Securing SMTP Message Flow between different Exchange Server 2007 organizations

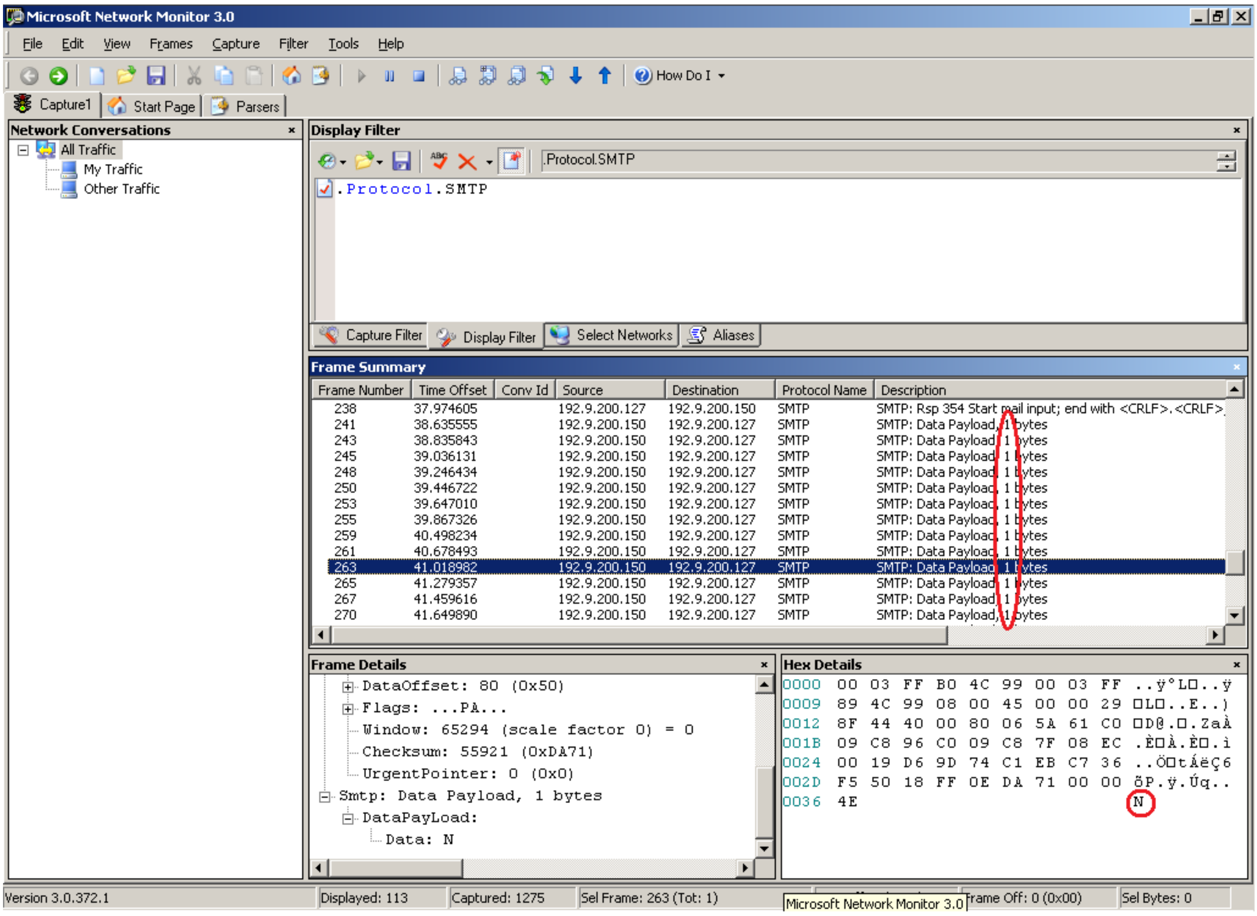
Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how how to secure SMTP message flow between Exchange Server 2007 in different Exchange organizations. Securing SMTP traffic between different Exchange 2007 organizations is much simpler as in previous versions of Exchange.

Basics

Is it nessessary to protect SMTP traffic between different Exchange Servers? Let’s make a simple test. Start a network trace with your favourite network. In this example I used Microsoft Network Monitor 3.0. After the trace is running start a Telnet session to your Exchange Server with port 25 and send a message over Telnet. Stop the network trace with Netmon and filter the captured traffic by the SMTP protocol. What do you see? Right, the whole authentication process of the SMTP session is cleartext.



```
.Protocol.SMTP
```

