COMTARSIA

Architekturübersicht SSL-Zertifikate

Comtarsia SignOn Solution 2006 / 2008

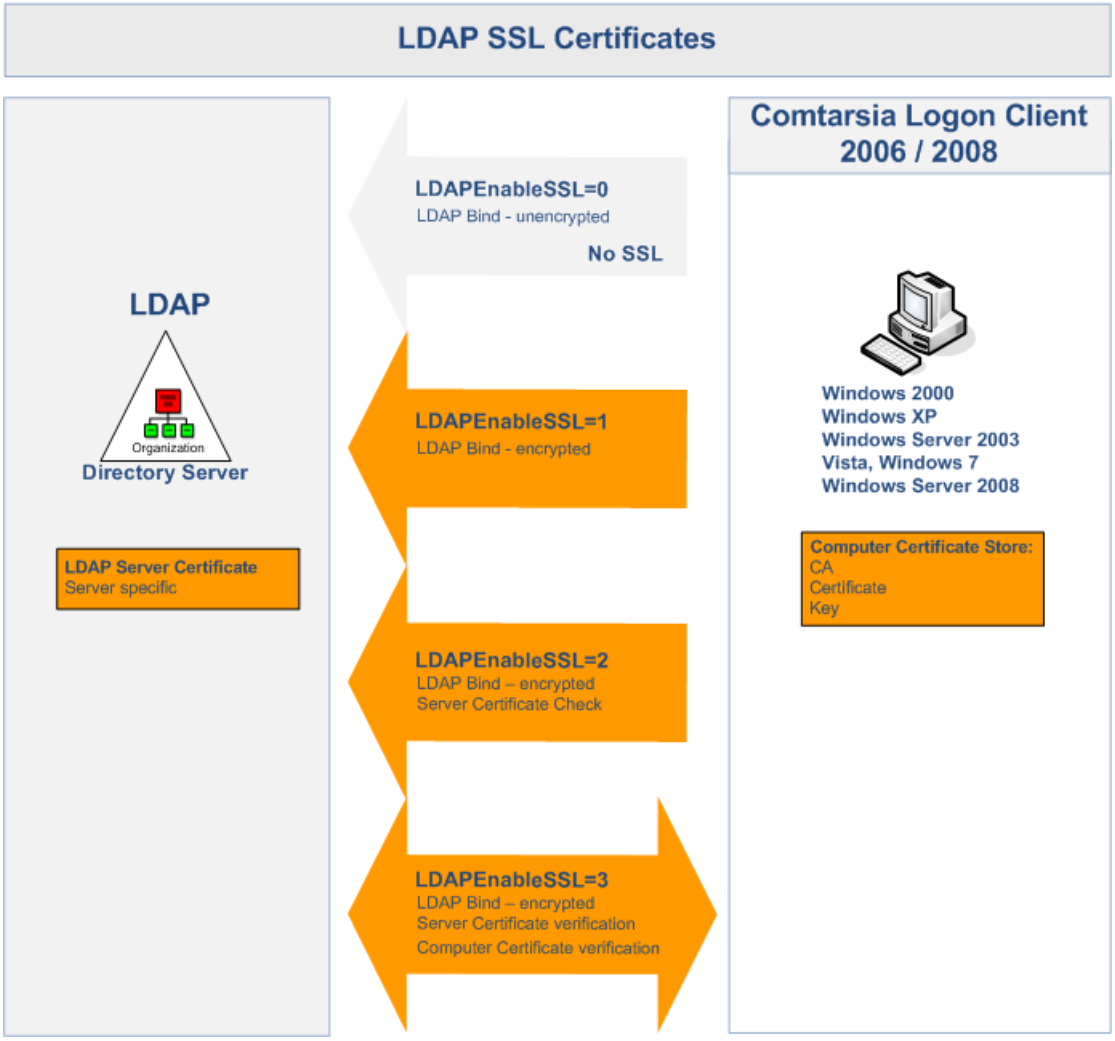
Comtarsia Logon Client 2006, Build 4.1.65.4
Comtarsia Logon Client 2008, Build 5.0.16.4
Comtarsia SignOn Gate 2006 Build 1.2.44.4

April 2010

Inhaltsverzeichnis

1. LDAP Zertifikate

1.1 Comtarsia Logon Client 2006 / 2008



Folgende Schlüssel und Zertifikate kommen bei der Kommunikation zwischen Comtarsia Logon Client und dem LDAP Server zum Einsatz.
Die Tabelle beschreibt die Quelle der Schlüssel/Zertifikate:

	CLC 2006/2008	*LDAP Server*
CA-Zertifikat	Computer CertStore	server spezifisch
Benutzer/Computer-Zertifikat	Computer CertStore	server spezifisch
Benutzer/Computer-Schlüssel	Computer CertStore	server spezifisch

1.1.1 Auswirkung der CLC 2006/2008 Konfiguration:

LDAPEnableSSL=0 „kein SSL“
Die gesamte Kommunikation des Clients mit dem LDAP Server findet unverschlüsselt statt. Diese Option eignet sich nur für den Testbetrieb und sollte keinesfalls in Produktionsumgebungen eingesetzt werden.

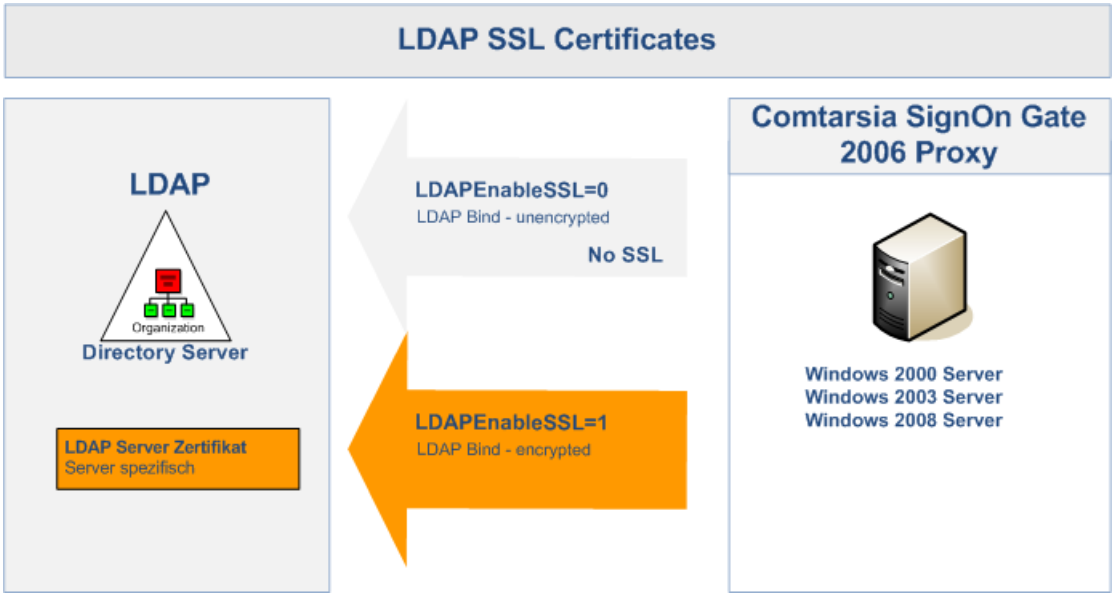
LDAPEnableSSL= 1 „ SSL without trusted server certificates"
Die Kommunikation mit dem LDAP Server wird verschlüsselt.
Das Zertifikat des Servers wird nicht überprüft und auch der Client benötigt kein Zertifikat.

