Building Security into Your System

Bill Major

Gregory Ponto

Overview

Building Security into Your System

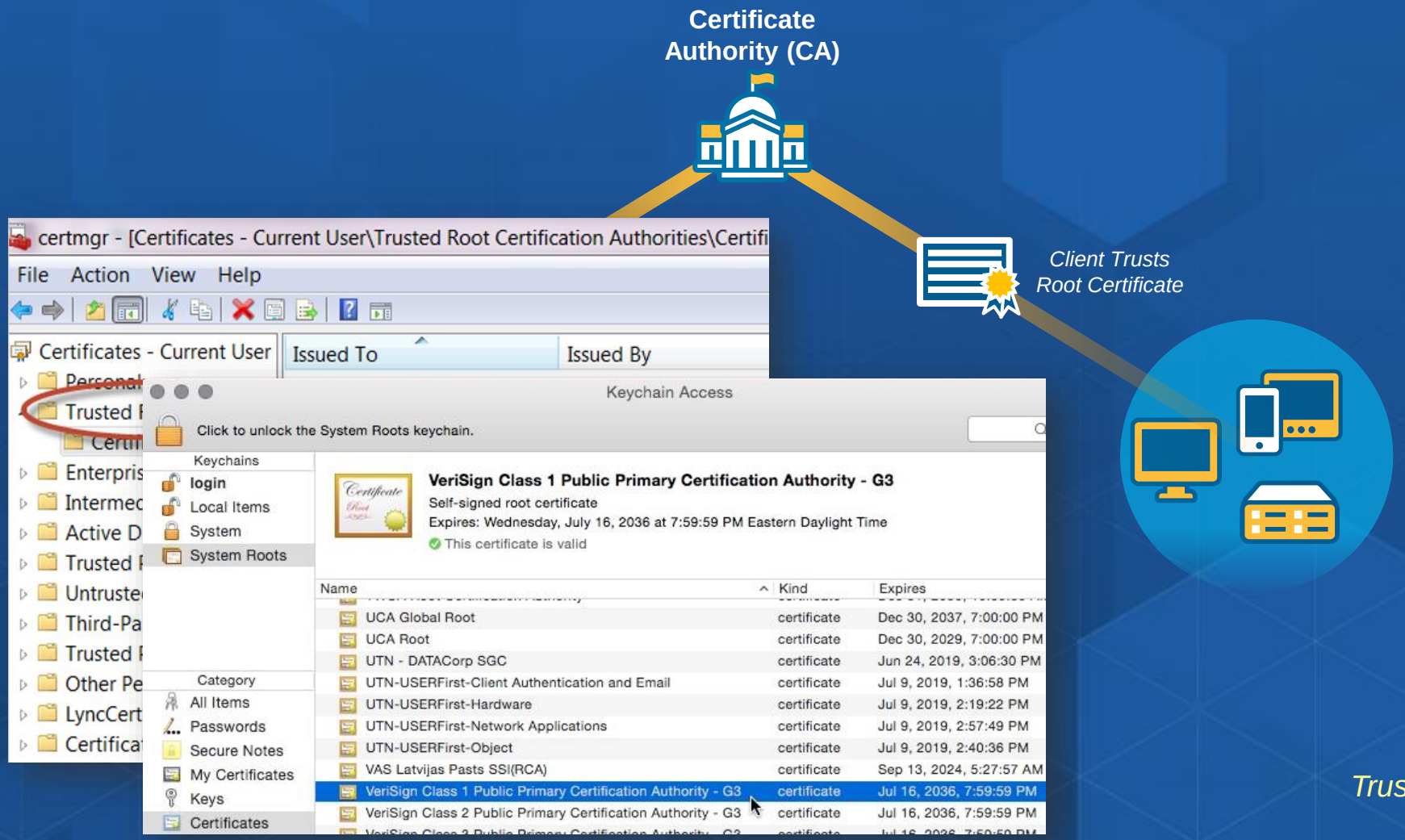
PKI Fundamentals	*Encrypted & Trusted Communication*
Implementing SSL/TLS	*How do I do it with ArcGIS?*
Scan ArcGIS Server/Portal	*Security Best Practices*