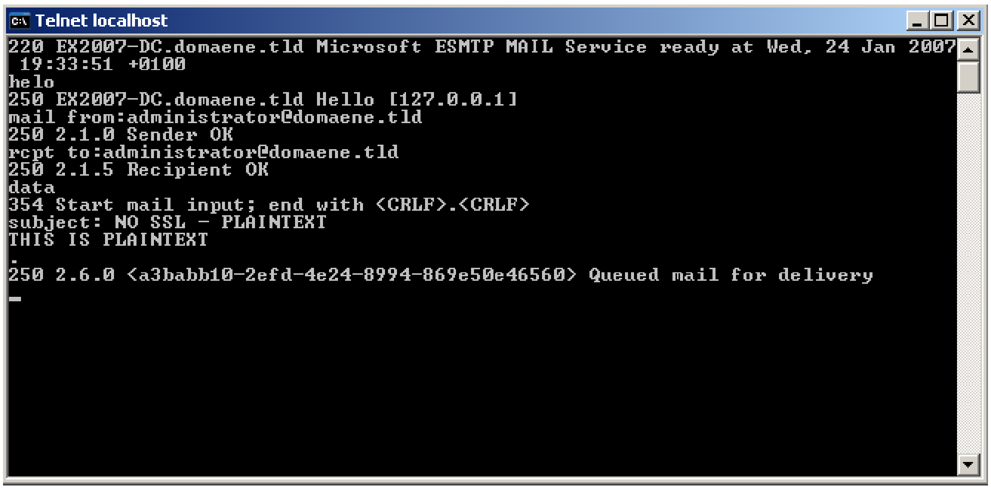
Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
238	37.974605		192.9.200.127	192.9.200.150	SMTP	SMTP: Rsp 354 Start mail input; end with <CRLF>.<CRLF>
241	38.635555		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
243	38.835843		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
245	39.036131		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
248	39.246434		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
250	39.446722		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
253	39.647010		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
255	39.867326		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
259	40.498234		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
261	40.678493		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
263	41.018982		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
265	41.279357		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
267	41.459616		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes
270	41.649890		192.9.200.150	192.9.200.127	SMTP	SMTP: Data Payload, 1 bytes

```
  DataOffset: 80 (0x50)
  Flags: ...PA...
  Window: 65294 (scale factor 0) = 0
  Checksum: 55921 (0xDA71)
  UrgentPointer: 0 (0x0)
Smtp: Data Payload, 1 bytes
  DataPayLoad:
    Data: N
```

```
0000  00 03 FF B0 4C 99 00 03 FF  ..ÿ°L□..ÿ
0009  89 4C 99 08 00 45 00 00 29  □L□..E..)
0012  8F 44 40 00 80 06 5A 61 C0  □D@.□.ZaÀ
001B  09 C8 96 C0 09 C8 7F 08 EC  .È□À.È□.ì
0024  00 19 D6 9D 74 C1 EB C7 36  ..Ö□tÁëÇ6
002D  F5 50 18 FF 0E DA 71 00 00  õP.ÿ.Úq..
0036  4E                          N
```

Version 3.0.372.1 | Displayed: 113 | Captured: 1275 | Sel Frame: 263 (Tot: 1) | Microsoft Network Monitor 3.0 | Frame Off: 0 (0x00) | Sel Bytes: 0

Figure 1: SMTP network trace with Netmon



```
220 EX2007-DC.domaene.tld Microsoft ESMTP MAIL Service ready at Wed, 24 Jan 2007
 19:33:51 +0100
helo
250 EX2007-DC.domaene.tld Hello [127.0.0.1]
mail from:administrator@domaene.tld
250 2.1.0 Sender OK
rcpt to:administrator@domaene.tld
250 2.1.5 Recipient OK
data
354 Start mail input; end with <CRLF>.<CRLF>
subject: NO SSL - PLAINTEXT
THIS IS PLAINTEXT
.
250 2.6.0 <a3babb10-2efd-4e24-8994-869e50e46560> Queued mail for delivery
_
```

Figure 2: Sending SMTP message via Telnet

OK, after we know that it is nessessary to implement some kind of more security between these Exchange Servers what is the right solution to do that? It is possible to use IPSEC between these Exchange servers but what does this mean in implementation work? At a minimum you have to use pre shared keys to implement IPSEC between these servers. This could be working well as long as you only have few Exchange Servers. Another solution implementing IPSEC between more than a handful servers are certificates but if you want to implement certificates between Exchange Servers you will need a PKI (Public Key Infrastructure).

Another solution securing SMTP traffic between these servers is new in Exchange Server 2007. You can use a built in function from Exchange Server 2007 to secure the SMTP traffic between Exchange 2007 servers in different Exchange Organizations.

Exchange Server 2007 uses several methods to ensure Message integrity and Message encryption.

- Mutual TLS
- Opportunistic TLS
- Direct Trust
- Domain Security

Mutual TLS

TLS (Transport Layer Security), the successor to Secure Sockets Layer (SSL) is used to encrypt message flow in Exchange Server 2007. The term Mutual means that both Exchange Servers that are envolved in the message Transport process will check the TLS certificate before the connection will be established. Mutual TLS is deloyed in a configuration where both the sender and the receiver authenticate one another before they send the data.

Opportunistic TLS

Opportunistic TLS is new to Exchange Server 2007. Exchange Server 2007 tries to secure the Message flow with other Exchange Servers or foreign messaging systems. Exchange Server 2007 tries to enable a TLS session with the other messaging system in form of an anonymous TLS request. This is different from Exchange Server 2003 where you must manually enable TLS between different Exchange Servers.

Direct Trust

All message traffic is automatically encrypted between Exchange Servers regardless if a Hub Transport or Edge Transport role will be used. Direct Trust doesn't use the complex X.509 certificate validation mechanism; instead it uses a direct validation in form of the presence of certificate in Active Directory. It doesn't matter if you will use self signed certificates or an internal Certificate Authority.

