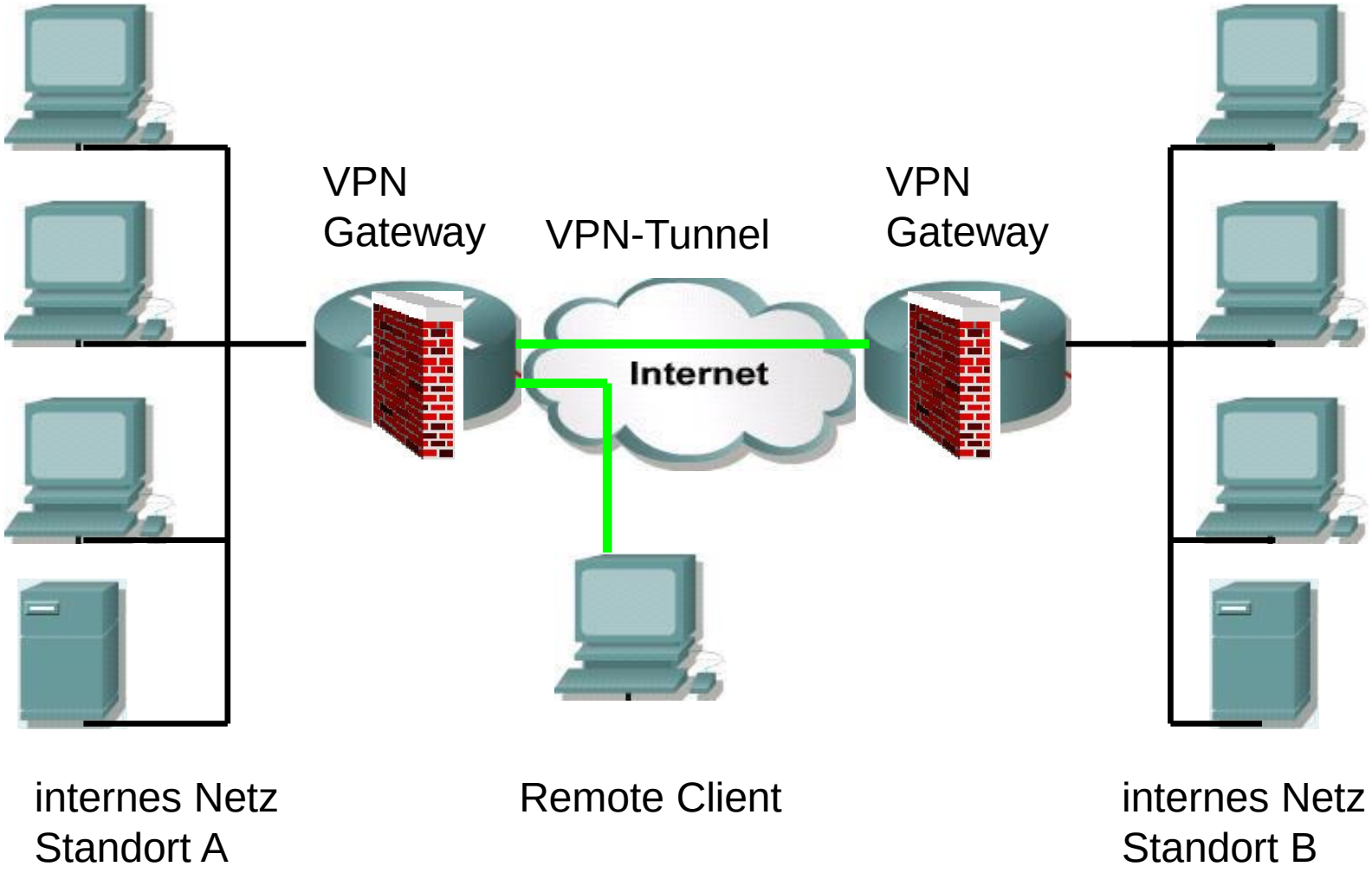
VPN

Virtual Private Network

https://de.wikipedia.org/wiki/Virtual_Private_Network

Virtual Private Networt



Virtual Private Networt

- VPN, Virtual Private Network bedeutet, dass eine verschlüsselte und damit sichere Verbindung zwischen genau zwei Endpunkten hergestellt werden kann.
- VPN ermöglicht einem Benutzer von einer privaten Lokalität über das Internet eine sichere Verbindung zu anderen Benutzern oder Firmen und Organisationen in der Art herzustellen, als würde sich der Benutzer im Intranet einer Firma befinden oder er und ein weiterer Benutzer hätten ein eigenes Intranet aufgebaut und gehörten zum gleichen Netzwerk.
- Im Internet als Transportmedium wird für diese Verbindung ein virtuelles Netz (ein „verschlüsselter Kanal“ oder „Tunnel“) angelegt, durch den die Rechner zweier lokal getrennter Bereiche wie in einem Netz kommunizieren können.
- Für diese Verbindung werden spezielle Protokolle eingesetzt

VPN Gateways

- VPN Gateways koppeln komplette lokale Netze über das Internet.
- VPN Gateways können Standalone Geräte sein, aber es werden auch viele Router, Firewalls und Internet Server mit VPN Funktionalität geliefert.
- Standalone Gateways bieten sich insbesondere bei hohen Verschlüsselungsdurchsätzen an, da diese Geräte mit spezieller Verschlüsselungshardware oft preiswerter und flexibeler einzusetzen sind, als universelle Systeme.

VPN Remote Clients