PKI Fundamentals

Encrypted & Trusted Communication

PKI Fundamentals

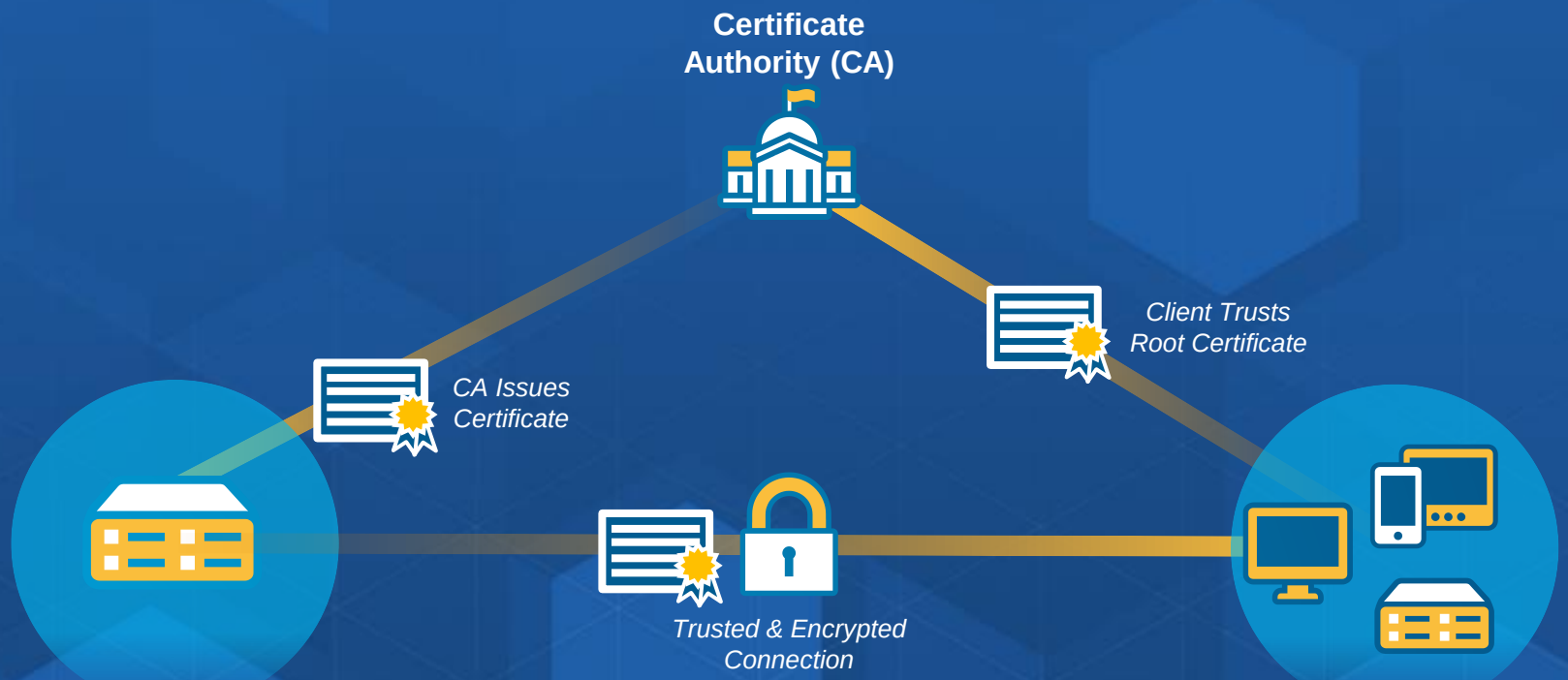
Certificate Authority (Root of Trust)