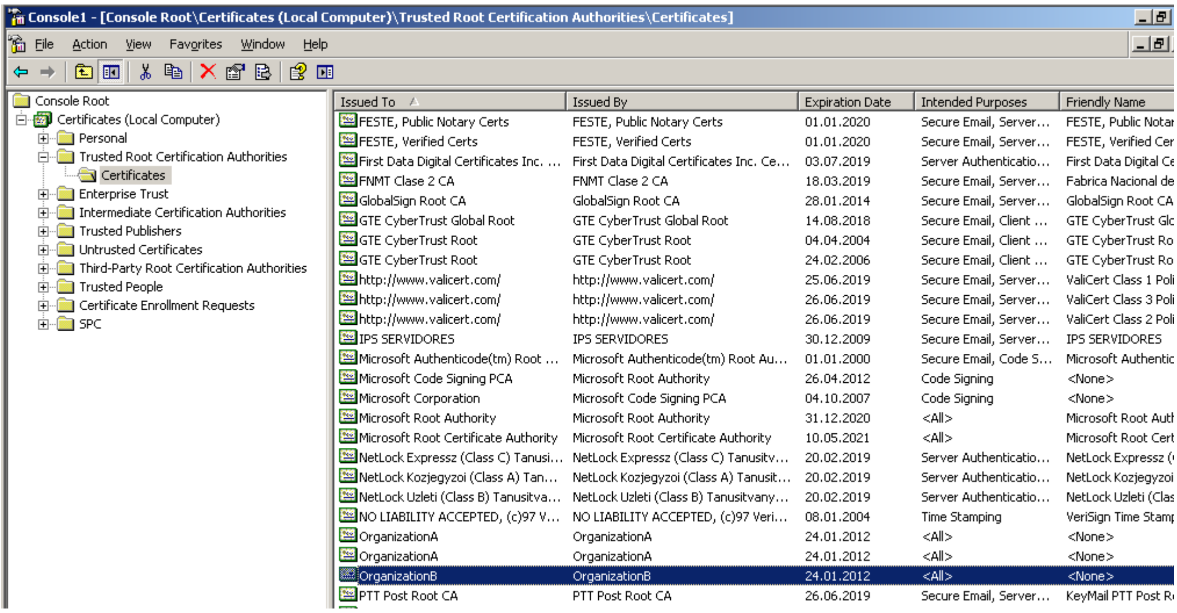
Domain Security

Domain Security is a combination of different techniques and features such as certificate Management, Exchange Server connector functionality and the behaviour of messaging clients like Microsoft Outlook 2007. The design goal of Domain Security with Exchange Server 2007 is also to establish a secure connection with mutual TLS.

Implementing TLS security

For the purpose of securing mailflow with mutual TLS you can use your Hub Transport servers or if you have implemented it you can use Exchange Servers with the Edge Server role.

As a first step you have to establish a certiticate cross Forest trust through the two Exchange organizations in this example. At a minimum you have to add the Root CA certificate from the external Certification authority (CA) to the trusted Root CA certificate store on the Hub Transport or Edge Transport Server. If you have multiple Edge- or Hub Transport Server it could be better implementing cross CA certificate trust or to add the Root CA certificate to the Trusted Root CA store via Group Policies. The following screenshot shows the Root CA certificate of OrganizationB.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Certificate Enrollment Requests
    - SPC

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
FESTE, Public Notary Certs	FESTE, Public Notary Certs	01.01.2020	Secure Email, Server…	FESTE, Public Notar
FESTE, Verified Certs	FESTE, Verified Certs	01.01.2020	Secure Email, Server…	FESTE, Verified Cer
First Data Digital Certificates Inc. …	First Data Digital Certificates Inc. Ce…	03.07.2019	Server Authenticatio…	First Data Digital Ce
FNMT Clase 2 CA	FNMT Clase 2 CA	18.03.2019	Secure Email, Server…	Fabrica Nacional de
GlobalSign Root CA	GlobalSign Root CA	28.01.2014	Secure Email, Server…	GlobalSign Root CA
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14.08.2018	Secure Email, Client …	GTE CyberTrust Glc
GTE CyberTrust Root	GTE CyberTrust Root	04.04.2004	Secure Email, Client …	GTE CyberTrust Ro
GTE CyberTrust Root	GTE CyberTrust Root	24.02.2006	Secure Email, Client …	GTE CyberTrust Ro
http://www.valicert.com/	http://www.valicert.com/	25.06.2019	Secure Email, Server…	ValiCert Class 1 Poli
http://www.valicert.com/	http://www.valicert.com/	26.06.2019	Secure Email, Server…	ValiCert Class 3 Poli
http://www.valicert.com/	http://www.valicert.com/	26.06.2019	Secure Email, Server…	ValiCert Class 2 Poli
IPS SERVIDORES	IPS SERVIDORES	30.12.2009	Secure Email, Server…	IPS SERVIDORES
Microsoft Authenticode(tm) Root …	Microsoft Authenticode(tm) Root Au…	01.01.2000	Secure Email, Code S…	Microsoft Authentic
Microsoft Code Signing PCA	Microsoft Root Authority	26.04.2012	Code Signing	<None>
Microsoft Corporation	Microsoft Code Signing PCA	04.10.2007	Code Signing	<None>
Microsoft Root Authority	Microsoft Root Authority	31.12.2020	<All>	Microsoft Root Auth
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	10.05.2021	<All>	Microsoft Root Cert
NetLock Expressz (Class C) Tanusi…	NetLock Expressz (Class C) Tanusitv…	20.02.2019	Server Authenticatio…	NetLock Expressz (
NetLock Kozjegyzoi (Class A) Tan…	NetLock Kozjegyzoi (Class A) Tanusit…	20.02.2019	Server Authenticatio…	NetLock Kozjegyzoi
NetLock Uzleti (Class B) Tanusitva…	NetLock Uzleti (Class B) Tanusitvany…	20.02.2019	Server Authenticatio…	NetLock Uzleti (Clas
NO LIABILITY ACCEPTED, (c)97 V…	NO LIABILITY ACCEPTED, (c)97 Veri…	08.01.2004	Time Stamping	VeriSign Time Stamp
OrganizationA	OrganizationA	24.01.2012	<All>	<None>
OrganizationA	OrganizationA	24.01.2012	<All>	<None>
OrganizationB	OrganizationB	24.01.2012	<All>	<None>
PTT Post Root CA	PTT Post Root CA	26.06.2019	Secure Email, Server…	KeyMail PTT Post R

