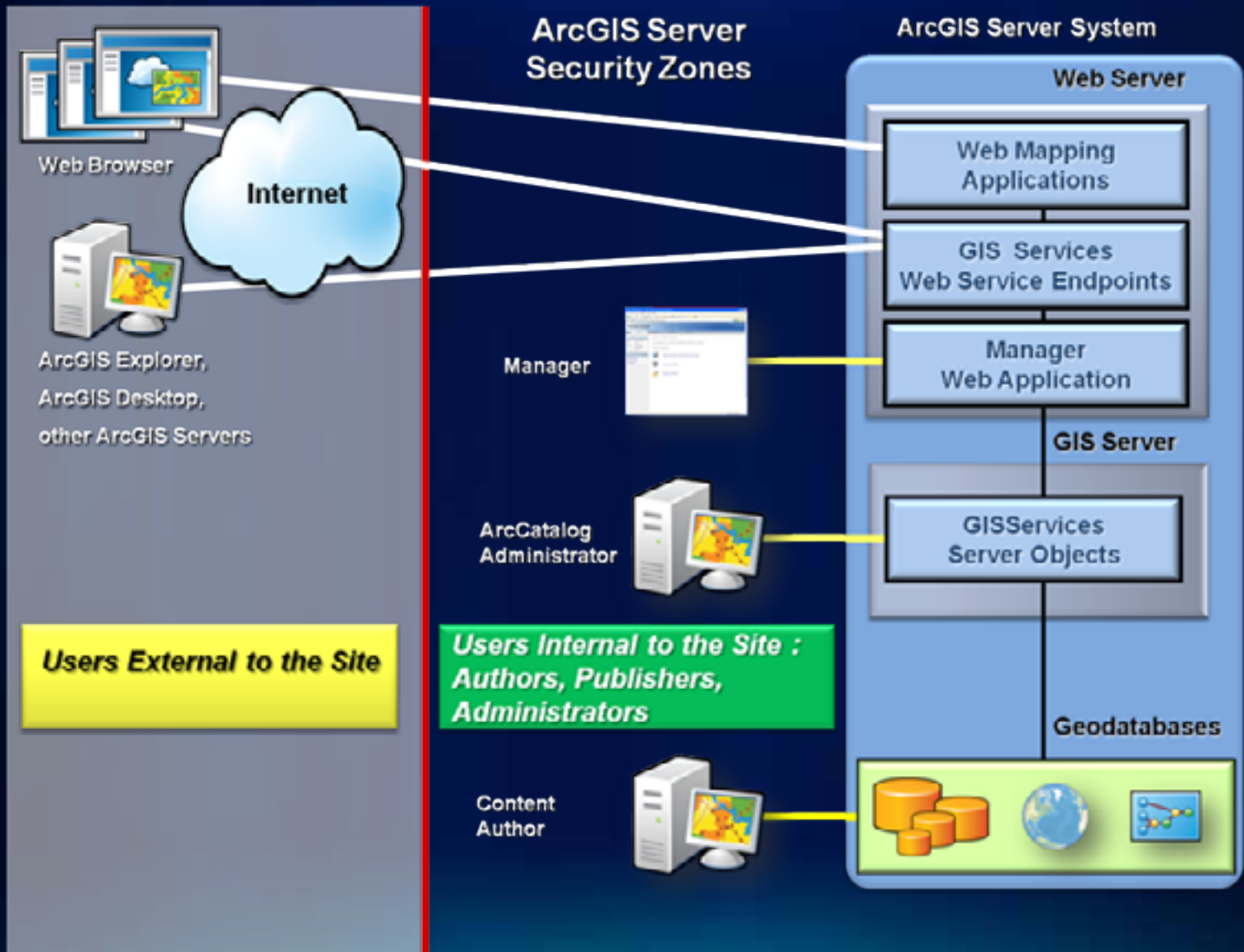
- We will answer questions at the end on the session

Security Overview

- **ArcGIS Server security provides access control**
 - Which users can access particular services and applications

- **Remember other security tasks**
 - Security during transmission
 - Operating system – updates, virus protection
 - Code – SQL injection, cross-site scripting, etc.
 - Physical security
 - User education – phishing, etc.