LDAPEnableSSL= 2 “SSL with trusted server certificates"
Der Logon Client überprüft das Zertifikat des LDAP Servers. Für diese Option muss ein das „CA“-Zertifikat der CA welche das LDAP-Server Zertifikat ausgestellt hat in den Trusted Root CA's Container des Computer Stores eingespielt sein.

LDAPEnableSSL = “3 SSL with trusted client certificates"
Der Logon Client überprüft das Zertifikat des LDAP Servers (wie 2) und übermittelt ein eigenes (Computerzertifikat) an den Server. Diese Option benötigt sowohl ein „CA“- als auch ein „Client“-Zertifikat.
Das Client Zertifikat muss sich im My-Container des Computer Certificate Store befinden. Die Auswahl des Computerzertifikates erfolgt über eine Suche nach einem Zertifikat im Computer Certificate Store welches den Computername (%COMPUTERNAME%) beinhaltet.

LDAPServerCertificateFlags=0
(Nur Comtarsia Logon Client 2006)
Hiermit können Flags an die Windows Crypto-API Funktion “CertGetCertificateChain” übergeben werden.
Im speziellen kann hiermit die Art der CRL-Überprüfung festgelegt werden.
Mögliche Werte sind:
0x10000000: Revocation checking is done on the end certificate and only the end certificate.
0x20000000: Revocation checking is done on all of the certificates in every chain.
0x40000000: Revocation checking is done on all certificates in all of the chains except the root certificate.
0x80000000: Revocation checking only accesses cached URLs.

1.2 SignOn Proxy 2006



Folgende Schlüssel und Zertifikate kommen bei der Kommunikation zwischen Comtarsia SignOn Proxy und dem LDAP Server zum Einsatz.
Die Tabelle beschreibt die Quelle der Schlüssel/Zertifikate:

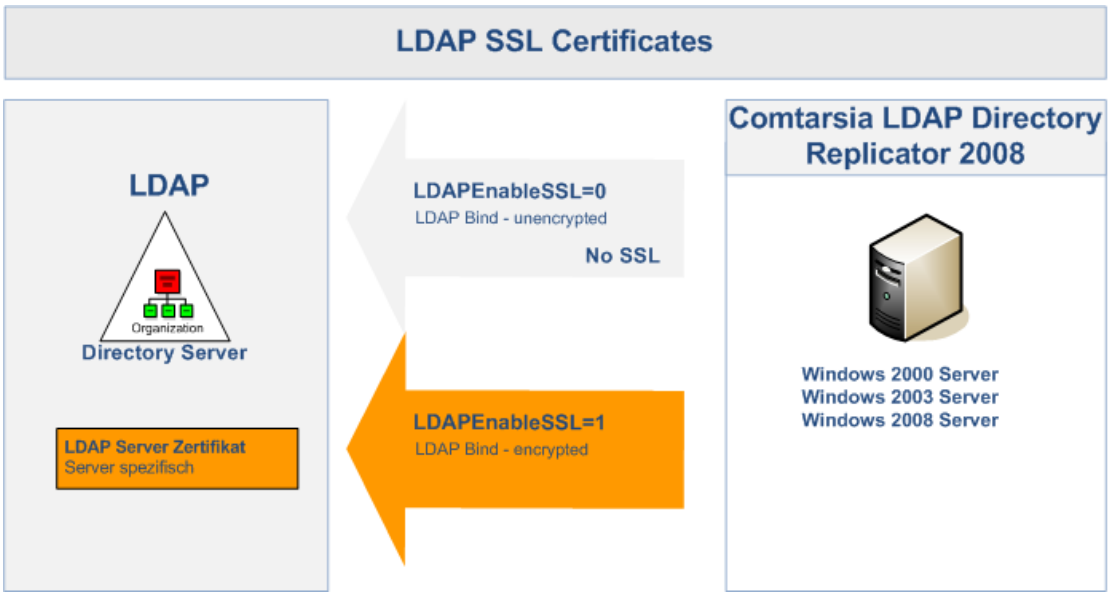
	SignOn Proxy 2006	*LDAP Server*
CA-Zertifikat	-	server spezifisch
Benutzer/Computer-Zertifikat	-	server spezifisch
Benutzer/Computer-Schlüssel	-	server spezifisch

1.2.1 Auswirkung der SignOn Proxy 2006 Konfiguration:

LDAPEnableSSL=0 „kein SSL"
Die gesamte Kommunikation des Clients mit dem LDAP Server findet unverschlüsselt statt. Diese Option eignet sich nur für den Testbetrieb und sollte keinesfalls in Produktionsumgebungen eingesetzt werden.

LDAPEnableSSL= 1 „ SSL without trusted server certificates"
Die Kommunikation mit dem LDAP Server wird verschlüsselt.
Das Zertifikat des Servers wird nicht überprüft und auch der Proxy benötigt kein Zertifikat.

1.3 LDAP Directory Replicator 2006



Folgende Schlüssel und Zertifikate kommen bei der Kommunikation zwischen LDAP Directory Replicator und den LDAP Server zum Einsatz.
Die Tabelle beschreibt die Quelle der Schlüssel/Zertifikate:

	LDAP Directory Replicator 2006	*LDAP Server*
CA-Zertifikat	-	server spezifisch
Benutzer/Computer-Zertifikat	-	server spezifisch
Benutzer/Computer-Schlüssel	-	server spezifisch