Figure 3: Root CA certificate from the other Exchange Organization

Subject name

Subject Names plays an important part in certificates used by Exchange Server 2007. The subject Name of a TLS certificate is used by DNS aware services. A DNS aware service calls the subject name of a certificate and compares this name with a request. ISA Server is good example when publishing Outlook Web Access or Outlook Anywhere in a HTTPS briding scenario where the common name on the certificate must exactly match the name in the URL that is used to access OWA or Outlook Anywhere. The Subject Name field in a certificate binds a certificate to a single server or a special domain name.

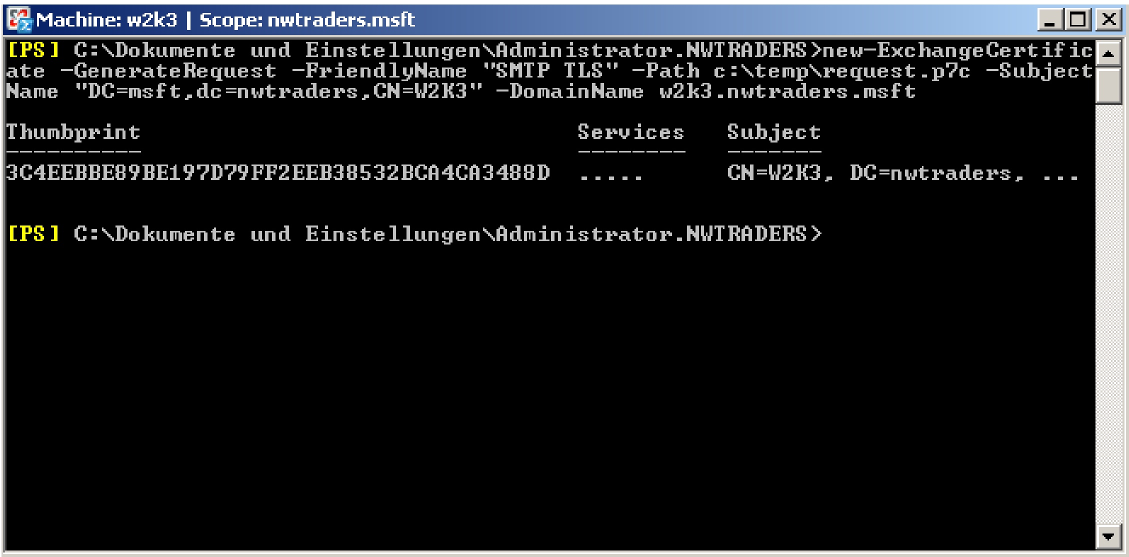
The following table give you an overview about the frequently used relative distinguished names also known as RDN.

Name	Abbreviation	Type	Max Size	Frequency\Max.\Recommended in certificate\request	Order in subject
Country/Region	C	ASCII	2	1\1	1
Domain Component	DC	ASCII	255	Many	1
State or Province	S	Unicode	128	1	2
Locality	L	Unicode	128	1	3
Organization	O	Unicode	64	11	4
Organizational Unit	OU	Unicode	64	Many\Many	5
Common Name	CN	Unicode	64	Many\1	6

Table 1: Commonly used Relative Distinguished Names

Request a certificate

The next step is to request a certificate via the Exchange Management Shell. The Certificate request file can be used to issue a certificate from the internal CA.



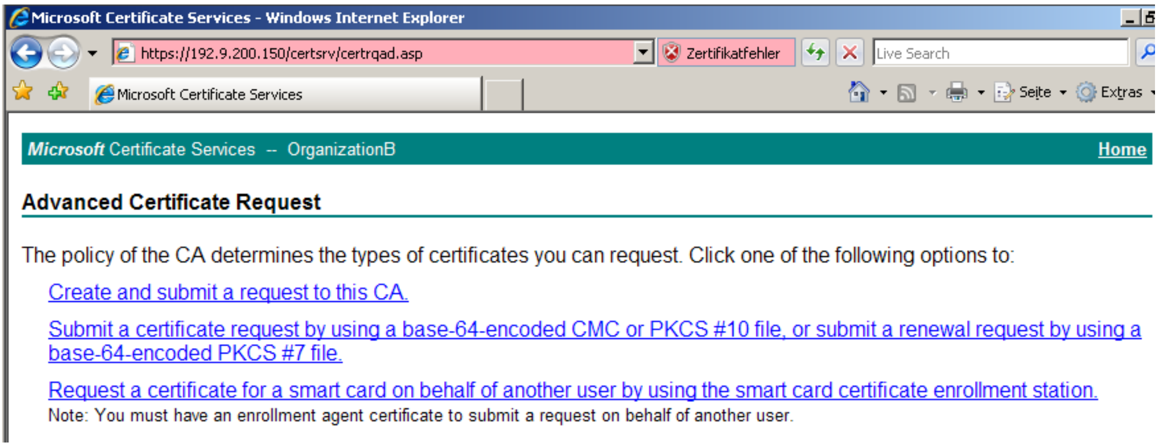
```
[PS] C:\Dokumente und Einstellungen\Administrator.NWTRADERS>new-ExchangeCertific
ate -GenerateRequest -FriendlyName "SMTP TLS" -Path c:\temp\request.p7c -Subject
Name "DC=msft,dc=nwtraders,CN=W2K3" -DomainName w2k3.nwtraders.msft

Thumbprint                                Services   Subject
----------                                --------   -------
3C4EEBBE89BE197D79FF2EEB38532BCA4CA3488D  .....      CN=W2K3, DC=nwtraders, ...


[PS] C:\Dokumente und Einstellungen\Administrator.NWTRADERS>
```