Trust, Encrypt, Communicate

PKI Fundamentals

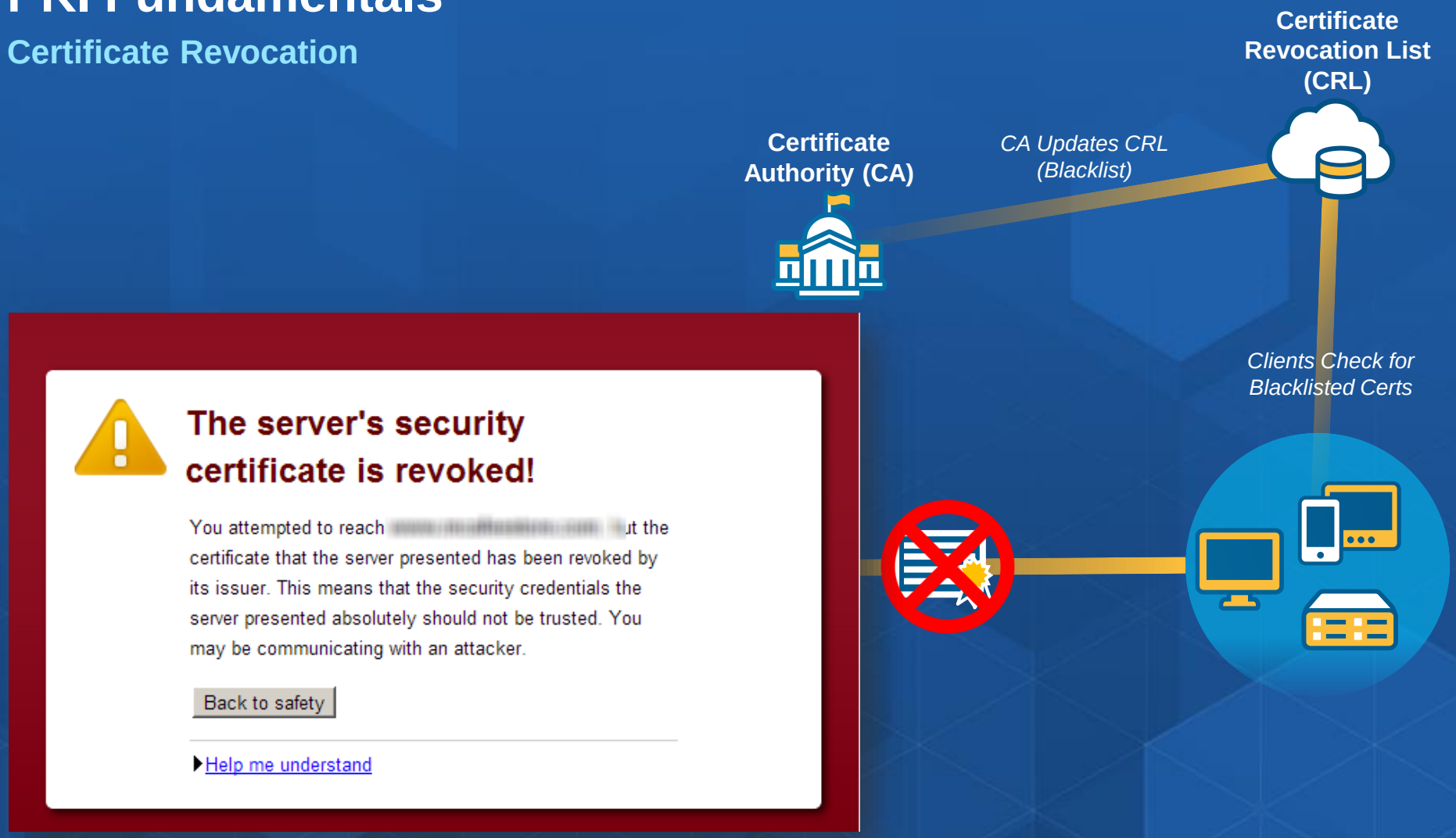
Establishing Trust for Encrypted Communication



Trust, Encrypt, Communicate

PKI Fundamentals

Certificate Revocation



What if a trusted server is compromised?

Implementing SSL/TLS

How do I do it with ArcGIS?