1.3.1 Auswirkung der LDR 2006 Konfiguration

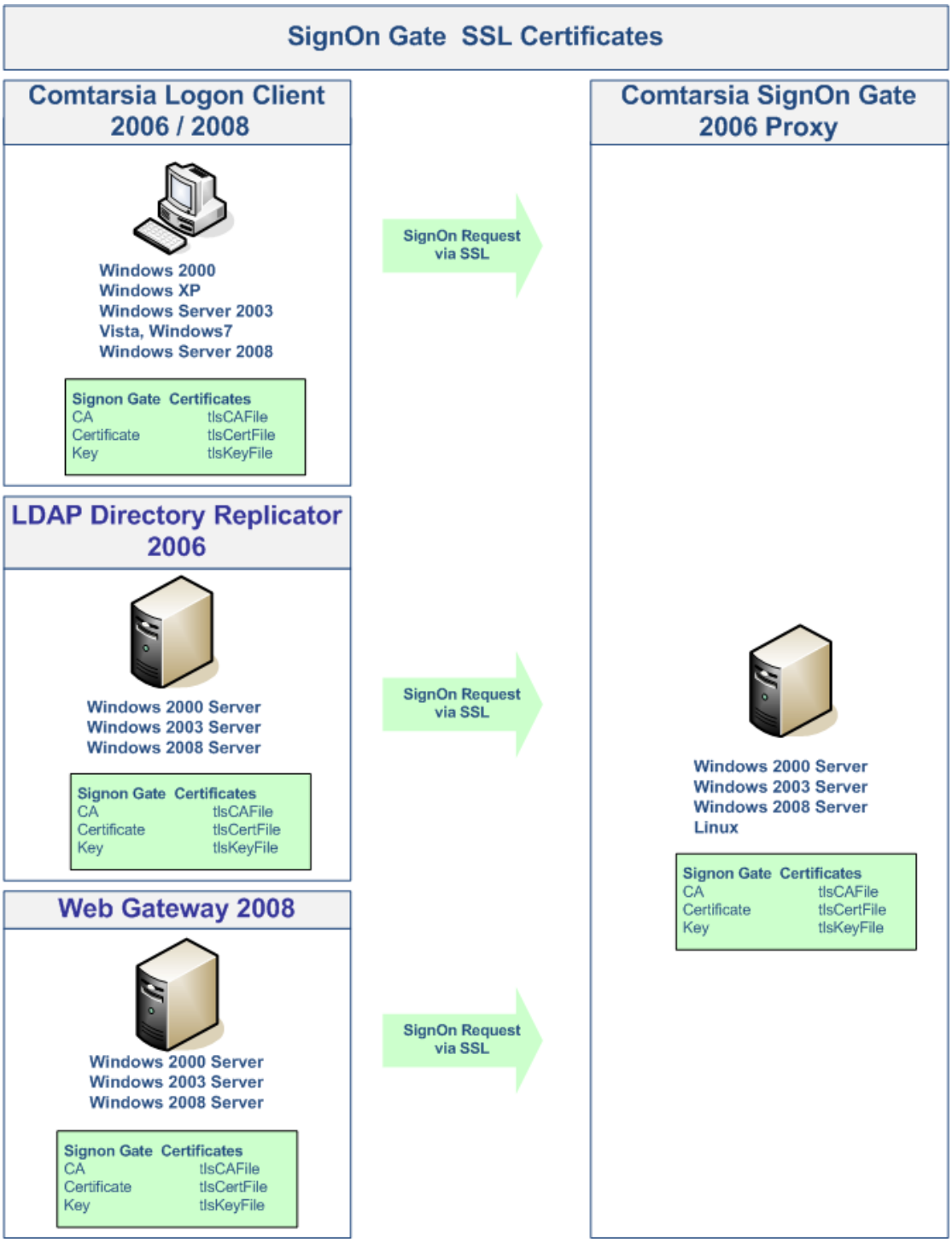
LDAPEnableSSL=0 „kein SSL"
Die gesamte Kommunikation des Clients mit dem LDAP Server findet unverschlüsselt statt. Diese Option eignet sich nur für den Testbetrieb und sollte keinesfalls in Produktionsumgebungen eingesetzt werden.

LDAPEnableSSL= 1 „ SSL without trusted server certificates"
Die Kommunikation mit dem LDAP Server wird verschlüsselt.
Das Zertifikat des Servers wird nicht überprüft und auch der LDR benötigt kein Zertifikat.

2. SignOn Gate Zertifikate

Der SignOn Proxy 2006 und der SignOn Agent 2006 haben die Möglichkeit Informationen zu den eigenen, als auch von aktzeptierten Zertifikaten in die LogDatei zu schreiben.
Hierfür müssen folgende Registry Werte gesetzt werden:
SignOn Agent:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOA_SYS_2006\LOG\
SignOn Proxy:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOP_2006\Log
Wert: logCertInfo=(REG_DWORD, default:0 - deaktiviert) 1 = aktiviert.
Dieser Wert sollte nur zum Testen bzw. zur Fehlersuche aktiviert werden.

2.1 CLC 2006/CLC 2008/LDR 2006/Web Gateway 2008 <-> SignOn Proxy 2006



Der Comtarsia Logon Client 2006/2008, der LDAP Directory Replicator 2006 und das Web Gateway 2008 werden bei der Kommunikation mit dem Comtarsia SignOn Gate Proxy 2006 als "SignOn Gate Clients" betrachtet.

Folgende Schlüssel und Zertifikate kommen bei der Kommunikation zwischen SingOn Gate Clients und den LDAP Server zum Einsatz.
Die Tabelle beschreibt die Quelle der Schlüssel/Zertifikate:

	SignOn Gate Clients	*SignOn Gate Proxy*
CA-Zertifikat	tlsCAFile	tlsCAFile
Benutzer/Computer-Zertifikat	tlsCertFile	tlsCertFile
Benutzer/Computer-Schlüssel	tlsKeyFile	tlsKeyFile

2.1.1 Zertifikate der Clients:

Die Zertifikate müssen im Base-64-ecoded X.509 Format gespeichert sein.
Der Pfad zu den Zertifikaten (und Private Key) (Werte: tlsCAFile, tlsCertFile, tlsKeyFile) ist in folgenden Registry Keys der Clients zu konfigurieren:

Comtarsia Logon Client 2006:
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\ComSyncClient]

Comtarsia Logon Client 2008:
[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\SyncClient]
Konfigurator: SyncClient-Tab

Comtarsia LDAP Directory Replicator 2006:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtLDR_2006\Replicator\Proxies\<ProxyName>]
Konfigurator: Proxies-Tab

Comtarsia WebGateway 2008:
[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\Web Gateway 2008\Proxies\<ProxyName>]
Konfigurator: Proxies-Tab

Die Zertifikate müssen die extended KeyUsage "id_kp_clientAuth (OID: 1.3.6.1.5.5.7.3.2)" gesetzt haben um vom SignOn Proxy akzeptiert zu werden.

Optional, (wenn trustOption "CERT_OIDS" am SignOn Proxy aktiviert) muss auch die extended KeyUsage "Comtarsia LogonClient (OID: 1.3.6.1.4.1.13823.1.3.3)" gesetzt sein um akzeptiert zu werden.

Optional, (wenn trustOption "CERT_FQDN" am SignOn Proxy aktiviert) muss der Common Name (CN) des Zertifikates des jeweiligen Clients mit dem Hostnamen des Clients übereinstimmen (bedeutet dass jeder Client ein eigenes Zertifikat benötigt).