Figure 4: Request Exchange certificates

Open the CA webconsole ans submit a certiciate request by using a base-64 encoded CMC or PKCS#10 file.


Microsoft Certificate Services - Windows Internet Explorer
https://192.9.200.150/certsrv/certrqad.asp
Zertifikatfehler
Live Search
Microsoft Certificate Services
Seite
Extras

Microsoft Certificate Services -- OrganizationB **Home**

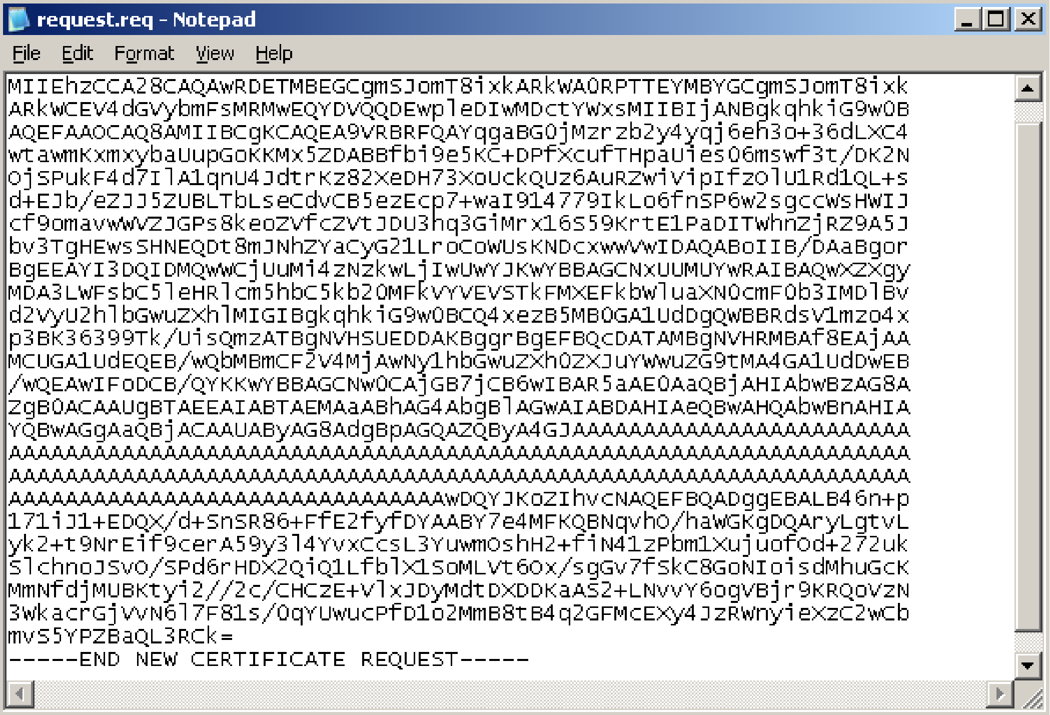
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- Create and submit a request to this CA.
- Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
  Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Figure 5: Enable the certificate with the webconsole

