

# EXC08: SSL Certificates and Exchange The (Next) Final Word

Michael B. Smith

The Essential Exchange

[michael@TheEssentialExchange.com](mailto:michael@TheEssentialExchange.com)



# Who is Michael B.?

- Remember the B! 😊
  - And yes, that really is my name!
- Long-time Exchange guy
  - Since 1996 and Exchange 5.0
- Eight year Exchange MVP
- Consultant and migration expert
  - Exchange, Active Directory, System Center

# Do you do social media?

- Then



- <http://facebook.com/ExchangeConnections>
- Discussions, announcements, and conversations about this and future Exchange Connection events

# Agenda

- **A little history**
  - Exchange 2003, Exchange 2007
- **Some fun facts**
  - Self-signed certificates and Keysizes
  - Common Name
  - Subject Name
  - TLS
  - CRL
- **More fun stuff**

# A quick comment

- Only discussing Exchange 2010 here today
- If you bring Lync into the conversation, attempting to use common certificates, and or use wildcard certs for everything in Lync – things get complicated

# Certificates and Exchange 2003

- Each set of front-ends in an admin group required a separate name space
  - Optionally, could have many name spaces
    - Could duplicate vDirs in IIS for many name spaces on a single FE (used in hosting)
    - Or one per front-end
    - Or one per admin group
  - Most had separate namespace for RPC/HTTP
    - Now called Outlook Anywhere

# Certificates and Exchange 2007

- The bottom dropped out
- Potential need for many certificates
  - But only a single vDir per server
  - Led to the introduction of SAN certificates
  - Initial guidance was for MANY names to get added to a SAN certificate (more on this later)
  - Eventually led to “same as” Exchange 2010

# Certificates and Exchange 2010

- You need:
  - IIS
  - AutoDiscover
  - TLS (optional)
  - POP and/or IMAP (optional)
  - Legacy (during migration)
- So...
  - mail.example.com
  - autodiscover.example.com
  - legacy.example.com

# Common Name

- Looks somewhat like a distinguished name in Active Directory
  - But backwards
- Above anything else, if you expect the SSL provider to approve a Certificate Signing Request, the Organization (O=) must be right
- This means the registrant must match the Organization

# Common Name: #2

- In the case below, the registrant is Smith Consulting – the Organization must match

Registrant:  
Smith Consulting

1092 Wintergreen Lane  
Charlottesville, Virginia 22903  
United States

Registered through: GoDaddy.com, Inc. (<http://www.godaddy.com>)  
Domain Name: THEESSENTIALEXCHANGE.COM  
Created on: 15-Aug-06  
Expires on: 15-Aug-12  
Last Updated on: 15-Aug-11

Administrative Contact:  
Smith, Michael michael@smithcons.com  
Smith Consulting  
1092 Wintergreen Lane  
Charlottesville, Virginia 22903  
United States  
+1.4349840081

## Common Name: #3

- The administrative and technical contacts will be sent an email to approve the certificate after initial check by provider
- For the prior registrant wanting a SSL certificate for “mail”, the CN may be:
  - C=US, O=Smith Consulting,  
CN=mail.theessentialexchange.com
- There are other potential segments, but C, O, and CN are most common

# Common Name: #4

- Other possible segments:
  - L = Locality (City)
  - S = State or Province
  - OU = Organizational Unit (division of company)
  - DC = domain component (typically only used with an internal certificate authority)

# Common Name: #5

- **Potential CN issues:**
  - Limited to 64 Unicode characters
  - If FQDN is longer, then the FQDN must be an alternate name
  - FQDN is limited to a subset of ASCII characters (upper, lower, numeric, hyphen, period)
  - Older versions of Outlook want the first alternate name to match the OA vDIR certificate

# Common Name: #6

- Internationalized Domain Names (IDNs)
  - Outlook has some support for IDNs
  - Exchange has some support for IDNs
  - Windows has some support for IDNs
  - Was not able to determine how this impacts Windows CA or New-ExchangeCertificate

# Subject Names

- **A rose by any other name:**
  - Subject Alternative Name (SAN) cert
  - Unified Communications Certificate (UCC)
- **An SSL certificate may have:**
  - Zero
  - One
  - Multiple
- **....alternate names**

## Subject Names: #2

- A certificate with zero alternate names:
  - Normal SSL certificate
- A certificate with one alternate name:
  - Probably also a normal SSL certificate
  - Some providers only provide SANs anymore
- Most providers charge different amounts for differing numbers of alternate names: 1-5, 6-10, 11-15, etc.

# Subject Names: #3

- What different services might you want to use an SSL certificate for in Exchange 2010?