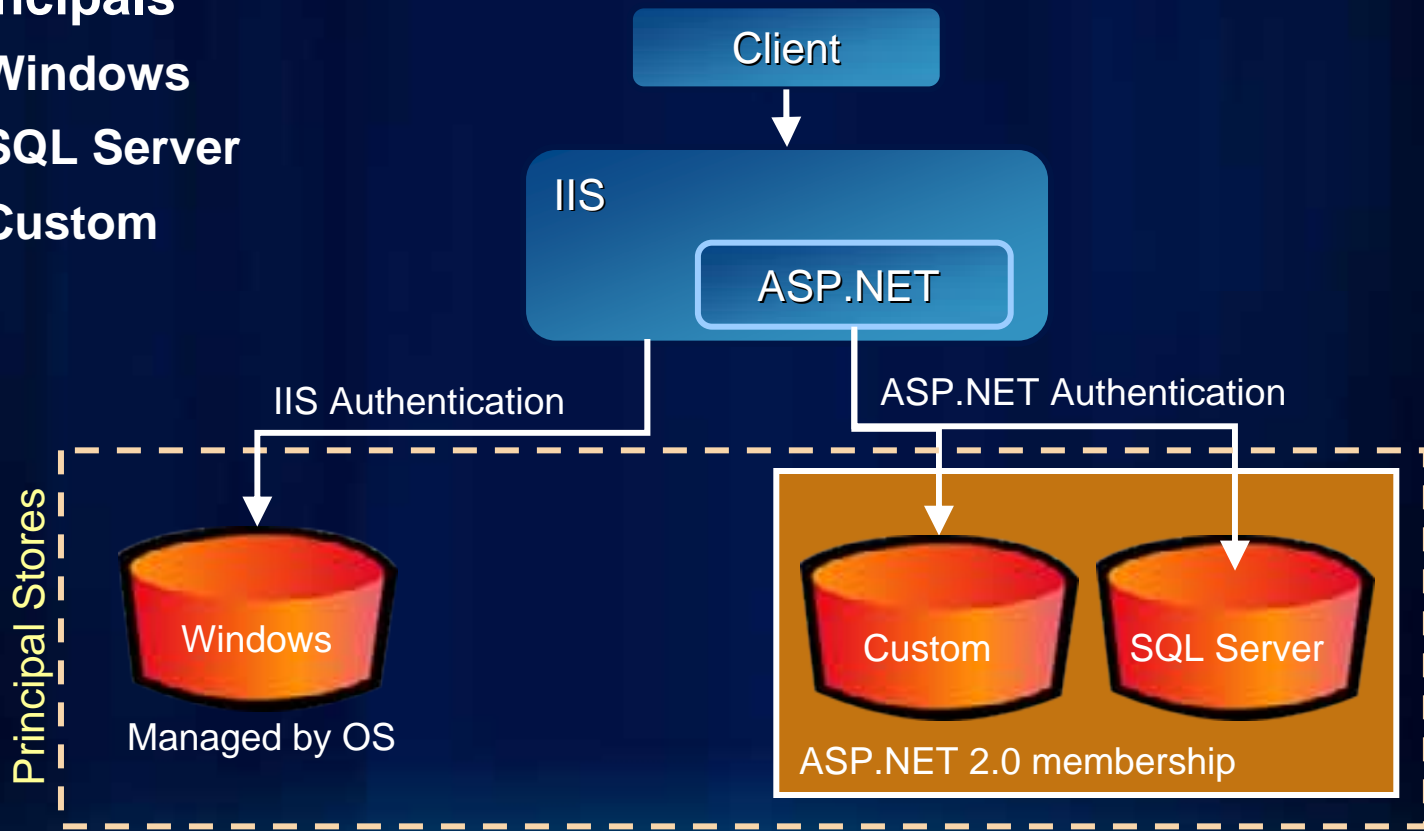
Access control model for web users

- **ArcGIS Server has role-based access control**
- **Uses standard security protocols**
 - **IIS / Java EE**
 - **Basic, Digest, Integrated Windows**
- **Token based services access**
 - **Windows: ASP.NET Membership and role provider**
 - **Java: ArcGIS Managed Authentication: JDBC, LDAP, Active Directory**