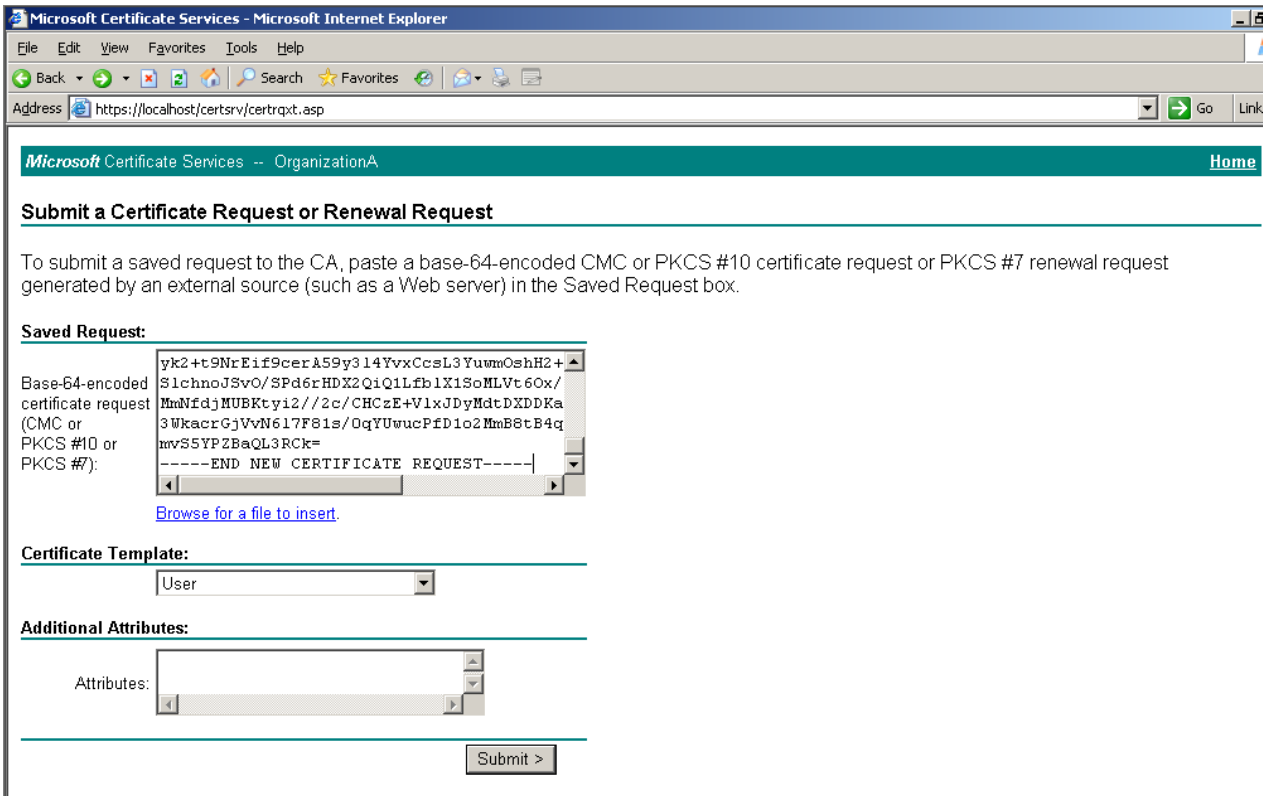
The following picture shows an example of the certificate request file. If your browser doesn't allow opening files, you can copy and paste the entire text from the request file into the certificate request section of the webconsole.



```
MIIEhzCCA28CAQAwRDETMBEGCgmSJomT8ixkARkWA0RPTTEYMBYGCgmSJomT8ixk
ARkWCEV4dGVybmFsMRMwEQYDVQQDEwpleDIwMDctYWxsMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA9VRBRFQAYqgaBG0jMzrzb2y4yqj6eh3o+36dLXC4
wtawmKxmxybaUupGoKKMx5ZDABBfbi9e5KC+DPfXcufTHpaUies06mswf3t/DK2N
ojSPukF4d7IlA1qnU4JdtrKz82XeDH73XoUckQUz6AuRZwiVipIfzolU1Rd1QL+s
d+EJb/eZJJ5ZUBLTbLseCdvCB5ezEcp7+waI914779IkLo6fnSP6w2sgcCWsHWIJ
cf9omavwWVZJGPs8keoZVfcZVtJDU3hq3GiMrx16S59KrtE1PaDITWhnZjRZ9A5J
bv3TgHEwsSHNEQDt8mJNhZYaCyG21LroCoWUsKNDcxwwVwIDAQABoIIB/DAaBgor
BgEEAYI3DQIDMQwWCjUuMi4zNzkwLjIwUWYJKWYBBAGCNxUUMUYwRAIBAQwXZXgy
MDA3LWFsbC5leHRlcm5hbC5kb20MFkVYVEVSTkFMXEFkbWluaXN0cmF0b3IMDlBv
d2VyU2hlbGwuZXhlMIGIBgkqhkiG9w0BCQ4xezB5MB0GA1UdDgQWBBRdsV1mzo4x
p3BK36399Tk/UisQmzATBgNVHSUEDDAKBggrBgEFBQcDATAMBgNVHRMBAf8EAjAA
MCUGA1UdEQEB/wQbMBmCF2V4MjAwNy1hbGwuZXh0ZXJuYWwuZG9tMA4GA1UdDwEB
/wQEAwIFoDCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8A
ZgB0ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIA
YQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByA4GJAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAWDQYJKoZIhvcNAQEFBQADggEBALB46n+p
171iJ1+EDQX/d+SnSR86+FfE2fyfDYAABY7e4MFKQBNqvhO/haWGKgDQAryLgtvL
yk2+t9NrEif9cerA59y3l4YvxCcsL3YuwmOshH2+fiN41zPbm1XujuofOd+272uk
SlchnoJSvO/SPd6rHDX2QiQ1LfblX1SoMLVt6Ox/sgGv7fSkC8GoNIoisdMhuGcK
MmNfdjMUBKtyi2//2c/CHCzE+VlxJDyMdtDXDDKaAS2+LNvvY6ogVBjr9KRQoVzN
3WkacrGjVvN6l7F81s/0qYUwucPfD1o2MmB8tB4q2GFMcEXy4JzRwnyieXzC2wCb
mvS5YPZBaQL3RCk=
-----END NEW CERTIFICATE REQUEST-----
```