- OWA
- IMAP
- EAS
- OA
- OAB
- Federation
- UM
- POP
- EWS
- ECP
- Autodiscover
- TLS

# Subject Names: #4

- You'll need these for internal and external
- For Exchange, wildcard works for almost everything, with a tiny bit of extra config:
  - Set-OutlookProvider EXPR
    - CertPrincipalName msstd:\*.example.com
- Not true for Lync
- Common certificate services in Exchange:
  - IMAP, POP, IIS, SMTP, UM (pre-SP1)
  - Outlook Anywhere

# Subject Names: #5

- By default, all IIS services grouped together:
  - OWA
  - EAS
  - EWS
  - UM (until sp1)
  - ECP
  - OAB

# Subject Names: #6

- Life is simpler on Exchange if your internal and external domains are the same
- Must import the original certificate on the same server your certificate request was created
- Then export it - including the private key - and import it everywhere else

# Subject Names: #7

- Be careful - some registrars limit the number of servers you can install a certificate upon
- This is a licensing limit - nothing in SSL implements that DRM
- Once you've installed a new certificate on Edge, enable for SMTP, resubscribe the server, reboot or restart Exchange ADAM services

# Subject Names: #8

## Best Practices for requesting CAS

- Local or NetBIOS name of the server
- All the accepted domain names for the org
- The FQDN for the server
- The Autodiscover FQDN for the domain
- The load-balanced identity of the server
- NetBIOS name and internal FQDN are not required - but considered a best practice so that you can use the names internally with no warnings

# Subject Names: #9

## Best Practices for requesting CAS

- So, for server “owa1” in external example.com domain, with internal domain of example.local, with load-balanced name of owa.example.com:
  - owa1
  - owa1.example.local
  - example.com
  - owa.example.com
  - autodiscover.example.com

# Subject Names: #10

## Best Practices for requesting CAS

- And, for server “owa2” in external example.com domain, with internal domain of example.local, with load-balanced name of owa.example.com:
  - owa2
  - owa2.example.local
  - example.com
  - owa.example.com
  - autodiscover.example.com

# Subject Names: #11

## Best Practices for requesting CAS

- But this is cr@p:
  - Leads to certificate proliferation. You can get by with:
    - owa.example.com
    - autodiscover.example.com
- Requires split DNS to work properly
- Internal load-balancing as well as external load-balancing
- Can't use internal server names

# Autodiscover FQDN

- Part of SAN, or
  - Separate virtual directories/IPs/etc., or
  - HTTP redirection, or
  - SRV (OL 2007 sp1 & above, domain joined)
- 
- AutodiscoverServiceInternalUri

# Certificate Revocation Checks

- `crl.microsoft.com` -- set to `127.0.0.1`
- Or in signed assemblies

```
<configuration>  
<runtime>  
<generatePublisherEvidence enabled="false"/>  
</runtime>  
</configuration>
```

- Increase the `ServicesPipeTimeout` value  
(to give the service more time to start).

A good value is 60000 or 90000

# Multi-site support

- Each site
  - Separate namespaces, at least for CAS
  - Plus a unique namespace to use as a fail-back URL in each site:
    - Mail-site1.example.com
    - Mail-site2.example.com
  - Set-OWAVirtualDirectory –FailBackURL <x>
  - All unique namespaces should be in SANs
  - Enable datacenter activation coordination (DAC) mode

# Transport Layer Security

- Exchange 2003 only supported direct TLS
- Exchange 2007/2010 support direct TLS and opportunistic TLS
- TLS is the “vNext” for SSL 3.0; uses modern SSL certificates
- Direct TLS is host-to-host
- Opportunistic is “can I do this, if so do it!”

## TLS: #2

- You add multiple names on your SMTP TLS certificates to support multiple direct partners per IP address
- The certificate name matching logic for the Domain Security (TLS) feature checks whether a domain name in the received certificate matches the domain name when it sends mail to that domain..

## TLS: #3

- For example purposes, consider a recipient domain, woodgrovebank.com. The matching logic searches through all DNS names on the certificates, and as long as one DNS name matches, the certificate is verified as a match for the specified domain.

# TLS: #4

- The matching logic accepts a certificate with an exact domain match (woodgrovebank.com)
- It also supports using wildcard character domain names in certificates so \*.woodgrovebank.com is accepted

## TLS: #5

- The matching logic also searches DNS one node deep. Therefore, mail1.woodgrovebank.com is also accepted as a match for woodgrovebank.com. However, DNS names more than two nodes deep are not accepted. Therefore, mail1.us.woodgrovebank.com, would not be accepted as a match

# TLS: #6

## Best Practices for requesting TLS

- **The FQDN of the server**
  - This may be different from the internal FQDN that is used between Edge Transport servers and Hub Transport servers and should match the A record that is published on the Internet (public) DNS server. This name should be entered as a CN in the SubjectName parameter of the New-ExchangeCertificate cmdlet.

# TLS: #7

## Best Practices for requesting TLS

- All the accepted domain names of the organization. Use the IncludeAcceptedDomain parameter of the New-ExchangeCertificate cmdlet for this.
- The FQDN for the connector if it is not covered by either of the previous items Use the DomainName parameter of the New-ExchangeCertificate cmdlet for this.

# Presentation Availability

- You can download the slides from here:
- [http://www.devconnections.com/updates/LasVegas\\_Fall11/Exchange](http://www.devconnections.com/updates/LasVegas_Fall11/Exchange)

# Your Feedback is Important

Please fill out a session evaluation form  
drop it off at the conference registration  
desk.

Thank you!