Authenticating users - Windows

- Authentication requires storage location for Principals

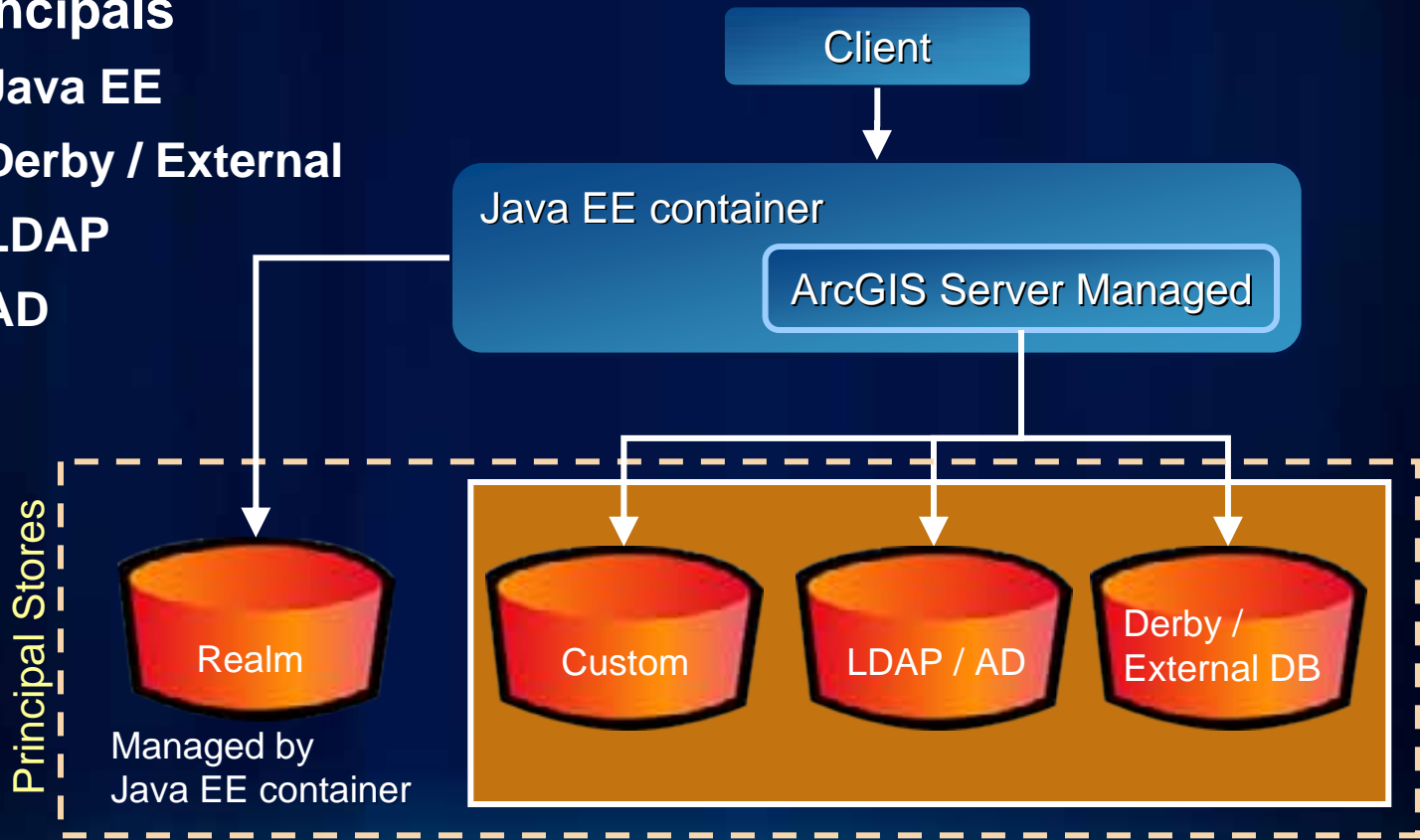
- Windows
- SQL Server
- Custom



Authenticating users - Java

- **Authentication requires storage location for Principals**

- Java EE
- Derby / External
- LDAP
- AD



Configuring security

- **Decide where users and roles will be stored**
- **Install supporting items as needed**
 - **Secure Sockets Layer (SSL) certificate for Web server**
 - **Database**
 - **Custom provider**
- **Configure security in Manager**
 - **Configure location for users and roles**
 - **Add and manage users and roles**
- **Secure GIS Web services using Manager**
- **Secure Applications (Flex, Silverlight, Javascript)**