Setting up SSL Certificates and Trusts

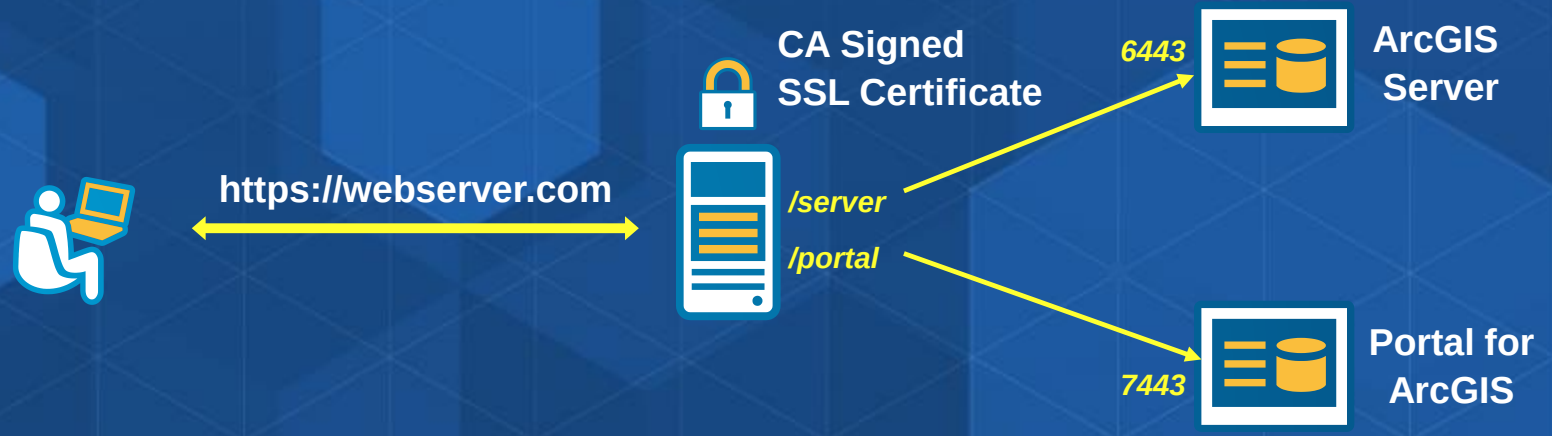
Server Certificates and Trust Stores

- Secure Socket Layer (SSL) - standard security technology for establishing an encrypted link between a web server and a browser
  - TLS v 1.2
- Most organizations have strict SSL requirements for security compliance.
- Certificate Authorities digitally sign server certificates for server identification and issuing user certificates for client identification (i.e. Public Key Infrastructure).
- Public key/private key pairing for encrypted communication
- Adjustments needed to configure On-premises Web GIS to work properly in these types of environments

Setting up SSL Certificates and Trusts

Server Certificates and Trust Stores

- Portal for ArcGIS, ArcGIS for Server, ArcGIS Data Store, Geoevent Extension for ArcGIS Server: all install self-signed certificates to support ports 7443, 6443, 2443, 6143 respectively.
- Consuming services from self-signed certificates is untrustworthy and easily compromised.
- Install Web Adaptors for Portal and ArcGIS Server and SSL-enable your web server.
- Users only communicate with Web Server over default HTTPS (i.e. 443)