2.1.2 Zertifikat des SignOn Proxy 2006:

Die Zertifikate müssen im Base-64-ecoded X.509 Format gespeichert sein.
Der Pfad zu den Zertifikaten (und Private Key) (Werte: tlsCAFile, tlsCertFile, tlsKeyFile) ist in der Registry im folgenten Registry Key zu konfigurieren:

Comtarsia SignOn Proxy 2006:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOP_2006\Parameter]

Das Zertifikat muss die extended KeyUsage "id_kp_clientAuth (OID: 1.3.6.1.5.5.7.3.2)" und "id_kp_serverAuth (OID: 1.3.6.1.5.5.7.3.1)" gesetzt haben. id_kp_serverAuth um von den Clients als Server akzeptiert zu werden und id_kp_clientAuth um vom SignOn Agent als Client akzeptiert zu werden.

Optional, (wenn trustOption "CERT_OIDS" auf mindesten 1 der Clients aktiviert) muss auch die extended KeyUsage "Comtarsia SignOn Proxy (OID: 1.3.6.1.4.1.13823.1.3.2)" gesetzt sein um akzeptiert zu werden.

Optional, (wenn trustOption "CERT_FQDN" auf mindesten 1 der Clients aktiviert) muss der Common Name (CN) des Zertifikates mit dem Hostnamen des SignOn Proxy übereinstimmen.

2.1.3 Auswirkung auf die Konfiguration

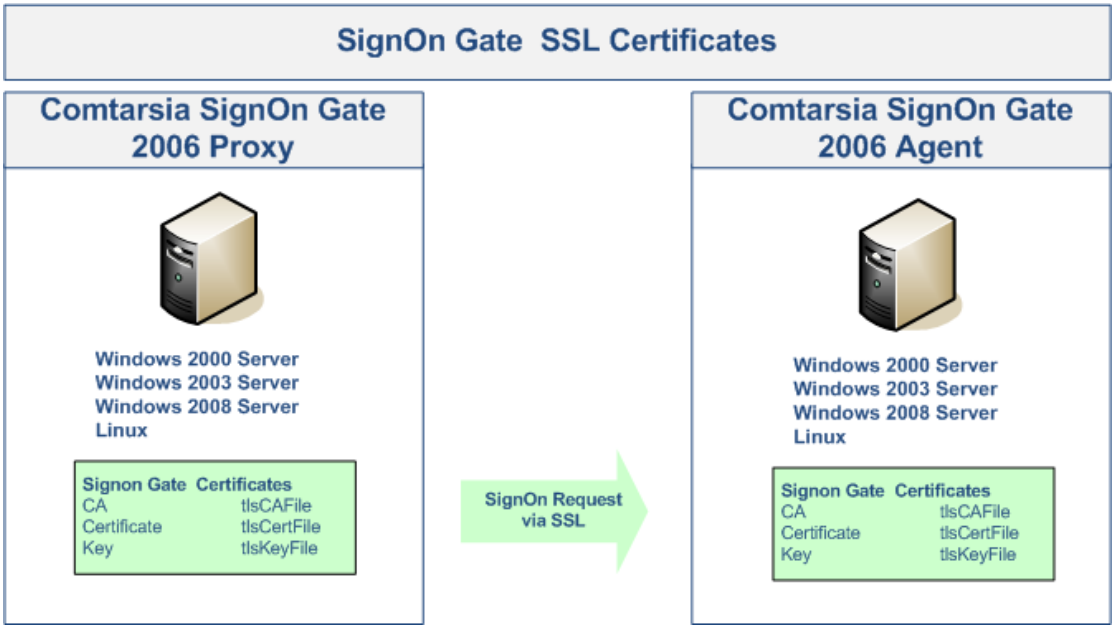
Auswirkung der Comtarsia Logon Client 2006, Comtarsia Logon Client 2008, Comtaris LDAP Replicator 2006 und der Comtarisa Web Gateway 2008 Konfiguration:

trustOptionsClient:0 (Siehe: trustOptions)
Bestimmt welche Anforderungen das Zertifikat der Gegenstelle erfüllen muss um als Vertrauenswürdig betrachtet zu werden.
Die folgenden trustOptions Flags können verwendet werden:
NO_CHECK, CERT_OIDS, CERT_FQDN.

Auswirkung der SignOn Proxy 2006 Konfiguration:

trustOptionsClient:0 (Siehe: trustOptions)
Bestimmt welche Anforderungen das Zertifikat der Gegenstelle erfüllen muss um als Vertrauenswürdig betrachtet zu werden.
Die folgenden trustOptions Flags können verwendet werden:
NO_CHECK, CERT_OIDS, CERT_FQDN.

2.2 SignOn Proxy 2006 <-> SignOn Agent 2006



Folgende Schlüssel und Zertifikate kommen bei der Kommunikation zwischen Comtarsia Logon Client und den LDAP Server zum Einsatz.
Die Tabelle beschreibt die Quelle der Schlüssel/Zertifikate:

	SignOn Gate Proxy	*SignOn Gate Agent*
CA-Zertifikat	tlsCAFile	tlsCAFile
Benutzer/Computer-Zertifikat	tlsCertFile	tlsCertFile
Benutzer/Computer-Schlüssel	tlsKeyFile	tlsKeyFile

2.2.1 Zertifikat des SignOn Proxy 2006

Der Pfad zu den Zertifikaten (und Private Key) (Werte: tlsCAFile, tlsCertFile, tlsKeyFile) ist in der Registry im folgenten Registry Key zu konfigurieren:
SignOn Proxy 2006[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOP_2006\Parameter]
Das Zertifikat muss die extended KeyUsage "id_kp_clientAuth (OID: 1.3.6.1.5.5.7.3.2)" und "id_kp_serverAuth (OID: 1.3.6.1.5.5.7.3.1)" gesetzt haben. id_kp_serverAuth um von den Clients als Server akzeptiert zu werden und id_kp_clientAuth um vom SignOn Agent als Client akzeptiert zu werden.

Optional, (wenn trustOption "CERT_OIDS" am SignOn Agent aktiviert) muss auch die extended KeyUsage "Comtarsia SignOn Proxy (OID: 1.3.6.1.4.1.13823.1.3.2)" gesetzt sein um akzeptiert zu werden.

Optional, (wenn trustOption "CERT_FQDN" am SignOn Agent aktiviert) muss der Common Name (CN) des Zertifikates mit dem Hostnamen des SignOn Proxy übereinstimmen.

Zertifikat des SignOn Agent 2006:
Der Pfad zu den Zertifikaten (und Private Key) (Werte: tlsCAFile, tlsCertFile, tlsKeyFile) ist in der Registry im folgenten Registry Key zu konfigurieren:

SignOn Proxy
2006[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOA_SYS_2006\CORE]

Das Zertifikat muss die extended KeyUsage "id_kp_serverAuth (OID: 1.3.6.1.5.5.7.3.1)" gesetzt haben um vom SignOn Proxy als Server akzeptiert zu werden.