More details on users and roles

- **User and role store usually same place, but can have**
 - Windows users + database roles
 - Windows users + roles in custom provider
 - Database users + roles in custom provider
- **Built-in roles (Token based security only)**
 - **Everyone (*):** all users permitted whether provide login or not
 - **Authenticated Users (@):** users who provide a valid login
 - **Anonymous (?):** users who do not provide a login

Session agenda

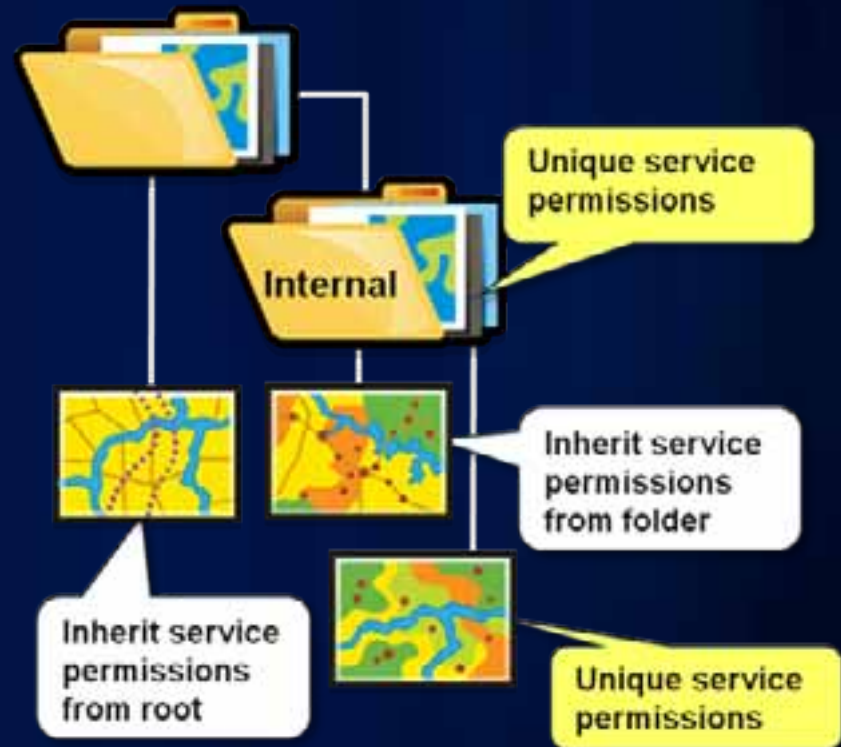
- **Security overview**
- **Setup and configuration**
- **Securing GIS Web services**
- **Using the token service**
 - **Using a proxy page**
- **Securing Web applications**
- **Security pass through**