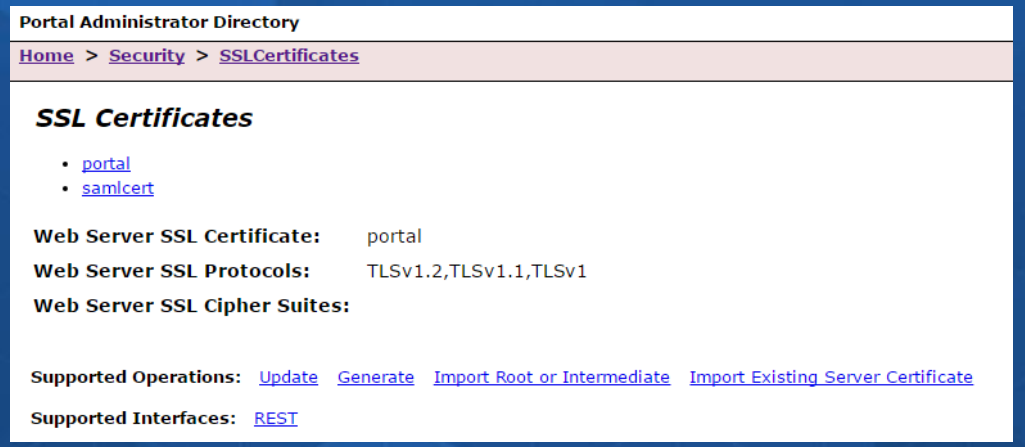
Setting up SSL Certificates and Trusts

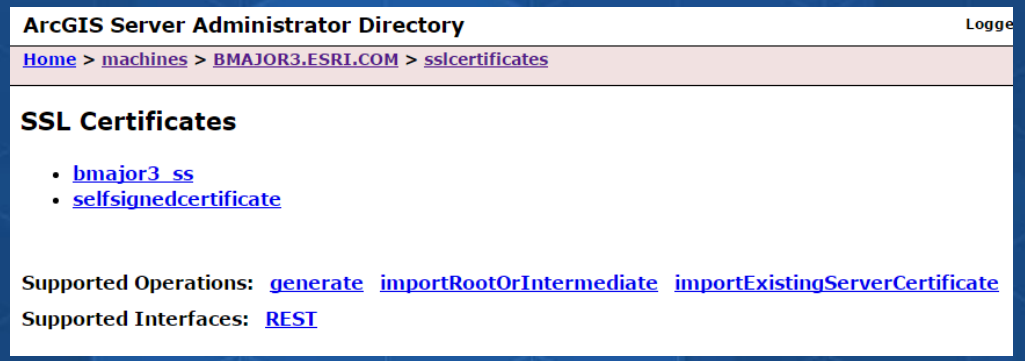
Updating Server Certificates

- Some organizations mandate no HTTP(S) ports without using a properly signed server certificate. Users must update the self-signed certificates with CA signed certificates.

- Portal Administrator Directory provides tools to generate a new Certificate Signing Request and ability to import Intermediate or Root certificates for trust.

- ArcGIS Server Administrator Directory provides identical interface.





Setting up SSL Certificates and Trusts

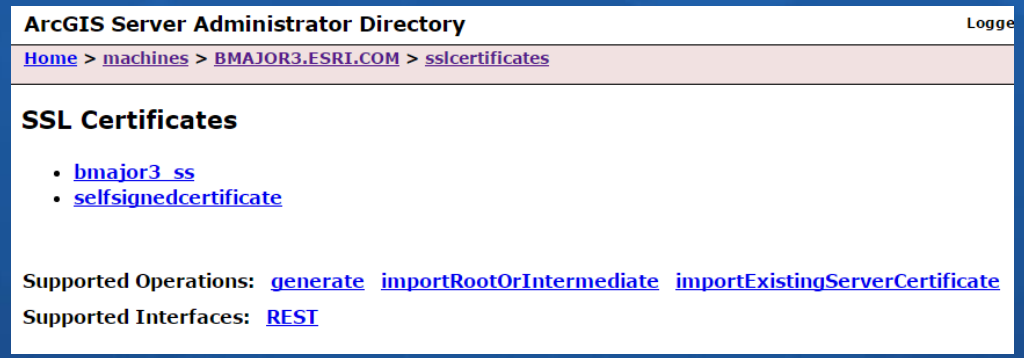
Establishing Trust to PKI resources

- In order to consume services from other SSL enabled web servers, proper “trust” must be created in ArcGIS Server and Portal.
- Importing CA Root and Intermediate certificates for external server certificates allows ArcGIS Server and Portal to “trust” the server SSL certificate being presented
  - This trust established proper encryption channel
- Example scenarios:
  - Adding an HTTPS Map Service to Portal from an external organization.
  - Using ArcGIS Server Print Service to generate thumbnails for Portal for ArcGIS, using HTTPS Map Services.