Figure 6: The certificate request file

Submit the certificate request


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://localhost/certsrv/certrqxt.asp
Go Links
Microsoft Certificate Services -- OrganizationA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
yk2+t9NrEif9cerA59y3l4YvxCcsL3YuwmOshH2+
SlchnoJSvO/SPd6rHDX2QiQ1Lfb1X1SoMLVt6Ox/
MmNfdjMUBKtyi2//2c/CHCzE+VlxJDyMdtDXDDKa
3WkacrGjVvN6l7F81s/OqYUwucPfD1o2MmB8tB4q
mvS5YPZBaQL3RCk=
-----END NEW CERTIFICATE REQUEST-----
```

Browse for a file to insert.

Certificate Template:

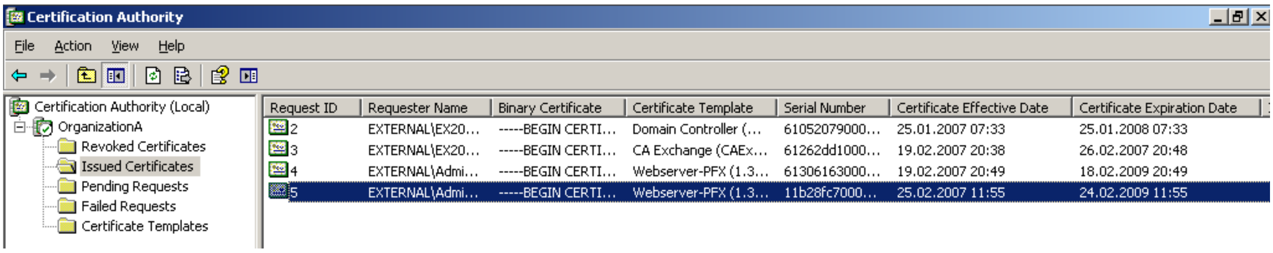
User

Additional Attributes:

Attributes:

Figure 7: Submit the Certificate request

In the following screenshot you will see the issued certificates from the internal Certificate Authority.



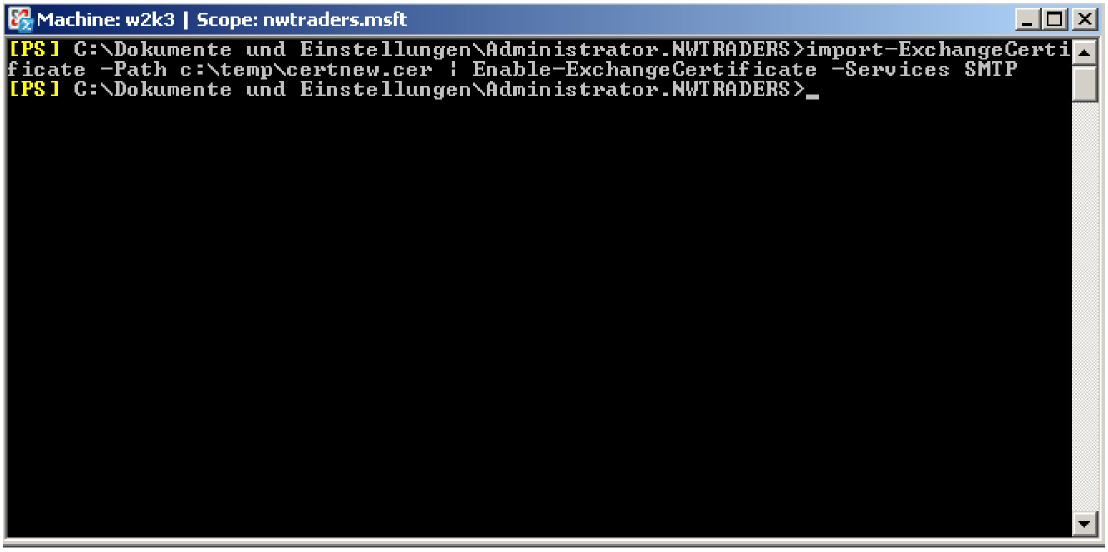
Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
2	EXTERNAL\EX20...	-----BEGIN CERTI...	Domain Controller (...	61052079000...	25.01.2007 07:33	25.01.2008 07:33
3	EXTERNAL\EX20...	-----BEGIN CERTI...	CA Exchange (CAEx...	61262dd1000...	19.02.2007 20:38	26.02.2007 20:48
4	EXTERNAL\Admi...	-----BEGIN CERTI...	Webserver-PFX (1.3...	61306163000...	19.02.2007 20:49	18.02.2009 20:49
5	EXTERNAL\Admi...	-----BEGIN CERTI...	Webserver-PFX (1.3...	11b28fc7000...	25.02.2007 11:55	24.02.2009 11:55

Figure 8: Issued certificates

Import the Certificate

It is important that you use the Exchange Management Shell to import the Certificate.

Import-ExchangeCertificate -Path c:\certificates\import.pfx | *Enable-ExchangeCertificate -Services SMTP*

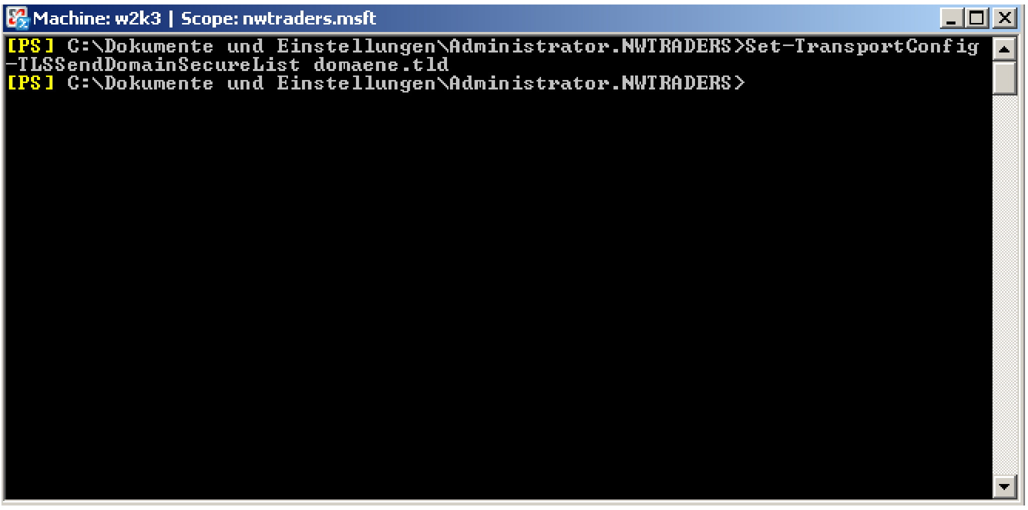


