ArcGIS and SSL Considerations

Bill Major and Craig Cleveland
Overview
ArcGIS Enterprise and SSL Considerations

1 - Fundamentals of Secure Communication

2 - Implementing SSL/TLS at the Web Tier

3 - Implementing SSL/TLS within ArcGIS Enterprise

4 - Troubleshooting Common SSL Problems
Fundamentals of Secure Communication

Encrypted & Trusted Communication
Fundamentals of Secure Communication
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 v1.2

- Certificate Authorities establish trust by digitally signing server certificates for server identification and issuing user certificates for client identification (i.e. Public Key Infrastructure).
  - Open Internet SSL Checker: https://www.sslshopper.com/ssl-checker.html

- Public key/private key pairing for encrypted communication

- Adjustments needed to configure ArcGIS Enterprise to work properly in secure/closed environments
Fundamentals of Secure Communication
Certificate Authority (Root of Trust)

Server

Certificate Authority (CA)

Clients Trust Root Certificate

Clients

Trust, Encrypt, Communicate
Fundamentals of Secure Communication
Intermediate Certificate Authority (Trust Chain)

Certificate Authority (CA)

Intermmediate Certificate Authority (CA)

Server Trusts Root Certificate

Server

Clients Trust Root Certificate

Clients Trust Intermediate Certificate

Clients
Fundamentals of Secure Communication

Establishing Trust for Encrypted Communication

Certificate Authority (CA)

CA Issues Certificate

Clients Trust Root Certificate

Trusted & Encrypted Connection

Trust, Encrypt, Communicate
Fundamentals of Secure Communication
Certificate Revocation

What if a trusted server is compromised?

The server's security certificate is revoked!

You attempted to reach [domainname], but the certificate that the server presented has been revoked by its issuer. This means that the security credentials the server presented absolutely should not be trusted. You may be communicating with an attacker.

[Back to safety]

[Help me understand]
Fundamentals of Secure Communication

Trust Stores

- To access the Windows trust store use the Microsoft Management Console
  - Start – MMC – File – Add/Remove Snap-in – Certificates

- To access the Mac trust store use Keychain Access
Fundamentals of Secure Communication
Trust Stores and Browsers

- Internet Explorer and Chrome use the Windows trust store
  - *Keychain Access for Macs (Chrome Only)*

- Firefox has its own trust store
  - *Managed separately!*
Trust Stores
Demonstration
Implementing SSL/TLS at the Web Tier
Setting up SSL Certificates and Trusts
SSL-Enable Your Web Server

• Some organizations mandate no HTTP(S) ports without using a properly signed server certificate.

• By default your web server only communicates via HTTP

• To enable SSL obtain a CA signed server certificate and configure your web server to use it
Setting up SSL Certificates and Trusts
SSL-Enable Your Web Server

1. Create certificate signing request

- CSR’s can be created in many ways – web servers, openssl, keytool, Portal & ArcGIS Server Admin pages

- The Common Name property of a CSR is the URL by which your web server will be accessed.
2. Present CSR to certificate authority

- Depending on deployment locale your CA may be public or local (e.g. DigiCert vs. Internal Organization CA)

- Be sure to specify a subject alternative name (SAN) when presenting your CSR to your CA (e.g. san:dns=myserver.esri.com). Now required by most major browsers (e.g. Chrome).
Setting up SSL Certificates and Trusts

SSL-Enable Your Web Server

3. Download signed certificate
4. Install and configure signed certificate on your web server.
SSL Enable Your Web Server

Demonstration
Implementing SSL/TLS within ArcGIS
SSL Touch Points in ArcGIS Enterprise

Example

**Client browser must trust CA chain**

Client Web Browser

Web Server

**Client browser must trust CA chain**

**Web Server must trust CA chain if :7443 is using CA signed**

Web Server

Secure LDAP

**Web Server must trust CA chain**

**Portal must trust CA chain of ArcGIS Server**

Portal for ArcGIS

**Portal must trust CA chain of ArcGIS Server**

External SSL ArcGIS Server

**Print Task ArcGIS Server and OS must trust CA chain to Portal, Web Server, and External ArcGIS Servers**

Federated ArcGIS Server
Portal for ArcGIS, ArcGIS Server, Data Store, GeoEvent and Web AppBuilder Developer Edition all install self-signed certificates to support communication on ports 7443, 6443, 2443, 6143 and 3344 respectively.