Securing ArcGIS Server services

- **Two ways to connect to an ArcGIS Server service**
- **Local (“Intranet”) connection**
 - Works only on intranets
 - Access to all server functionality
 - User must be a member of the agsusers or agsadmin groups
- **Web service (“Internet”) connections**
 - SOAP, REST, WMS, KML
 - Works on intranets and over Internet

Securing GIS Web services

- Services inherit folder permissions
- Good practice to secure folders
- Permissions changes cascade to all children
 - **Set permissions on root first**



Capabilities have same security as service

- **Services**
 - **Map, Geodata, Geoprocessing, Geocode, Geometry, Globe, Image, Search**
- **Capabilities**
 - **KML, WMS, WFS, WCS, Mobile Data, Feature Access, Network Analysis**
- **What if I want secure editing with public viewing?**
 - **Publish two map services**

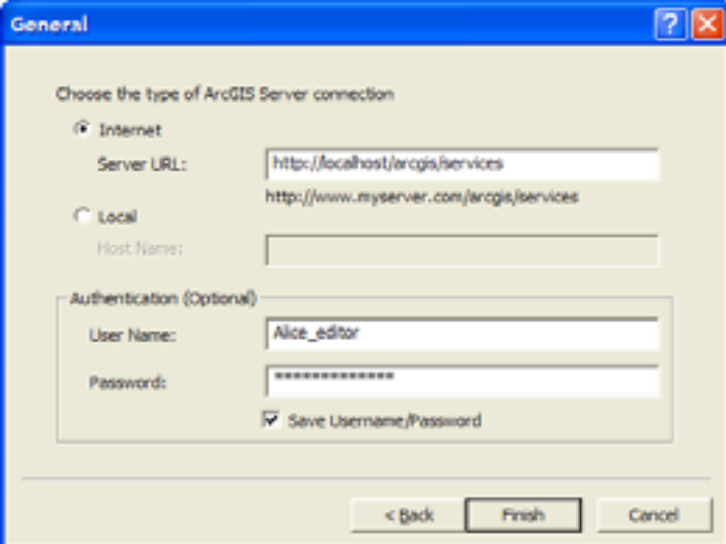
Transitioning ArcGIS Server: Open to Secure

- Enabling security for services is set separately from permissions
 - Security-Settings tab
- With no security, everyone has access to everything
- If you enable security before changing permissions, no one will be able to use existing services



Using secured services

- **ArcGIS Desktop, ArcGIS Explorer**
 - Provide identity in connection dialog
- **SOAP, and REST applications**
 - Use token or Windows authentication
 - More on this shortly



The image shows a screenshot of the 'General' dialog box in ArcGIS, titled 'General'. The dialog is for configuring an ArcGIS Server connection. It has a blue title bar with a question mark icon and a close button. The main content area is light yellow and contains the following elements:

- Choose the type of ArcGIS Server connection:**
 - Internet**
 - Server URL:
 - Local**
 - Host Name:
- Authentication (Optional):**
 - User Name:
 - Password:
 - Save Username/Password

At the bottom of the dialog, there are three buttons: '< Back', 'Finish', and 'Cancel'.

SSL for services

- **Require Encrypted Web Access for folders and services**
 - **AGS Manager or ArcCatalog**
 - **You can't set encrypted access on a service, it has to be a folder**

- **When?**
 - **Using Basic or Digest security**
 - **You don't want a token to be intercepted in transmission**
 - **Data being displayed in dynamic service is sensitive**
 - **Attributes of a query contain sensitive information**

Demo

Securing GIS Web services

Session agenda

- **Security overview**
- **Setup and configuration**
- **Securing GIS Web services**
- **Using the token service**
 - **Using a proxy page**
- **Securing Web applications**
- **Security pass through**

The Token service

- **User authentication web service**
 - Token provided to access services
 - Uses HTTPS by default
- **Why do we need it?**
 - Web service security when using
 - Windows: ASP.NET membership / role provider
 - Java: ArcGIS Server Managed Authentication
- **Used only with GIS Web services**
 - Not used by default with Windows users
 - Not used to authenticate Web application users

What is in a Token?