- Ein Remote Client ist ein einzelner Rechner (oftmals ein Notebook), der sich in das Internet einwählt und dann über einen VPN Tunnel die Verbindung in das zentrale Netzwerk herstellt.
- Hierzu wird auf dem System ein VPN Client benötigt, der die Verschlüsselung durchführt.
- Microsoft lieferte mit dem Windows Betriebssystem direkt einen PPTP VPN Client. Auf diese Weise konnten VPN Verbindungen mit MS Windows Remote Systemen sehr bequem mit PPTP aufgebaut werden. PPTP ist aber wegen Sicherheitsproblemen nicht mehr aktuell.

VPN Typen und Einsatzbereiche

- Remote – Access VPN, Host-to-Network, End-to-Site
  - Arbeiten von zu Hause oder unterwegs
- Branch-Office VPN, Network-to-Network, Site-to-Site
  - Anbindung einzelner Firmenstandorte
- Remote-Desktop-VPN, End-to-End, Host-to-Host
  - Fernwartung
- Intranet VPN
  - Absicherung interner Netzbereiche z.B bei WLAN
- Extranet VPN
  - Beschränkter Zugriff für Partnerfirmen und Kunden

Tunneling-Protokolle

	IPsec	L2TP	PPTP	SSTP	TLS/SSL OpenSSL	OpenSSH
OSI-Schicht	Schicht 3	Schicht 2	Schicht 2	Schicht 3	Schicht 4	Schicht 4
Standard	Ja	Ja	Nein	Nein MS	Ja	?
Paketauthentisierung	Ja	Nein	Nein	ja	Ja	Ja
Benutzerauthentisierung	Ja	Ja	Ja	Ja	Ja	?Ja
Datenver-schlüsselung	Ja	Nein	Ja	Ja	Ja	Ja
Schlüssel-management	Ja	Nein	Nein	Ja	Ja	Ja
Tunneling	IP	IP/IPX	IP/IPX	IP	IP/HTTP/SMTP/POP/…	IP/Telnet/FTP/…
Hauptan-wendung	End-to-End End-to-Site Site-to-Site	Provider	End-to-Site	End-to-Site	End-to-Site OpenVPN	End-to-Site