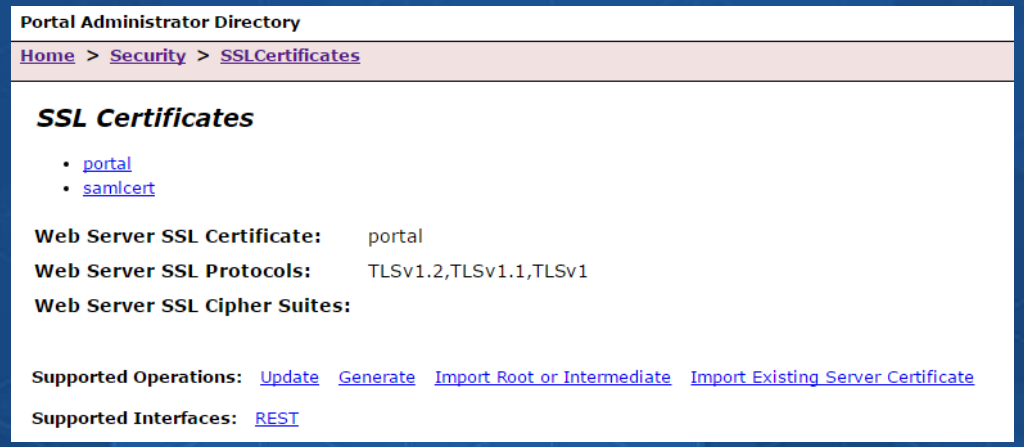
Setting up SSL Certificates and Trusts

Importing Certificates to establish Trust

- In ArcGIS Server, use the Administrator Directory.
- On the Server, import the CA Root and Intermediate certificates into the OS Trust Store (needed for GP Services).

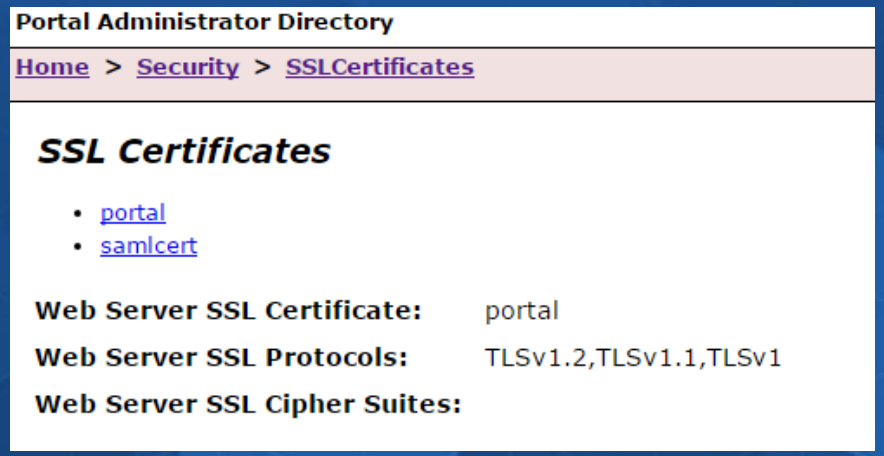


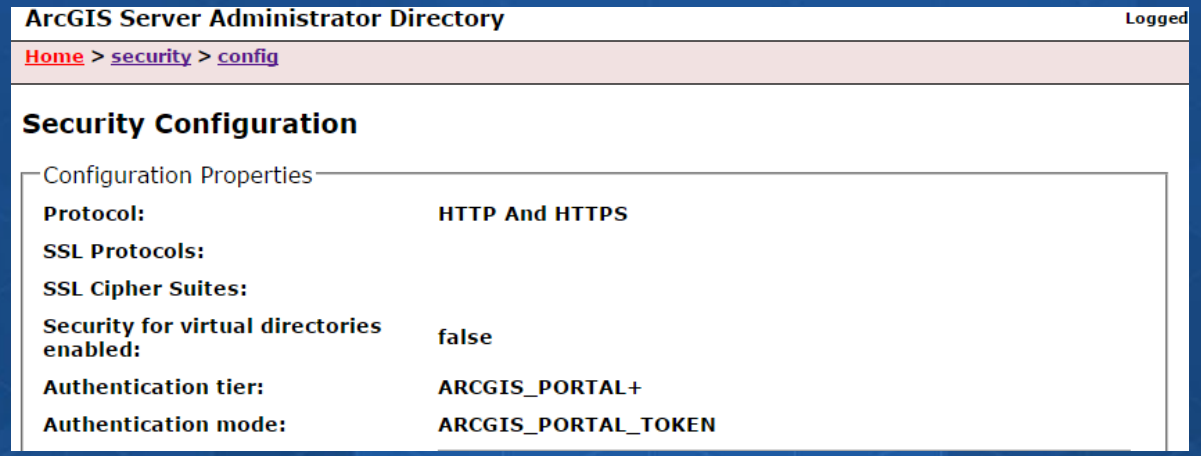
- In Portal for ArcGIS, use the Portal Administrator Directory.



Restrict SSL protocols and cipher suites

- As a Web GIS Administrator you can specify which secure sockets layer (SSL) protocols and encryption algorithms the portal's internal web server uses to secure communication.