- **Token is a string with encrypted information:**
 - **User name**
 - **Expiration time**
 - **Client ID (optional)**
 - **IP address or Web URL (HTTP Referrer)**
 - **If included, expiration can be a longer time period (weeks/months)**
 - **Used by most clients – Desktop, ADF, Web API/REST applications, etc.**
 - **If not included, shorter expiration time – needs to be renewed**

Token :

npWVMq1IK0V1qSpexMyKQEGGJzA511zVX1YVD19zB5XCKNGY7B7E21JGGV9zJFCVQq5JGvzK1#EXU

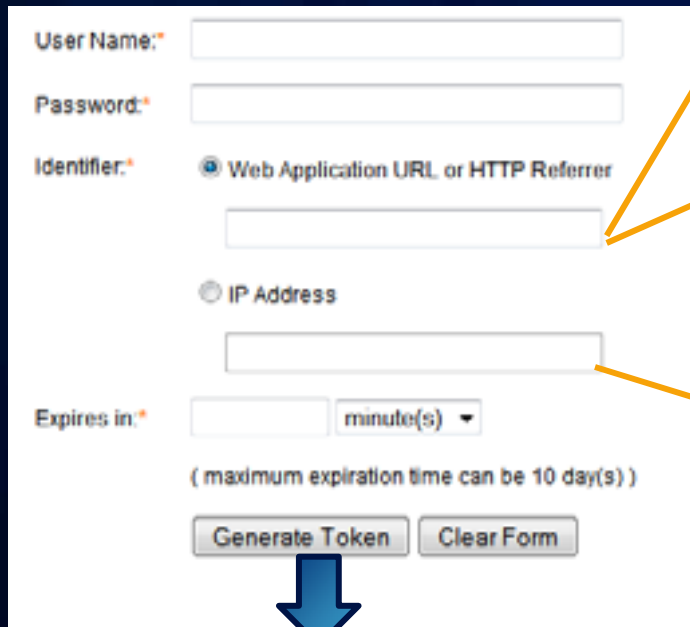
Working with the Token service

- **ArcGIS Clients will work with tokens automatically**
 - ArcGIS Desktop, ArcGIS Engine, ArcGIS Explorer
- **Other Clients will require explicit token management**
 - **SOAP-based clients not using ADF**
 - Use server-side code to acquire and use token
 - **Web API/REST Clients**
 - Developer obtains a token from get-token Web page
 - Developer embeds token in application or proxy

Getting a token

Services Directory

[Login](#) | [Get Token](#)
[Help](#) | [API Reference](#)