PPTP Point to Point Tunneling Protocol

- ist ein von Microsoft initiiertes Protokoll
- arbeitet auf Layer-2 sozusagen als "virtuelles Kabel".
- PPTP ist multiprotokollfähig und kann zum Beispiel in IP und IPX Netzwerken genutzt werden.
- PPTP ist insbesondere im Bereich Remote-User VPN interessant.
- Alle Microsoft Betriebssysteme kamen bereits mit installierter PPTP Client Software
- PPTP ist durch einen Bug im Schlüsselaustausch als "relativ unsicheres" VPN Protokoll inzwischen bei neuen VPN's mit höherem Sicherheitsbedarf von IPSec fast komplett verdrängt.
- Nachfolger bei MS ist Secure Socket Tunneling Protocol SSTP oder L2TP/IPSec

IPSec Internet Protocol Security

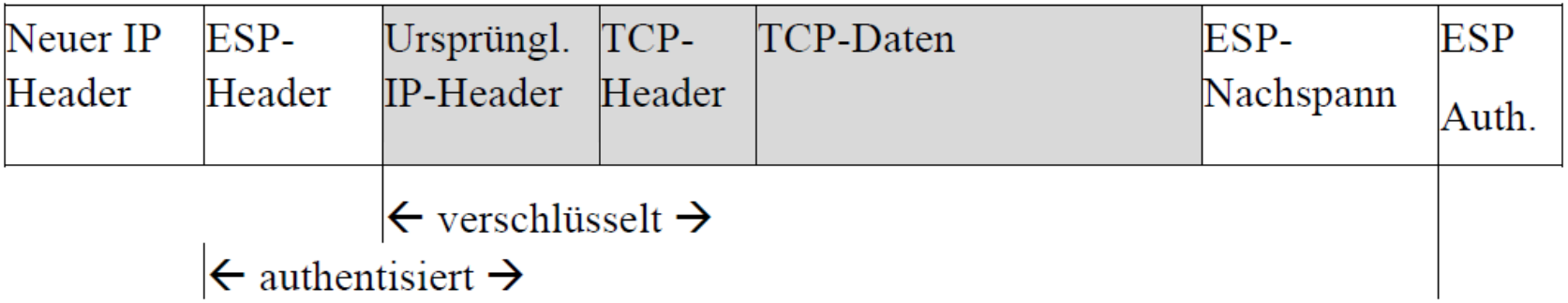
- Unter IPSec versteht man eine Reihe von Protokollen zur Schlüsselverwaltung, zur Authentisierung und Verschlüsselung.
- IPSec ist im Rahmen von IPv6 entwickelt worden und bereits vor der Umsetzung auf den IPv4 Standard aufgesetzt worden.
- Die IPSec-Spezifikationen definieren zwei IP-Protokolle:
  - Encapsulating Security Payload (ESP) für die Verschlüsselung und Authentisierung
  - Authentication Header (AH) für die Authentisierung
- speziell zu installierende Client Software benötigt

IPSec Internet Protocol Security 2

- Mit Hilfe von IPSec können IP-Pakete als ESP- bzw. AH-Pakete in der dritten ISO/OSI-Schicht transportiert werden
- Bei einer UDP-Kapselung von ESP werden die Pakete in der vierten ISO/OSI-Schicht transportiert.
- Da ESP auch ohne Verschlüsselung und somit zur reinen Authentisierung verwendet werden kann, ist der Einsatz von AH nicht sehr weit verbreitet.
- Beide Protokolle unterstützen den Tunnel-Mode und den Transport-Mode

ESP Tunnelmodus

- ESP wird für VPN im Tunnelmodus eingesetzt



OpenVPN

- Open-source commercial Software für VPN
- Eigenes Protokoll auf Basis OpenSSL für Tunnel
- Verwendet SSL/TLS für Schlüsselaustausch
- Bietet Pre-Shared Keys, Certificate und Username/Password Authentication
- Läuft über UDP (oder TCP) mit beliebigem Port (1194)
- Erweiterbar über Plug-ins
- Verfügbar für viele Betriebssysteme
- Eigene Clientsoftware, nicht kompatibel mit anderen VPN-Clients