- Each of these self-signed certificates can be replaced with CA signed certificates to have completely secure communication.

- Consuming services from self-signed certificates is untrustworthy and easily compromised.
  
  - Remember Certificate Authorities establish trust!

- Additionally disable HTTP communication in Portal and ArcGIS Server.
Secure Communication Via ArcGIS Web Adaptor

- The first step to implementing secure communication is installing and configuring the Web Adaptor
  - Moves traffic from 6443/6080 (ArcGIS Server) and 7443/7080 (Portal) to 443/80

- Moving traffic to default ports allows ArcGIS to take advantage of signed server certificates at the web tier
Disable HTTP
ArcGIS Server and Portal for ArcGIS

- Additionally disable HTTP communication in Portal and ArcGIS Server to use only HTTPS communication

- From the ArcGIS Server admin, and the Portal My Organization settings disable all HTTP communication
So far we’ve only covered installing and configuring CA signed certificates on the web tier, and disabling HTTP. Now the replacement of self-signed certificates needs to be completed at the app tier to have *fully trusted, and secure communication.*
Updating internal ArcGIS Enterprise Certificates
Portal for ArcGIS

• The Portal Administrator directory provides tools to Import Intermediate or Root certificates and Existing Server Certificates, as well as the ability to generate a new Certificate Signing Request.
  - Used for updating internal ArcGIS Enterprise certificates, as well as establishing trust chains with external servers

• Accessed via Portaladmin – Security – SSLCertificates. Import appropriate certificates and then Update.
Updating internal ArcGIS Enterprise Certificates

Portal for ArcGIS

- When working in closed environments you must import root and intermediate certificates in addition to the existing server certificate!
  - Hybrid environments using signed certificates from known CA’s may not need this step (e.g. CA is DigiCert)

- New at 10.6 – option to *not* restart Portal service after importing certificates
  - At 10.5/1.5.1 Portal service restarted automatically
  - At 10.4.1 and prior Portal service needed to be restarted manually
Updating internal ArcGIS Enterprise Certificates
ArcGIS Server

- ArcGIS Server Administrator Directory provides nearly identical tools to Portal, including the ability to Import Intermediate or Root certificates and Existing Server Certificates, as well as the ability to generate a new Certificate Signing Request.


<table>
<thead>
<tr>
<th>ArcGIS Server Administrator Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home</strong> &gt; <strong>machines</strong> &gt; <strong>WIN-49BHV9ORSS</strong> &gt; <strong>sslcertificates</strong></td>
</tr>
</tbody>
</table>

**SSL Certificates**
- selfsignedcertificate

Supported Operations:  
generate  importRootOrIntermediate  importExistingServerCertificate

Supported Interfaces:  REST
Updating internal ArcGIS Enterprise Certificates

ArcGIS Server

- Import appropriate certificates, browse back to [machine name] and then Update.