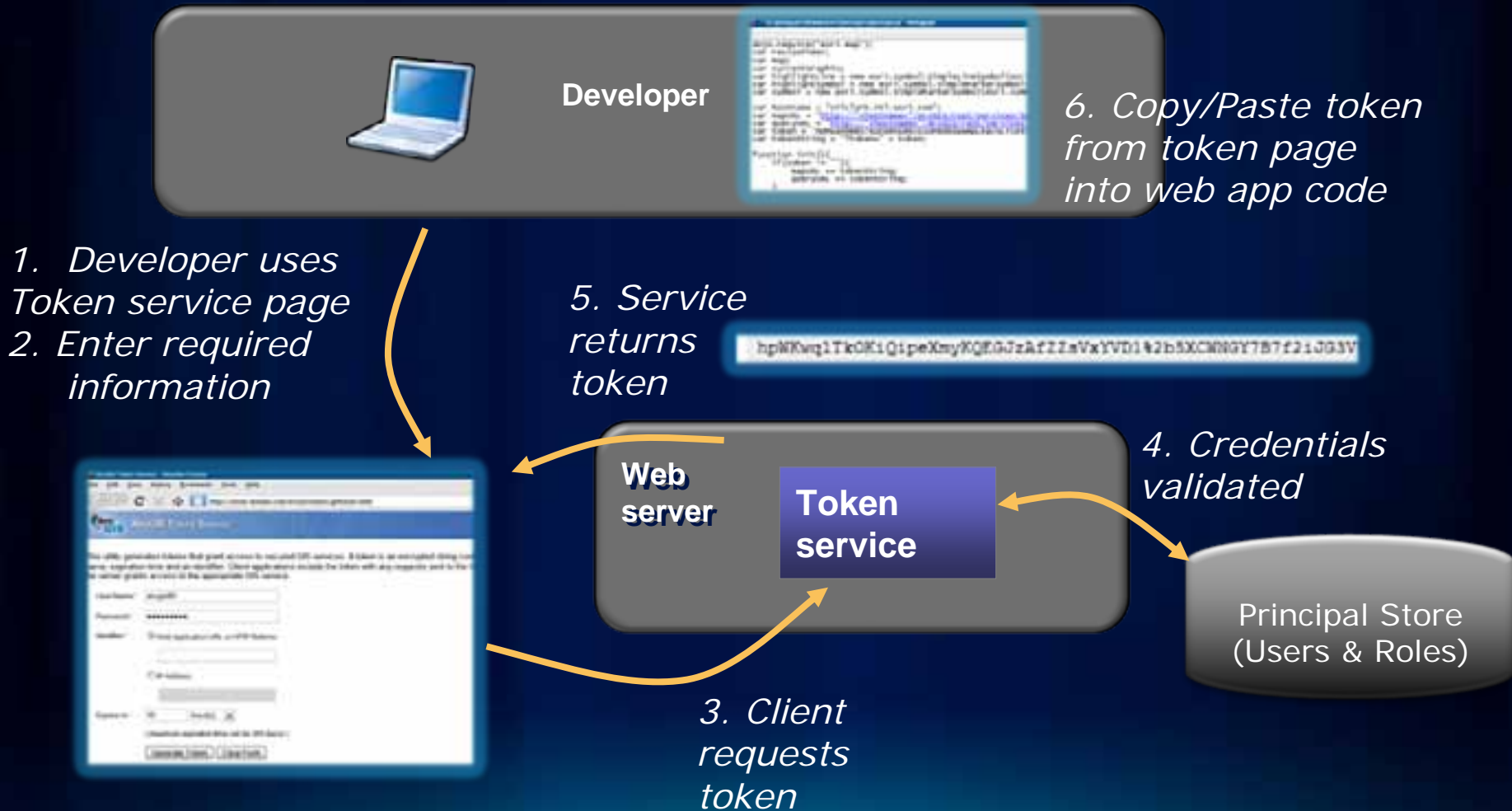
The screenshot shows a web form for generating a token. It includes fields for 'User Name', 'Password', and 'Identifier'. The 'Identifier' section has two radio buttons: 'Web Application URL or HTTP Referrer' (selected) and 'IP Address'. Below the 'Identifier' fields is an 'Expires in' field with a dropdown menu set to 'minute(s)'. At the bottom are 'Generate Token' and 'Clear Form' buttons. A blue arrow points from the 'Get Token' link in the top navigation to the form. Three orange arrows point from the form fields to the list on the right: one from the 'User Name' field to the first URL, one from the 'Identifier' field to the second URL, and one from the 'Expires in' field to the third bullet point.

- [HTTP://myWebAppHost/myApp](http://myWebAppHost/myApp)
 - App must be accessed via HTTP
- myWebAppHost/myApp
 - App can be accessed via HTTP or HTTPS
- Use IP with proxy page (more later)

Copy the following token into your application.