OpenVPN

```
SSL/TLS -> Reliability Layer -> \
           --tls-auth HMAC       \
                                  \
                                   > Multiplexer ----> UDP
                                  /                    Transport
IP         Encrypt and HMAC      /
Tunnel -> using OpenSSL EVP --> /
Packets    interface.
```

Verschlüsselungsverfahren

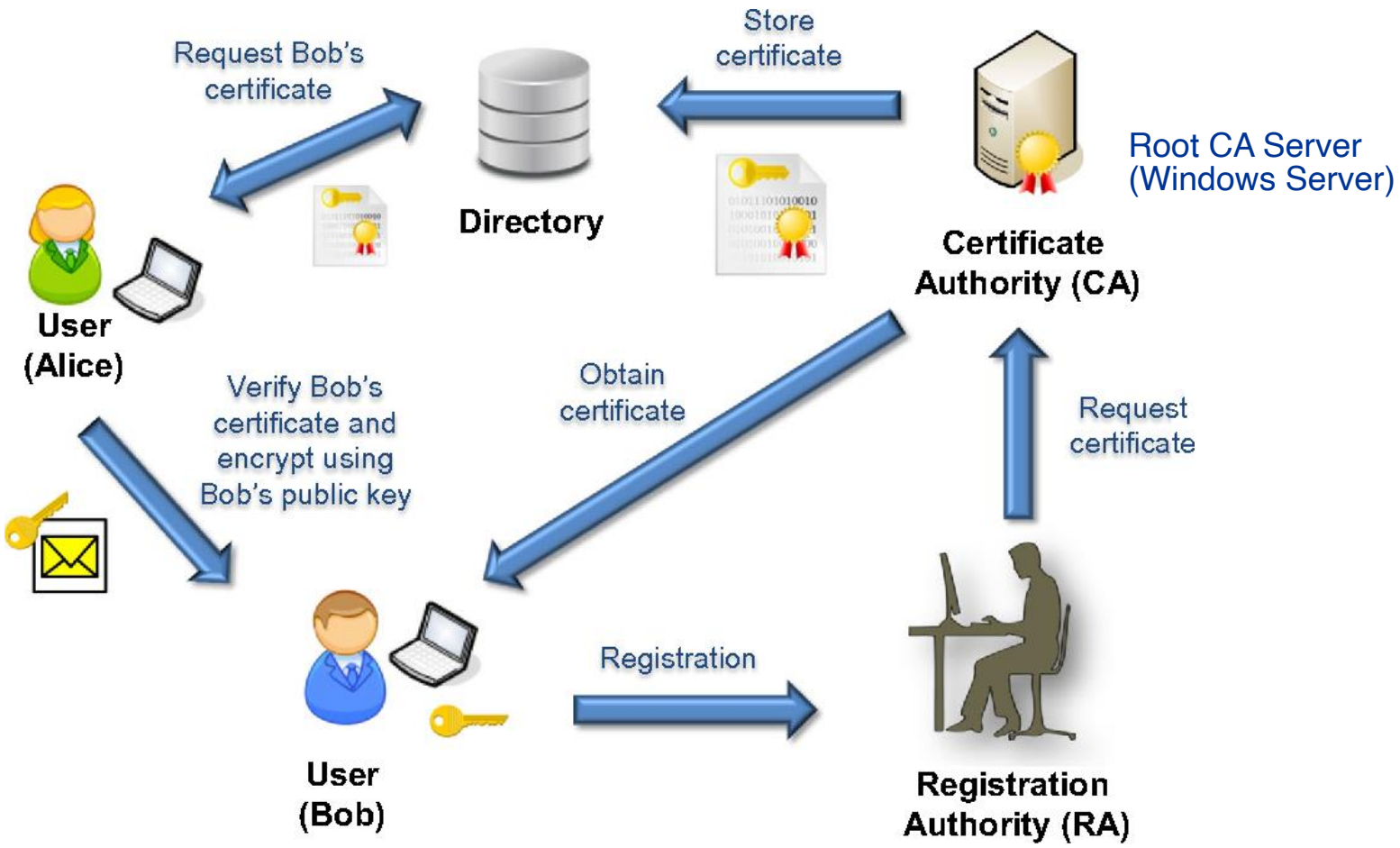
Bez.	Bezeichnung	Typ	Anm.
DES	Data Encryption Standard	SYM	zu geringe Schlüssellänge 56 bit
3DES	Triple-DES	SYM	168 bit und rechenintensiv
AES	Advanced Encryption Standard	SYM	Nachfolger v. DES 128/192/256 bit
RSA	Rivest, Shamir, Adleman	ASM	1024/2048/4096/8192 bit
SHA-2/3	Secure Hash Algorithm	Hash	SHA-256/384/512 Nachf. von MD5
Twofish		SYM	Nachfolger v. Blowfish, frei, schnell
	Hybridverfahren	HYB	Kombination von SYM und ASM
DH	Diffie Hellman	SYM	Schlüsselaustausch
ECC	Elliptic Curve Cryptography	HYB	Ell. Kurven, Nachfolge v. RSA
MAC	Message Authentication Codes	SYM	
DSA	Digital Signature Algorithm		Auf Basis Ell. Kurven