```
[PS] C:\Dokumente und Einstellungen\Administrator.NWTRADERS>import-ExchangeCerti
ficate -Path c:\temp\certnew.cer | Enable-ExchangeCertificate -Services SMTP
[PS] C:\Dokumente und Einstellungen\Administrator.NWTRADERS>_
```

Figure 9: Import the Certiciate into Exchange

Allow the Domain domaene.tld for as a secure Domain list with the Exchange Management Shell

Set-TransportConfig -TLSReceiveDomainSecureList domaene.tld

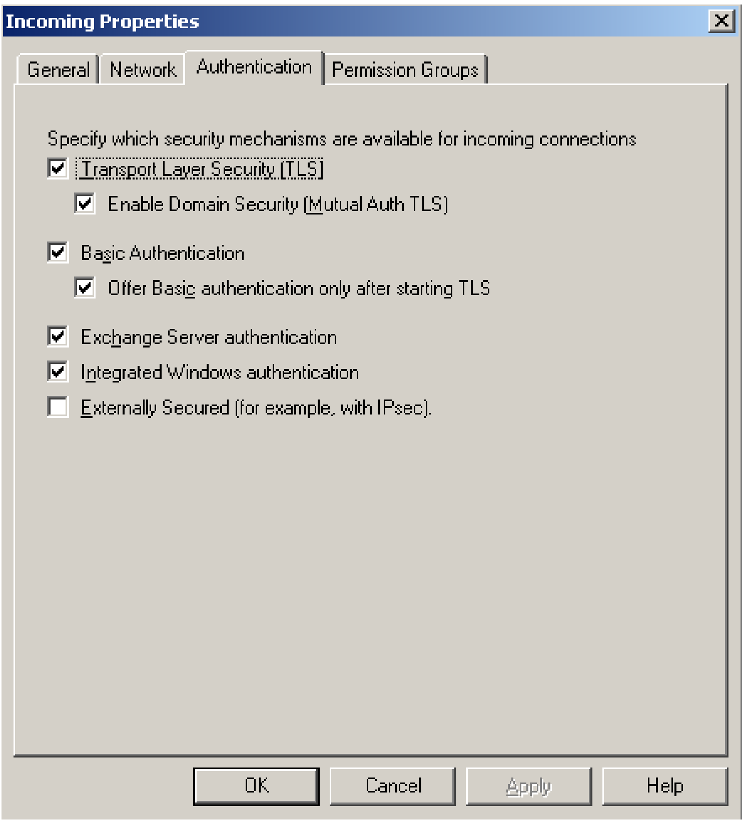


```
[PS] C:\Dokumente und Einstellungen\Administrator.NWTRADERS>Set-TransportConfig
-TLSSendDomainSecureList domaene.tld
[PS] C:\Dokumente und Einstellungen\Administrator.NWTRADERS>
```

Figure 10: Enable Domain Secure List

Enabling Domain Security on the SMTP Send Connector named “Outbound”

Set-SendConnector Outbound -DomainSecureEnabled:$True



Specify which security mechanisms are available for incoming connections

☑ Transport Layer Security (TLS)

☑ Enable Domain Security (Mutual Auth TLS)

☑ Basic Authentication

☑ Offer Basic authentication only after starting TLS

☑ Exchange Server authentication

☑ Integrated Windows authentication

□ Externally Secured (for example, with IPsec).

Figure 11: Enable Domain Security with TLS in the Exchange Management Console

Enabling Domain Security on the SMTP Receive Connector named “Inbound”

Set-ReceiveConnector Inbound -DomainSecureEnabled:$True -AuthMechanism TLS

Please note:

E-Mail messages that have been successful delivered through the domain secured mail flow connection are displayed in Outlook 2007 as "Domain Secure" messages.

Conclusion

As you have seen in this article it isn’t complicated implementing secure SMTP messaging between Exchange 2007 servers in different Exchange 2007 organizations and you don’t need a complicated solution like implementing IPSEC between these Servers.

Related Links

Implementing Domain Security for Exchange Server 2007
http://technet.microsoft.com/en-us/library/ea756304-4e1a-49b2-95ae-511af8540830.aspx