- When working in closed environments you must import root and intermediate certificates in addition to the existing server certificate!
  - Hybrid environments using signed certificates from known CA’s may not need this step (e.g. CA is DigiCert)

- *No ArcGIS Server service restart required…ArcGIS Server does this automatically.
Updating internal ArcGIS Enterprise Certificates
Data Store for ArcGIS

- Data Store for ArcGIS ships with a number of batch files for managing its properties, and one of those is updatesslcertificate.bat.
  - Accessed at C:\Program Files\ArcGIS\DataStore\tools

- The certificate file must be in PKCS12 format with a file extension of .pfx or .p12

- Prompted for Data Store restart at completion of process
Updating Internal ArcGIS Enterprise Certificates

Demonstration

Command Prompt:
```
C:\>Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\windows\system32\cd c:\program files\arcgis\datastore\tools
C:\program files\arcgis\datastore\tools\updatesslcertificate.bat
"Usage: updatesslcertificate <filename_with_path> <password> <alias>"
C:\program files\arcgis\datastore\tools\updatesslcertificate.bat c:\temp\mysecfx secretpassword! newdatastorecert
This operation will restart the ArcGIS Data Store web server.
Do you wish to continue (Yes or No)? Yes
```
Establishing Trust to external resources
Importing Root and Intermediate Certificates

• In order to consume services from other SSL enabled web servers, proper trust must be created in ArcGIS Server and Portal.

• Importing Root and Intermediate certificates for external server certificates allows ArcGIS Server and Portal to trust the server SSL certificate being presented
  - This trust establishes 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.
Establishing Trust to external resources
Portal for ArcGIS

- In Portal for ArcGIS use the Portal Administrator directory to import Root and Intermediate certificates
Establishing Trust to external resources

ArcGIS Server

- In ArcGIS Server use the Administrator Directory import Root and Intermediate certificates

- On the Server, import Root and Intermediate certificates into the OS Trust Store (needed for GP Services).
Additional Considerations
Restrict SSL protocols and cipher suites

- Within the respective ArcGIS Enterprise components you can specify which SSL protocols and encryption algorithms to use to secure communication.
Import SSL Certificates in AGOL?
Trust in AGOL for custom CAs

- Adding ArcGIS Server service URLs as items coming from custom CA SSL endpoints in AGOL can sometimes cause problems.
- Fall 2017 release of AGOL introduced APIs to import root or intermediate CA certificates
- API calls only to do this; no UI experience at moment.

- List Certificates (GET)
  - https://www.arcgis.com/sharing/rest/portals/self/certificates?f=json&token=...

- Add Certificate (POST)
  - https://www.arcgis.com/sharing/rest/portals/<orgid>/certificates/register
### Importing Certificates into Portal

**Demonstration**

<table>
<thead>
<tr>
<th>SSL Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>portal</td>
</tr>
</tbody>
</table>

**Web Server SSL Certificate:**
- portal

**Web Server SSL Protocols:**
- TLSv1.2, TLSv1.1, TLSv1

**Web Server SSL Cipher Suites:**
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

**Supported Operations:**
- Generate
- Import Root or Intermediate
- Import Existing Server Certificate

**Supported Interfaces:**
- REST
Common SSL Problems
Recent releases of Chrome have enforced the need for a subject alternative name.

Must be included with your CSR.
### How do you know you have an SSL Problem?

#### Log Analysis

<table>
<thead>
<tr>
<th>Level</th>
<th>URL</th>
<th>Message</th>
<th>Date</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Invalid SSL certificate found. PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target</td>
<td>2018-03-04T05:15:10,68</td>
<td>Sharing</td>
<td></td>
</tr>
</tbody>
</table>
Unable to perform analysis
Missing trust chain in portaladmin

- Add trust chain to portaladmin endpoint
Federation issues when using DNS aliases

URL Name Mismatch

- ArcGIS Enterprise creates self-signed certificates
- Federation with a DNS alias will succeed but…
  - you will get errors later
- Make sure Admin URL used in Federation matches Certificate Name (or SAN)
Key Takeaways

- SSL is about secure and encrypted communication

- SSL begins at the web tier, and extends to each ArcGIS Enterprise component which provides support for SSL
  - *Web tier is easy, application tier takes some more work*...
Please Take Our Survey on the App

Download the Esri Events app and find your event

Select the session you attended

Scroll down to find the feedback section

Complete answers and select “Submit”