Public Key Infrastructure PKI

- Certificate Authority CA: The authority that authenticates the identity of individuals, computers and other entities.
- Registration Authority: A subordinate CA that issues a certificate on the behalf of root CA for specific uses.
- SSL Certificate: The Data file that includes the public key and other information.
- Certificate Management System: Stores, validates and revokes certificates.

PKI

Public-Key-Infrastruktur



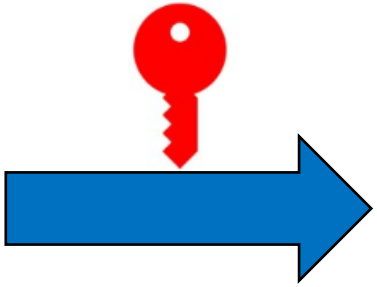
Certifikate

Identity Information and
Public Key of HTL-Wels

Name: ELSI
Organization: HTL
Address: Wels
Country: Austria

Public Key
of
HTL-Wels

CA verifies the identity of HTL-Wels and encrypts with its Private Key



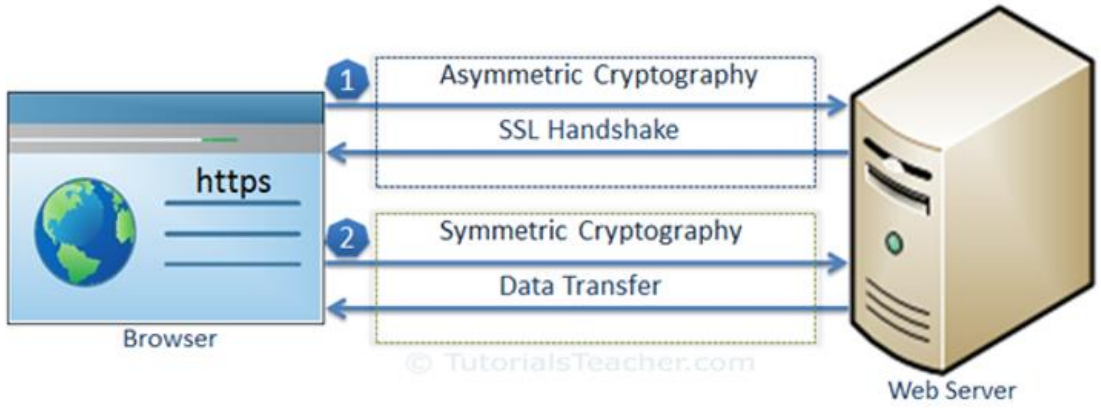
Certificate of HTL-Wels

Name: ELSI
Organization: HTL
Address: Wels
Country: Austria
Validity: -2022/07

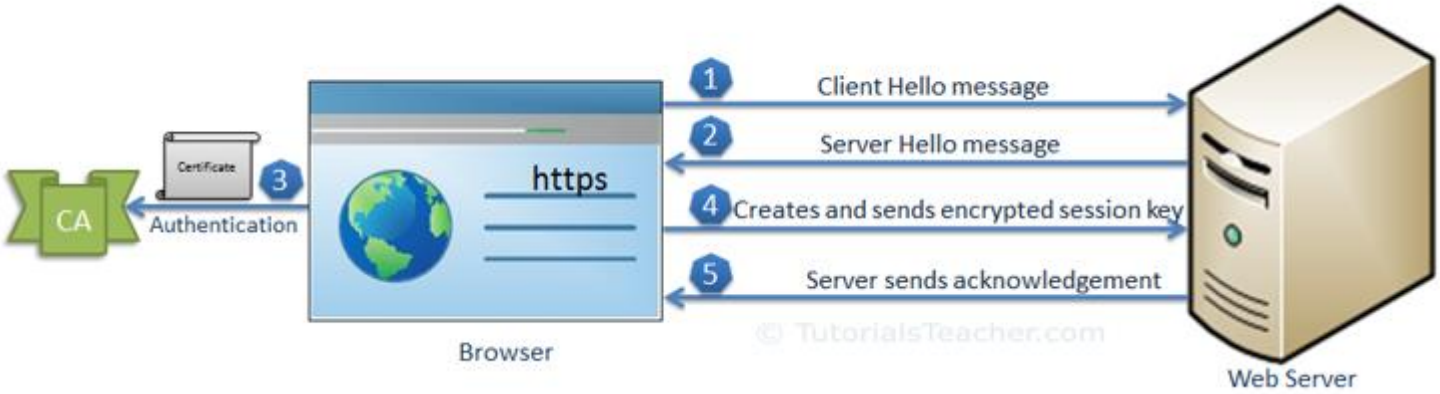
Public Key
of
HTL-Wels

Digital Signature
of the CA

Data Transfer over SSL



SSL Handshake



A Typical Certificate (X.509)

Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha256WithRSAEncryption Issuer: C=AT, ST=UA, L=Wels, O=HTL-Wels, OU=MyHTLOU, CN=MyVPN/name=MyServer/emailAddress=georg.elsinger@htl-wels.at Validity Not Before: Oct 23 