Optional, (wenn trustOption "CERT_OIDS" am SignOn Proxy aktiviert) muss auch die extended KeyUsage "Comtarsia SignOn Agent (OID: 1.3.6.1.4.1.13823.1.3.1)" gesetzt sein um akzeptiert zu werden.

Optional, (wenn trustOption "CERT_FQDN" am SignOn Proxy aktiviert) muss der Common Name (CN) des Zertifikates mit dem Hostnamen des SignOn Agent übereinstimmen.

2.2.2 Auswirkung der Konfiguration

Auswirkung der Comtarsia Logon Client 2006/2008, Comtarsia LDAP Directory Replicator 2006 und Comtarsia 2008 Konfiguration:

trustOptionsServer:0 (Siehe: trustOptions)
Bestimmt welche Anforderungen das Zertifikat der Gegenstelle erfüllen muss um als Vertrauenswürdig betrachtet zu werden.
Die folgenden trustOptions Flags können verwendet werden:
NO_CHECK, CERT_OIDS, CERT_FQDN.

Auswirkung der SignOn Proxy 2006 Konfiguration:

trustOptionsServer:0 (Siehe: trustOptions)
Bestimmt welche Anforderungen das Zertifikat der Gegenstelle erfüllen muss um als Vertrauenswürdig betrachtet zu werden.
Die folgenden trustOptions Flags können verwendet werden:
NO_CHECK, CERT_OIDS, CERT_FQDN, ACCEPT_LIST.

2.2.3 trustOptions

trustOptions Flags:
0x000 NO_CHECK Keine Überprüfung
0x001 ACCEPT_LIST Vertrauensstellung anhand der IP-basierenden „Accept List“ (nur für SignOn Agent 2006)

0x002 CERT_OIDS Vertrauensstellung anhand von Zertifikat OIDs (siehe auch "Extended KeyUsage OIDs")
0x100 CERT_FQDN Überprüfung, ob das verwendete Zertifikat mit dem Hostnamen übereinstimmt.

Trustoptions Registry Parameter:
CLC 2006 (kommunikation mit Proxy:)
[HKEY_LOCAL_MACHINE\SOFTWARE\PCS\GINA\ComSyncClient]
trustOptionsClient=(default:0)<trustOptionsFlags>
Konfigurator: SignOn Gate-Tab:Trust Options

CLC 2008 (kommunikation mit Proxy:)
[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\SOSProfile 001\SyncClient]
trustOptionsClient=(default:0)<trustOptionsFlags>

LDR 2006 (kommunikation mit Proxy:)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtLDR_2006\Replicator\Proxies\<ProxyName>]
trustOptionsClient=(default:0)<trustOptionsFlags> Konfigurator: Proxies-Tab:Trust Options

WebGateway 2008 (kommunikation mit Proxy:)
[HKEY_LOCAL_MACHINE\SOFTWARE\Comtarsia\Web Gateway 2008\Proxies\<ProxyName>] trustOptionsClient=(default:0)<trustOptionsFlags>
Konfigurator: Proxies-Tab:Trust Options

SignOn Proxy 2006 (Kommunikation mit Clients:)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOP_2006\Parameter] trustOptionsClient=(default:0)<trustOptionsFlags>
Konfigurator: Security-Tab:Trust Options > Communication Client

SignOn Proxy 2006 (Kommunikation mit Agent:)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOP_2006\Parameter] trustOptionsServer=(default:0)<trustOptionsFlags>
Konfigurator: Security-Tab:Trust Options > Communication Proxy

SignOn Agent 2006 (kommunikation mit Proxy:)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ComtSOA_SYS_2006\CORE] trustOptionsServer=(default:0)<trustOptionsFlags>
Konfigurator: General-Tab:Trust Options

2.2.4 ExtendedKeyUsage OIDs

Comtarsia Comtarsia Logon Client Certificate:
1.3.6.1.4.1.13823.1.3.3 Comtarsia Logon Client-Certificate (optional) This is a Comtarsia specific OID for the "Comtarsia LogonClient"
1.3.6.1.5.5.7.3.2 id_kp_clientAuth (required) it's a "Client" for the SignOn Proxy

1.3.6.1.4.1.13823.1.3.3, 1.3.6.1.5.5.7.3.2

Comtarsia SignOn Proxy Certificate:

1.3.6.1.4.1.13823.1.3.2 Comtarsia Proxy-Certificate (optional) This is a Comtarsia specific OID for the "Comtarsia SignOn Proxy"
1.3.6.1.5.5.7.3.1 id_kp_serverAuth (required) it's a "Server" for the Logon Client
1.3.6.1.5.5.7.3.2 id_kp_clientAuth (required) it's a "Client" for the SignOn Agent

1.3.6.1.4.1.13823.1.3.2, 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2

Comtarsia SignOn Agent Certificate:
1.3.6.1.4.1.13823.1.3.1 Comtarsia Agent-Zertifikat (optional) This is a Comtarsia specific OID for the "Comtarsia SignOn Agent"
1.3.6.1.5.5.7.3.1 id_kp_serverAuth (required) it's a "Server" for the SignOn Proxy

1.3.6.1.4.1.13823.1.3.1, 1.3.6.1.5.5.7.3.1
---

3. Troubleshooting

3.1 LDAP Kommunikation

3.1.1 Comtarisa Logon Client 2006

Gutfall:

CLC 2006 - LDAP Server Bind OK: (CLC 2006: comt_ldap.log, LogLevel:Debug)

```
19.04.2010 10:19:16.209  <comt_ldap_connect:5:1216> --- comt_ldap_connect ---
.
.
.
19.04.2010 10:19:16.209  <comt_ldap_server_connect:5:1216> connecting to
mails.comtarsia.com:636 with ssl 2; pri: 0, weigth: 0
.
.
.
19.04.2010 10:19:16.365  <DisplayCertChainContext:5:1216> Certificate 0/0 [0x0/0x102]:
'C=AT, S=Some-State, L=Vienna, O=Comtarsia, OU=Test, CN=mails.comtarsia.com'
19.04.2010 10:19:16.365  <DisplayCertChainContext:5:1216> Certificate 0/1 [0x0/0x10C]:
'DC=com, DC=comtarsia, DC=adsdom1, CN=COMTARSIA ROOT CA 10'
.
.
.
19.04.2010 10:19:16.490  <comt_ldap_server_connect:5:1216> bind rc: 0
```

Beispiele von möglichen Fehlern:

Der CLC 2006 vertraut dem LDAP Server Zertifikat nicht (LDAP SSL Modus 2) da der Zertifizierungsstelle nicht vertraut wird (CERT_E_UNTRUSTEDROOT) (CLC 2006:comt_ldap.log, Loglevel:Debug)

```
15.04.2010 13:31:28.550  <DisplayCertChainContext:5:1348> Global TrustStatus
dwErrorStatus: 0x20, dwInfoStatus: 0x100
15.04.2010 13:31:28.550  <DisplayCertChainContext:5:1348> Certificate 0/0 [0x0/0x102]:
'C=AT, S=Some-State, L=Vienna, O=Comtarsia, OU=Test, CN=mails.comtarsia.com'
15.04.2010 13:31:28.550  <DisplayCertChainContext:5:1348> Certificate 0/1 [0x20/0x10C]:
'DC=com, DC=comtarsia, DC=adsdom1, CN=COMTARSIA ROOT CA 10'
15.04.2010 13:31:28.550  <DisplayWinVerifyTrustError::4:1348> Error 0x800b0109
(CERT_E_UNTRUSTEDROOT) returned by CertVerifyCertificateChainPolicy!
15.04.2010 13:31:28.550  <comt_connect_to_host::1:1348> failed to check server
certificate!
```

LDAP Server Nicht erreichbar: (CLC 2006:comt_ldap.log, Loglevel:Debug) (Zeitunterschied beachten)

```
19.04.2010 10:04:35.256  <comt_ldap_server_connect:5:288> connecting to
mails.comtarsia.com:636 with ssl 2; pri: 0, weigth: 0
19.04.2010 10:04:35.256  <comt_ldap_server_connect:5:288> timeout: 10 s
19.04.2010 10:04:35.256  <comt_ldap_server_connect:5:288> ldap_ssl_init done
19.04.2010 10:04:46.302  <comt_ldap_server_connect:1:288> ldap_open error, sslLastError:
1A
19.04.2010 10:04:46.381  <comt_ldap_server_connect:1:288> resolveSSLError(sslLastError):
'COMT_LDAP_ERROR_UNDEFINED'
19.04.2010 10:04:46.381  <comt_ldap_connect:5:288> server is not working rc: 26
```

3.1.2 Comtarisa Logon Client 2008

Gutfall:

CLC 2008 - LDAP bind ok (CLC 2008 / ComtRPCSrv.log / Loglevel:Detal MSG, Flags: LDAP und LDAP SSL) ("Executing LDAP query")

```
 2010.04.19 11:09:36.357 0B98:0BB4:00 <85:CCP:LDAPFunctions::userAuthenticate:38:S0:C0> -
---- LDAP START -----
.
.
.

2010.04.19 11:09:36.373 0B98:0BB4:00 <5:CCP:LDAPFunctions::userAuthenticate:321:S0:C0>
Connecting to LDAP: 'sles10sp2':636 (SSL: 1 / Type: 0 / Timeout: 10s), UserDN:
'uid=SCTEST2,ou=Users,dc=SLES10SP2DOM'
.
.
.
2010.04.19 11:09:36.545 0B98:0BB4:00 <5:CCP:LDAPFunctions::userAuthenticate:363:S0:C0>
Executing LDAP query: '(&(objectClass=Person)(uid=SCTEST2))', Query base:
'dc=SLES10SP2DOM', Scope: 2
```

Beispiele von möglichen Fehlern:

Der CLC 2008 vertraut dem LDAP Server Zertifikat nicht (LDAP SSL Modus 2) da der Zertifizierungsstelle nicht vertraut wird (CERT_E_UNTRUSTEDROOT)

```
2010.04.15 14:26:47.414 09A0:09EC:00
<85:CCP:Comt::CLDAP::LDAPGeneric::ConnectToLdapServer:4599:S0:C0> performing socket
connect...
2010.04.15 14:26:47.414 09A0:09EC:00
<85:CCP:Comt::CLDAP::LDAPGeneric::ConnectToLdapServer:4610:S0:C0> socket connect to LDAP
server done.
```

```
2010.04.15 14:26:47.460 09A0:09EC:00
<85:CCP:Comt::CLDAP::LDAPGeneric::DisplayCertChain:5622:S0:C0> Server subject: C=AT,
S=Some-State, O=Comtarsia, OU=Test, CN=sles10sp2.comtarsia.com
2010.04.15 14:26:47.460 09A0:09EC:00
<85:CCP:Comt::CLDAP::LDAPGeneric::DisplayCertChain:5639:S0:C0> Server issuer: DC=com,
DC=comtarsia, DC=adsdom1, CN=COMTARSIA ROOT CA 10
2010.04.15 14:26:58.367 09A0:09EC:00
<85:CCP:Comt::CLDAP::LDAPGeneric::DisplayWinVerifyTrustError:5822:S0:C0> Error
0x800b0109 (CERT_E_UNTRUSTEDROOT) returned by CertVerifyCertificateChainPolicy!
2010.04.15 14:26:58.367 09A0:09EC:00
<85:CCP:Comt::CLDAP::LDAPGeneric::comt_connect_to_host:1596:S0:C0> failed to check
server certificate!
```

Der CLC 2008 vertraut dem LDAP Server Zertifikat nicht (LDAP SSL Modus 2) da der Common Name (CN) des Zertifikates nicht mit dem Hostnamen übereinstimmt. (CERT_E_CN_NO_MATCH)

```
2010.04.15 14:51:01.070 0C48:0E00:00
<85:CCP:Comt::CLDAP::LDAPGeneric::ConnectToLdapServer:4599:S0:C0> performing socket
connect...
2010.04.15 14:51:01.085 0C48:0E00:00
<85:CCP:Comt::CLDAP::LDAPGeneric::ConnectToLdapServer:4610:S0:C0> socket connect to LDAP
server done.
2010.04.15 14:51:01.117 0C48:0E00:00
<85:CCP:Comt::CLDAP::LDAPGeneric::DisplayCertChain:5622:S0:C0> Server subject: C=AT,
S=Some-State, O=Comtarsia, OU=Test, CN=sles10sp2.comtarsia.com
2010.04.15 14:51:01.117 0C48:0E00:00
<85:CCP:Comt::CLDAP::LDAPGeneric::DisplayCertChain:5639:S0:C0> Server issuer: DC=com,
DC=comtarsia, DC=adsdom1, CN=COMTARSIA ROOT CA 10
2010.04.15 14:51:01.132 0C48:0E00:00
<85:CCP:Comt::CLDAP::LDAPGeneric::DisplayWinVerifyTrustError:5822:S0:C0> Error
0x800b010f (CERT_E_CN_NO_MATCH) returned by CertVerifyCertificateChainPolicy!
2010.04.15 14:51:01.148 0C48:0E00:00
<85:CCP:Comt::CLDAP::LDAPGeneric::comt_connect_to_host:1596:S0:C0> failed to check
server certificate!
```

3.1.3 Comtarsia SignOn Gate Proxy 2006

Gutfall:

SOP 2006 - LDAP Verbingung OK: (SOP 2006: comt_ldap.log, Loglevel:13)

```
19.04.2010 10:19:17.450  <LdapChkPwdPipe:5:4416> --- comt_ldap Flag 80 START ---
.
.
.
19.04.2010 10:19:17.470  <comt_ldap_server_connect:5:4416> Connecting to
mails.comtarsia.com:389 without ssl; pri: 0, weigth: 0
.
.
.
19.04.2010 10:19:17.570  <comt_ldap_sasl_bind:5:4416> rc: 0 errcode: 0 ''
19.04.2010 10:19:17.570  <comt_ldap_server_connect:5:4416> bind rc: 0
19.04.2010 10:19:17.570  <comt_ldap_server_connect:5:4416> comt_ldap_simple_bind_s done
19.04.2010 10:19:17.570  <comt_ldap_server_connect:5:4416> ldap_bind ok
```

3.2 Comtarsia SignOn Gate Kommunikation

3.2.1 Comtarsia SignOn Gate Client-> SignOn Proxy 2006

Gutfall:

CLC 2006 - SOP 2006 Verbingung OK: (CLC 2006: comtsyncclient.log):

```
2010.04.19 10:19:17.131 0654:03DC:00 <5:main:410:S0:C0> starting sync...
2010.04.19 10:19:17.131 0654:03DC:00 <5:main:429:S0:C0> SMem.getFlag: 100
2010.04.19 10:19:17.334 0654:03DC:00 <5:main:603:S0:C0> Connecting to:
192.168.2.101:2003
2010.04.19 10:19:18.021 0654:03DC:00 <5:main:697:S0:C0> sync done, time: 890
```

CLC 2008 - SOP 2006 Verbindung OK: (CLC 2008 / ComtRPCSrv.log):

```
2010.04.19 11:09:38.342 0B98:0BB4:00
<5:CCP:Comt::Prod::SOG::SyncClient::sendSyncPacket:224:S0:C0> Connecting to:
192.168.2.101:2003
2010.04.19 11:09:39.623 0B98:0BB4:00
<5:CCP:Comt::Prod::SOG::SyncClient::sendSyncPacket:332:S0:C0> Sync done, time: 2406 ms
```

SignOn Proxy 2006 akzeptiert das Client (CLC 2006/CLC 2008/WebGateway 2008/LDR 2006) Zertifikat:

```
19.04.2010  10:19:17:260 LISTENER   4948              ->
19.04.2010  10:19:17:260 LISTENER   4948              -> Connect from
192.168.2.183:1645 (Socket:448) accepted (Connection Nr:3).
19.04.2010  10:19:17:290 LOGIC3     6108  448         -> Peer certificate:
19.04.2010  10:19:17:290 LOGIC3     6108  448         -> Issuer:            CN =
COMTARSIA ROOT CA 10, DC = adsdom1, DC = comtarsia, DC = com
19.04.2010  10:19:17:290 LOGIC3     6108  448         -> Subject:           CN =
client.comtarsia.com, OU = Test, O = Comtarsia
19.04.2010  10:19:17:290 LOGIC3     6108  448         -> Extended key usage:
1.3.6.1.4.1.13823.1.3.3, 1.3.6.1.5.5.7.3.2
19.04.2010  10:19:17:290 LOGIC3     6108  448         -> Valid from / until: Nov 26
14:18:28 2008 GMT / Nov 20 12:32:28 2018 GMT
19.04.2010  10:19:17:290 LOGIC3     6108  448         -> Peer FQDN:         crxpsp3de
19.04.2010  10:19:17:290 LOGIC3     6108              -> TLS handshake completed
successfully (Socket:448)
```

Beispiele von möglichen Fehlern:

SignOn Proxy 2006 lehnt das Client (CLC 2006/CLC 2008/WebGateway 2008/LDR 2006) Zertifikat ab, da es die Extended KeyUsage OID für "Comtarsia Logon Client" nicht beinhaltet, der Proxy jedoch das CERT_OIDS Flag für trustOptionsClient aktiviert hat:

```
14.04.2010  13:50:44:107 LISTENER   4620              ->
14.04.2010  13:50:44:107 LISTENER   4620              -> Connect from
192.168.2.183:3555 (Socket:392) accepted (Connection Nr:1).
14.04.2010  13:50:44:147 LOGIC3     5208              ->
<2:Comt::Net::SSLSocketOpenSSL::verifyPeerCertificate:359:S0:C0><ProxyAgentComm::runImpl
:604> Peer certificate verification failed, OID '1.3.6.1.4.1.13823.1.3.3' not found!
```

```
14.04.2010  13:50:44:147 LOGIC3     5208                -> Exception occured. Proxy
response not sent to client: 127.0.0.1:3555 socket:392 (closing connection)
14.04.2010  13:50:44:147 LOGIC3     5208                -> Sync time: 30 ms for client:
```

SignOn Proxy 2006 lehnt das Client (CLC 2006/CLC 2008/WebGateway 2008/LDR 2006) Zertifikat ab, da es der Zertifikats Common Name (CN) nicht mit den Hostnamen des Clients übereinstimmt, der Proxy jedoch das CERT_FQDN Flag für trustOptionsClient aktiviert hat.:

```
14.04.2010  13:56:19:369 LISTENER   3084                ->
14.04.2010  13:56:19:369 LISTENER   3084                -> Connect from
192.168.2.183:1059 (Socket:392) accepted (Connection Nr:1).
14.04.2010  13:56:19:400 LOGIC1     1568                ->
<2:Comt::Net::SSLSocketOpenSSL::verifyPeerCertificate:340:S0:C0><ProxyAgentComm::runImpl
:604> Subject name (client.comtarsia.com) does not match peer FQDN (crxpsp3de)!
14.04.2010  13:56:19:400 LOGIC1     1568                -> Exception occured. Proxy
response not sent to client: 192.168.2.183:1059 socket:392 (closing connection)
14.04.2010  13:56:19:400 LOGIC1     1568                -> Sync time: 21 ms for client:
```

SignOn Proxy 2006 Startet nicht da das eingetragene tlsCAFile Zertifikat nicht gefunden werden konnte.

```
14.04.2010  14:03:48:275 THRD_CRTL   132                ->
14.04.2010  14:03:50:789 LISTENER   5472                ->
<2:Comt::Net::SSLSocketOpenSSL::setVerifyContext:97:S0:C0><ComListener::runImpl:211>
Error loading CA certificates 'sw2k3rootca.pem''(null)'!
14.04.2010  14:03:50:789 LISTENER   5472                -> Initialisation ERROR listener
terminates itself
14.04.2010  14:03:50:789 THRD_CRTL   132                -> Initialisation ERROR ComtSOP
terminates itself
```