`uLjCoVvnUP-IUTnhMtJtm3KYjZ_77efAeDQVCGaB3sY.`

How developers commonly use the Token service



How the Web APIs/REST clients use the Token



Using a token

- **Append the token to the URL of the server**
 - `http://myserver/arcgis/services/USA/MapServer?token=h
pWKwq...`
- **Use HTTPS for maximum security over unsecure networks**
 - **Needed to guard against token hijacking and replay attacks**

Demo

Using secure services in a flex application

Using a proxy page for token management

- **Tokens in web API applications expire**
 - HTTP error code of 498
 - Refresh embedded tokens periodically (source / config file update)
- **Proxy page**
 - Embed token using servers IP address as referrer
 - Pro: Token not exposed to client
 - Con: Tokens must still be updated in proxy page
 - Embed user name and password for dynamic token generation
 - Pro: No ongoing maintenance
 - Con: User name and password is unencrypted on the server
- **Forum post contains dynamic proxy:**
<http://forums.esri.com/Thread.asp?c=158&f=2396&t=297001>

Proxy page security

- **Proxy page contains no security logic**
 - If left unsecure proxy provides unsecure back door to services
- **Include proxy in web application and secure the application**
- **See [Using the proxy page](#) in JavaScript API help**

Demo

Using a proxy page for token management

Session agenda

- **Security overview**
- **Setup and configuration**
- **Securing GIS Web services**
- **Using the token service**
 - **Using a proxy page**
- **Securing Web applications**
- **Security pass through**

Application security considerations

- **Browser based applications (JavaScript, Flex, Silverlight)**
 - Application and web services need to be secured
 - Web services are accessed from the browser



Securing Web API applications

- **Can't secure applications with only client-side code**
- **Secure using the web server / container**
 - IIS / Java EE
- **Using ASP.NET**
 - Wrap code in .aspx page
- **Other**

Session agenda

- **Security overview**
- **Setup and configuration**
- **Securing GIS Web services**
- **Using the token service**
 - **Using a proxy page**
- **Securing Web applications**
- **Security pass through**

Passing identity from Web API to Services

- **JavaScript, Flex, and Silverlight**
 - It just works
- **Integrated Windows / Basic automatically pass credentials from application to web services**

Passing identity to Secured Services

- Web application requests token from tokens services
 - Tokens service parameters
 - username
 - password
 - clientid (ref.[URL], ip.[IP ADDRESS])
 - Expiration (minutes)
 - E.g. :
[https://host/ArcGIS/tokens/?request=getToken&username=user
&password=pass&clientid=ref.myAppHost&expiration=10](https://host/ArcGIS/tokens/?request=getToken&username=user&password=pass&clientid=ref.myAppHost&expiration=10)
- Append token to layer

Demo

Modifying Web application content
based on user's role

Security patterns

Application configuration	Public app with secure services	Secure app with secure services	Public app with login for secure services	Single sign on
Security model	Token based security	All security models	Token based security	IIS Security using Integrated Windows Authentication
Embed token in proxy page	No	Yes	No	N/A
Network	Internet / Intranet	Internet / Intranet	Internet / Intranet	Intranet

Security resources for ArcGIS Server

- **ArcGIS Server Resource Center**
 - <http://resources.arcgis.com>
 - **Accessing secure services: Web APIs**
- **Enterprise Resource Center**
 - <http://resources.arcgis.com/content/enterprise/10.0/about>
- **Supporting Resources for ArcGIS Server**
 - **ArcGIS Server Help**
 - **Web APIs, REST, SOAP Developer Help**

Want to Learn More?

ESRI Training and Education Resources

- **Instructor-Led (Classroom) Training**
 - [ArcGIS Server: Web Administration Using the Microsoft .NET Framework](#)
- **Self-Study (Virtual Campus) Training**
 - [ArcGIS Server Setup and Administration](#)
 - [Implementing Security for ArcGIS Server .NET Solutions](#)

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

Summary

- **ArcGIS Server Manager enables users to**
 - **Configure user and role stores**
 - **Secure GIS Web services**
- **Clients work with security**
 - **ArcGIS Clients (Desktop, Explorer, Engine) work seamlessly**
 - **SOAP and REST clients may require working with tokens**
- **Token management is key to maintaining secure applications**

Questions

- Thank you
- Please fill out the survey