11:05:42 2019 GMT Not After : Oct 20 11:05:42 2029 GMT Subject: C=AT, ST=UA, L=Wels, O=HTL-Wels, OU=MyHTLOU, CN=client1/name=MyServer/emailAddress=georg.elsinger@htl-wels.at Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public-Key: (2048 bit) Modulus: 00:e1:79:44:cb:af:f5:d0:9a:b8:46:d7:4d:59:fc:
5c:e0:8c:ea:6f:1a:a6:77:90:b5:9b:09:f6:15:3d:
5b:3e:c8:f8:24:3f:2f:80:cb:78:b5:46:4f:90:1c:
91:ad:6a:38:9d:e2:76:72:ee:be:f7:1d:96:f4:2c:
0b:55:b4:5e:83:76:9c:35:e2:70:98:19:8d:f4:ff:
ee:43:8b:c8:71:05:6c:7d:87:32:b3:86:0c:59:1e:
38:4e:74:84:03:09:88:cb:98:f0:e9:4b:c6:18:8b:
e9:e9:3c:e5:0f:aa:0d:49:29:ad:85:6d:d3:b0:23:
d5:4e:e7:4e:35:9c:0f:e8:6c:5e:7b:15:61:bf:6d:
99:02:ce:dc:95:29:56:f5:8c:01:a7:1a:b2:6e:5c:
77:1c:fd:06:44:04:15:c5:89:d0:fc:1c:ac:4a:56:
50:e1:d5:b7:f8:2b:52:56:61:15:89:d2:53:c9:c0:
82:ce:7e:46:e3:f7:8d:bb:e1:fa:85:0e:ee:dc:8f:
91:3d:78:1a:af:bc:1f:bf:b4:47:b7:8a:dc:26:40:
cb:a6:2f:2a:be:87:07:06:c0:5b:54:51:ef:33:b2:
81:b4:a9:9e:63:00:31:fa:6e:68:dd:48:be:61:a8:
12:1e:f5:c7:b1:b1:b6:11:3a:a9:87:25:a8:ae:72: 74:8d Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: CA:FALSE Netscape Comment: Easy-RSA Generated Certificate X509v3 Subject Key Identifier: F9:E7:F6:47:A5:7D:55:6E:A5:41:37:C5:6E:52:7F:A3:3A:20:8D:99 X509v3