SignOn Proxy 2006 lehnt das Client (CLC 2006/CLC 2008/WebGateway 2008/LDR 2006) Zertifikat ab, da es von einer nicht vertrauenswürdigen CA ausgestellt wurde. (zb: Proxy vertraut CA_A, client Zertifikate wurden jedoch von CA_B ausgestellt)

```
14.04.2010  14:07:23:705 LISTENER   3976                ->
14.04.2010  14:07:23:705 LISTENER   3976                -> Connect from
192.168.2.183:1102 (Socket:392) accepted (Connection Nr:1).
14.04.2010  14:07:23:725 LOGIC1     4816                ->
<2:Comt::Net::SSLSocketOpenSSL::postAccept:828:S0:C0><ProxyAgentComm::runImpl:604> Error
accepting SSL connection: 1!
14.04.2010  14:07:23:725 LOGIC1     4816                -> Exception occured. Proxy
response not sent to client: 192.168.2.183:1102 socket:392 (closing connection)
14.04.2010  14:07:23:725 LOGIC1     4816                -> Sync time: 10 ms for client:
```

SignOn Proxy 2006 lehnt das Client (CLC 2006/CLC 2008/WebGateway 2008/LDR 2006) Zertifikat ab, da es abgelaufen, oder noch nicht gültig ist.

```
14.04.2010  14:14:31:290 LISTENER   5624                ->
14.04.2010  14:14:31:290 LISTENER   5624                -> Connect from
192.168.2.183:1128 (Socket:392) accepted (Connection Nr:1).
14.04.2010  14:14:31:310 LOGIC1     1952                ->
<2:Comt::Net::SSLSocketOpenSSL::postAccept:828:S0:C0><ProxyAgentComm::runImpl:604> Error
accepting SSL connection: 1!
14.04.2010  14:14:31:310 LOGIC1     1952                -> Exception occured. Proxy
response not sent to client: 192.168.2.183:1128 socket:392 (closing connection)
14.04.2010  14:14:31:310 LOGIC1     1952                -> Sync time: 10 ms for client:
```

Der Client lehnt das SignOn Proxy Zertifikat ab da es abgelaufen ist

CLC 2006 log: (%SYSTEMROOT%\comtsyncclient.log):

```
2010.04.14 15:15:00.187 0780:0784:00 <5:main:603:S0:C0> Connecting to:
192.168.2.101:2003
2010.04.14 15:15:00.218 0780:0784:00
<2:Comt::Net::SSLSocketOpenSSL::connect:274:S0:C0><main:677> Connect error rc: -1,
rc2: 1, lc: 522, 'error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed'
2010.04.14 15:15:00.218 0780:0784:00 <5:main:697:S0:C0> sync done, time: 234
```

SignOn Proxy 2006 log:

```
14.04.2010  14:33:18:090 LISTENER   5164                -> 
14.04.2010  14:33:18:090 LISTENER   5164                -> Connect from
192.168.2.183:3650 (Socket:392) accepted (Connection Nr:1).
14.04.2010  14:33:18:100 LOGIC1     4672                ->
<2:Comt::Net::SSLSocketOpenSSL::postAccept:828:S0:C0><ProxyAgentComm::runImpl:604>
Error accepting SSL connection: 1!
14.04.2010  14:33:18:100 LOGIC1     4672                -> Exception occured. Proxy
response not sent to client: 127.0.0.1:3650 socket:392 (closing connection)
14.04.2010  14:33:18:100 LOGIC1     4672                -> Sync time: 0 ms for
client:
```

3.3 Comtarsia SignOn Proxy -> SignOn Agent Kommunikation

Gutfall:

SOP 2006 - SOA 2006 Verbindung OK: (SOP 2006: ComtSOP.log)

```
19.04.2010  10:19:17:710 LOGIC3_1   6032  CRXPSP3DE    -> Agent (W2K3DEDOMSRV1:2002[1])
communication starting (DOMAIN: DOMAIN1_)
19.04.2010  10:19:17:740 LOGIC3_1   6032  CRXPSP3DE    -> SYNCUSER TOKEN successfully
sent to W2K3DEDOMSRV1 (DOMAIN: DOMAIN1_)
19.04.2010  10:19:17:841 LOGIC3_1   6032  CRXPSP3DE    -> Proxy sync success for DOMAIN:
DOMAIN1_
```

SOP 2006 - SOA 2006 Verbindung OK: (SOA 2006: ComtSOA.log)

```
19.04.2010  10:19:17:720 LISTENER   4144                -> Connect from
192.168.2.101:4783 (Socket:680) accepted (Connection Nr:1).
19.04.2010  10:19:17:740 LOGIC3     4684                -> TLS handshake completed
successfully (Socket:680)
```

Beispiele von möglichen Fehlern:

SignOn Agent vertraut SignOn Proxy nicht:
SignOn Agent 2006 lehnt das SignOn Proxy 2006 Zertifikat ab, da der Common Name nicht mit dem Hostnamen übereinstimmt, der SignOn Agent jedoch das CERT_FQDN Flag für trustOptionsServer aktiviert hat.

SignOn Proxy Log:

```
14.04.2010  14:27:04:392 LOGIC1_1   5912                -> Agent (W2K3DEDOMSRV1:2002[1])
communication starting (DOMAIN: DOMAIN1_)
```

```
14.04.2010  14:27:04:433 LOGIC1_1   5912                -> SYNCUSER TOKEN successfully
sent to W2K3DEDOMSRV1 (DOMAIN: DOMAIN1_)
14.04.2010  14:27:04:433 LOGIC1_1   5912                ->
<2:Comt::Net::SSLSocketOpenSSL::readBytes:708:S1:C2746><ProxyProcessDomainReq::runImpl:3
31> Read error rc: -1, system rc: 10054
```

SignOn Agent Log:

```
14.04.2010  14:27:04:392 LISTENER   4392                -> Connect from
192.168.2.101:3640 (Socket:576) accepted (Connection Nr:1).
14.04.2010  14:27:04:433 LOGIC4     5064                ->
<2:Comt::Net::SSLSocketOpenSSL::verifyPeerCertificate:340:S0:C0><SyncLogic::runImpl:849>
Subject name (proxy.comtarsia.com) does not match peer FQDN
(w2k3deDomSrv1.adsdom101.comtarsia.com)!
14.04.2010  14:27:04:433 LOGIC4     5064                -> Exception occured. Domain
response not sent to client: 192.168.2.101:3640 socket:576 (closing connection)
```


4. Disclaimer

Alle Seiten unterliegen dem Urheberschutz und dürfen nur mit schriftlicher Genehmigung von Comtarsia IT Services GmbH kopiert oder in eigene Angebote integriert werden.

Alle Rechte vorbehalten.

Irrtümer und Änderungen vorbehalten!

Die Comtarsia IT Services gibt keinerlei Zusicherungen oder Gewährleistungen für andere Websites, auf welche in diesen Handbuch verwiesen wird. Wenn Sie auf eine Nicht-Comtarsia IT Services Website zugreifen, ist das eine unabhängige Site, über deren Inhalt wir keine Kontrolle haben.
Dies gilt auch dann, wenn diese Site möglicherweise das Comtarsia IT Services Logo enthält.

Darüber hinaus bedeutet ein Link aus unserer Site heraus auf eine andere nicht, daß wir uns mit deren Inhalt identifizieren oder deren Nutzung unterstützen.