Scan ArcGIS Server/Portal

Security Best Practices

Scan ArcGIS for Server and Portal for ArcGIS for Best Practices

- Starting at 10.4, ArcGIS Server and Portal for ArcGIS come with a Python utility that will scan your setup for security best practices.
- portalScan.py and serverScan.py (under /tools directory)
- Findings can include:
  - Determines if HTTPS only communication
  - REST services directories are enabled/disabled
  - Anonymous access exposed
  - Proxy restrictions
  - Standardized Queries are enforced; protect against SQL injection attacks
  - Filter web content enabled; protects against XSS attacks
  - Token requests via GET/POST exposed

Demo

Scanning Portal & Server

```
    Directory: C:\Program Files\ArcGIS\Server\tools\admin


Mode
----
-a---
-a---
-a---
-a---
-a---
-a---
-a---
-a---
-a---
-a---


PS C:\Prograr
PS C:\Prograr
```

C:\Python27\ArcGISx6410.4\python.exe

```
Enter ArcGIS for Server fully qualified domain name: gregp2.esri.com
Enter administrator username: siteadmin
Enter administrator password:
```

```
    Directory: C:\Program Files\ArcGIS\Server\tools\admin


Mode
----
-a---          4
-a---          4
-a---          4
-a---          4
-a---          4
-a---          4
-a---          4
-a---          4
-a---          4
-a---          4
-a---         6/


PS C:\Program Fi
```

ArcGIS for Server Security Scan Report - 2016-06-23

gregp2.esri.com

Potential security items to review

Id	Severity	Property Tested	Scan Results
SS08	Important	Cross-domain requests	Cross-domain requests are unrestricted. To reduce the possibility of an unknown application sending malicious commands to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust.
SS07	Important	Rest services directory	The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks.
SS11	Recommended	PSA account status	The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your identity store.

Scan ArcGIS Server for Security Best Practices

http://server.arcgis.com/en/server/latest/administer/windows/scan-arcgis-server-for-security-best-practices.htm

```
    Directory: C:\Program Files\ArcGIS\Portal\tools\security

Mode
----
-a---          12

PS C:\Program F
PS C:\Program F
```

C:\Python27\ArcGISx6410.4\python.exe

```
Enter Portal for ArcGIS fully qualified domain name: gregp2.esri.com
Enter administrator username: portaladmin
Enter administrator password:
```

```
    Directory: C:\Program Files\ArcGIS\Portal\tools\security


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---          12/11/2
-a---           6/23/2                                          html


PS C:\Program Files\
```

Portal for ArcGIS Security Scan Report - 2016-06-23

gregp2.esri.com

Potential security items to review

Id	Severity	Property Tested	Scan Results
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses.
PS06	Recommended	Anonymous access	To prevent any user from accessing content without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access.
PS05	Recommended	Built-in account sign-up	By default, users can click the Create An Account button on the portal sign-up page to create a built-in portal account. If you are using enterprise accounts or you want to create all accounts manually, this option should be disabled.

Scan Portal for ArcGIS for Security Best Practices

http://server.arcgis.com/en/portal/latest/administer/windows/scan-your-portal-for-security-best-practices.htm

Key Takeaways

- PKI is about Encrypted Communication
- Web GIS provides support for PKI
- Scan your Server for Security Best Practices
- Web GIS 10.4+ is Recommended

Resources / References

Scan ArcGIS Server for Security Best Practices
http://server.arcgis.com/en/server/latest/administer/windows/scan-arcgis-server-for-security-best-practices.htm

Scan Portal for ArcGIS for Security Best Practices
http://server.arcgis.com/en/portal/latest/administer/windows/scan-your-portal-for-security-best-practices.htm

Security Best Practices with Web GIS
http://server.arcgis.com/en/server/latest/administer/windows/best-practices-for-configuring-a-secure-environment.htm
http://server.arcgis.com/en/portal/latest/administer/windows/security-best-practices.htm

Encrypting Web GIS Communication
http://server.arcgis.com/en/server/latest/administer/windows/secure-arcgis-server-communication.htm

ArcGIS Trust Site
http://trust.arcgis.com

Questions?

Bill Major bmajor@esri.com
Gregory Ponto gponto@esri.com

Security Standards & Architecture Team
securesoftwareservices@esri.com