A Typical Certificate (X.509) continued

Authority Key Identifier:
keyid:09:20:B7:41:78:D5:74:FF:E1:A4:76:7F:8F:5D:D6:27:E4:A5:35:5B
DirName:/C=AT/ST=UA/L=Wels/O=HTL-Wels/OU=MyHTLOU/CN=MyVPN/name=MyServer/emailAddress=georg.elsinger@htl-wels.at
serial:69:EE:FF:91:5C:9E:7B:A1:62:D2:0E:7C:9F:AF:16:88:18:57:12:48
X509v3 Extended Key Usage: TLS Web Client Authentication
X509v3 Key Usage: Digital Signature X509v3 Subject Alternative Name: DNS:client1 Signature Algorithm: sha256WithRSAEncryption
74:dd:f9:0b:40:45:57:8b:a3:0c:f6:06:a6:48:6b:c1:4c:60:
2a:37:11:f0:6b:a0:f0:c9:b8:42:93:34:a0:0d:c5:5d:e8:c9:
71:c8:5a:ed:d2:15:79:60:c7:1c:f2:8d:95:71:cc:d7:c7:3c:
31:ce:da:2a:59:a3:8c:5f:05:e6:ee:17:60:9c:95:a3:cf:07:
d1:89:de:e5:18:44:46:0f:cb:db:4d:45:e6:78:fc:26:8c:1c:
e0:18:90:53:70:a9:a6:f8:ea:50:ac:23:65:fd:15:dd:ad:58:
de:4d:12:02:e3:14:e0:a0:15:01:58:03:5e:e4:6e:15:17:e9:
b6:9e:f1:35:88:0d:52:2d:77:41:2d:4a:ab:b0:80:3b:2b:d8:
50:be:6a:ff:b4:31:fe:61:eb:2a:40:03:8a:57:00:05:46:b0:
54:4c:ff:2a:40:2a:b2:4f:00:fb:3b:ea:b5:d9:17:79:3f:d8:
01:42:f7:34:92:6d:2b:64:e1:3d:a4:be:3d:5f:93:ef:ae:ec:
84:37:be:a3:5d:36:36:9f:72:28:0c:60:9c:ea:d3:4d:82:5f:
a8:d1:26:53:bf:46:c6:35:b4:6c:69:97:6a:b5:1e:89:11:8c:
ca:5a:94:e6:e3:b0:e9:f2:4b:47:88:68:1a:40:b1:8b:ef:19: 5f:4b:db:87

A Typical Certificate (X.509) continued

-----BEGIN CERTIFICATE-----
MIIFKzCCBBOgAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMCQVQ
xCzAJBgNVBAgTAlVBMQ0wCwYDVQQHEwRXZWxzMREwDwYDVQQKEwhIVEwtV2V
sczEQMA4GA1UECxMHTXlIVExPVTEOMAwGA1UEAxMFTXlWUE4xETAPBgNVBCkT
CE15U2VydmVyMSkwJwYJKoZIhvcNAQkBFhpnZW9yZy5lbHNpbmdlckBodGwtd2Vscy5
hdDAeFw0xOTEwMjMxMTA1NDJaFw0yOTEwMjAxMTA1NDJaMIGeMQswCQYDVQQG
EwJBVDELMAkGA1UECBMCVUExDTALBgNVBAcTBFdlbHMxETAPBgNVBAoTCEhUT
C1XZWxzMRAwDgYDVQQLEwdNeUhUTE9VMRAwDgYDVQQDEwdjbGllbnQxMREwD
wYDVQQpEwhNeVNlcnZlcjEpMCcGCSqGSIb3DQEJARYaZ2VvcmcuZWxzaW5nZXJAa
HRsLXdlbHMuYXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDheUTL
r/XQmrhG101Z/FzgjOpvGqZ3kLWbCfYVPVs+yPgkPy+Ay3i1Rk+QHJGtajid4nZy7r73HZ
b0LAtVtF6Ddpw14nCYGY30/+5Di8hxBWx9hzKzhgxZHjhOdIQDCYjLmPDpS8YYi+npPO
UPqg1JKa2FbdOwI9VO5041nA/obF57FWG/bZkCztyVKVb1jAGnGrJuXHcc/QZEBBXFid
D8HKxKVlDh1bf4K1JWYRWJ0lPJwILOfkbj94274fqFDu7cj5E9eBqvvB+/tEe3itwmQMum
Lyq+hwcGwFtUUe8zsoG0qZ5jADH6bmjdSL5hqBIe9cexsbYROqmHJaiucnSNAgMBAAG
jggFyMIIBbjAJBgNVHRMEAjAAMC0GCWCGSAGG+EIBDQQgFh5FYXN5LVJTQSBHZ
W5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFPnn9kelfVVupUE3xW5Sf6M
6II2ZMIHcBgNVHSMEgdQwgdGAFAkgt0F41XT/4aR2f49d1ifkpTVboYGipIGfMIGcMQsw
CQYDVQQGEwJBVDELMAkGA1UECBMCVUExDTALBgNVBAcTBFdlbHMxETAPBgNV
BAoTCEhUTC1XZWxzMRAwDgYDVQQLEwdNeUhUTE9VMQ4wDAYDVQQDEwVNeV
ZQTjERMA8GA1UEKRMITXlTZXJ2ZXIxKTAnBgkqhkiG9w0BCQEWGmdlb3JnLmVsc2lu
Z2VyQGh0bC13ZWxzLmF0ghRp7v+RXJ57oWLSDnyfrxaIGFcSSDATBgNVHSUEDDAK
BggrBgEFBQcDAjALBgNVHQ8EBAMCB4AwEgYDVR0RBAswCYIHY2xpZW50MTANBg
kqhkiG9w0BAQsFAAOCAQEAdN35C0BFV4ujDPYGpkhrwUxgKjcR8Gug8Mm4QpM0oA
3FXejJccha7dIVeWDHHPKNlXHM18c8Mc7aKlmjjF8F5u4XYJyVo88H0Yne5RhERg/L20
1F5nj8Jowc4BiQU3CppvjqUKwjZf0V3a1Y3k0SAuMU4KAVAVgDXuRuFRfptp7xNYgNUi1
3QS1Kq7CAOyvYUL5q/7Qx/mHrKkADilcABUawVEz/KkAqsk8A+zvqtdkXeT/YAUL3NJJt
K2ThPaS+PV+T767shDe+o102Np9yKAxgnOrTTYJfqNEmU79GxjW0bGmXarUeiRGMyl
qU5uOw6fJLR4hoGkCxi+8ZX0vbhw==
-----END CERTIFICATE-----