

Inhaltsverzeichnis

1.	EINLEITUNG	11
1.1.	Grundsätzliche PKI-Alternativen	11
2.	VORAUSSETZUNGEN	13
3.	RICHTLINIEN UND PKI.....	13
3.1.	Sicherheitsrichtlinie	13
3.2.	Zertifikatrichtlinie	14
3.3.	Zertifikatsverwendungserklärung (Certificate Practice Statement, CPS).....	14
4.	ZERTIFIZIERUNGSSTELLEN TYPEN.....	15
4.1.	Unternehmenszertifizierungsstellen	15
4.2.	Eigenständige Zertifizierungsstellen	15
4.3.	Unternehmens- und eigenständige Zertifizierungsstellen	15
4.4.	Stammzertifizierungsstellen	16
4.5.	Untergeordnete Zertifizierungsstellen	16
4.6.	Zwischenzertifizierungsstellen	16
5.	ENTWURF EINER ZERTIFIZIERUNGSSTELLENHIERARCHIE.....	16
5.1.	Eine dreischichtige Zertifizierungsstellenhierarchie	16
5.1.1.	Eine dreischichtige Hierarchie wird in folgenden Szenarien empfohlen:	16
5.2.	Eine zweischichtige Zertifizierungsstellenhierarchie	17
5.2.1.	Eine zweischichtige Hierarchie wird in folgenden Szenarien empfohlen:.....	17
6.	ORGANISATION DER AUSSTELLENDEN ZERTIFIZIERUNGSSTELLEN ...	18
7.	AUSWAHL EINER ARCHITEKTUR	18
7.1.	Wie viele Stufen benötigt eine PKI?	18
8.	SAMMLUNG DER ERFORDERLICHEN INFORMATIONEN.....	19
9.	IDENTIFIKATION PKI-FÄHIGER ANWENDUNGEN.....	20
9.1.	PKI-fähige Anwendungen	20
9.2.	Identifikation von Zertifikatempfängern.....	20
10.	BESTIMMUNG DER SICHERHEITSANFORDERUNGEN.....	20
10.1.	Bauliche, organisatorische und betriebliche Maßnahmen	20
10.2.	Räumliche Sicherheit der Offline-Zertifizierungsstellen	22
10.3.	Zusätzliche Sicherheitsmaßnahmen für Online-Zertifizierungsstellen	22
10.4.	Sicherheitsmaßnahmen in der Konfiguration der Zertifizierungsstellen.....	23
10.4.1.	Beschränkung der Serverrollen	23
10.4.2.	Absicherung der Server mit Sicherheitskonfigurations-Assistenten	23
10.4.3.	Aktivierung aller Überwachungsoptionen einer Zertifizierungsstelle.....	23
10.4.4.	Aktivierung der BitLocker-Datenträgerschlüsselung	23
10.4.5.	Beschränkung der Mitgliedschaft in lokaler Administratorengruppe	23
10.4.6.	Durchsetzung der Rollentrennung	23
10.5.	Schutz des privaten Schlüssels der Zertifizierungsstelle	23
10.5.1.	Verwendung eines Smartcard-Kryptografie-Diensteanbieters.....	24
10.5.2.	Verwendung von Hardwaresicherheitsmodulen.....	24
10.5.3.	Sichere Gehäuse für Zertifizierungsstellencomputer	24
10.5.4.	Sicherheitsmaßnahmen im (virtuellen) Serverumfeld.....	25
10.6.	Unterschiedliche Sicherheitsanforderungen für Zertifikate.....	27

10.7.	Datenarchivierung	27
10.7.1.	Technische Sicherheitsmaßnahmen.....	27
11.	BESTIMMUNG DER TECHNISCHEN ANFORDERUNGEN.....	28
11.1.	Die Festlegung der PKI-Verwaltungsrollen	28
11.2.	Die Minimierung des Ausfallrisikos	29
11.3.	Die Festlegung der Gültigkeit von Zertifikaten	29
11.4.	Wahl der Schlüssellänge.....	30
11.5.	Ausstellung von Zertifikaten.....	31
11.6.	Beschaffung und Ausstellung von Trust Center Zertifikaten.....	31
11.7.	Überwachung des Lebenszyklus von Zertifikaten	32
11.8.	Festlegung der Veröffentlichungspunkte.....	32
12.	ERMITTLUNG DER BETRIEBLICHEN ANFORDERUNGEN	32
12.1.	Minimierung der PKI-bezogenen Kosten	32
12.2.	Hohe Verfügbarkeit von Zertifizierungsstellen	32
12.3.	Haftung der Teilnehmer	33
13.	ERMITTLUNG EXTERNER ANFORDERUNGEN.....	33
13.1.	Externe Organisationen möchten Zertifikate verifizieren können	33
13.2.	Zertifikate sollen in einer Partnerorganisation genutzt werden	33
13.3.	Gesetze.....	33
13.4.	Überprüfung von Zertifikaten in externen oder Perimeter-Netzwerken	33
14.	SAMMELN DER AD DS-ANFORDERUNGEN	33
14.1.	Namenskonventionen.....	33
14.2.	Auswahl der Domäne.....	34
14.3.	Definieren der Organisationseinheitsstruktur	34
15.	IDENTIFIKATION VON ZERTIFIKATEMPFÄNGERN.....	34
16.	PKI-FÄHIGE ANWENDUNGEN	34
17.	SSL-VERSCHLÜSSELUNG FÜR WEBSERVER.....	34
17.1.	Webserverzertifikate von Zertifizierungsstellen im eigenen Netz.....	35
17.2.	Webserverzertifikate von Zertifizierungsstellen kommerzieller Anbieter	35
18.	REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE	35
19.	SICHERE E-MAIL	36
19.1.	S/MIME Zertifikate von Zertifizierungsstellen kommerzieller Anbieter	36
19.2.	S/MIME Zertifikate von Zertifizierungsstellen im eigenen Netz	36
20.	VIRTUELLE PRIVATE NETZWERKE (VPN)	36
21.	802.IX AUTHENTIFIZIERUNG	37
22.	EFS-VERSCHLÜSSELUNG	38
23.	CODE-SIGNING.....	38
24.	BEREITSTELLUNG VON SMARTCARDS.....	40
25.	VERSCHLÜSSELUNGSARTEN.....	40
26.	ALGORITHMEN UND SCHLÜSSEL	41
27.	DATENVERSCHLÜSSELUNG.....	42
27.1.	Symmetrische Verschlüsselung.....	42
27.2.	Asymmetrische Verschlüsselung	43

27.3.	Asymmetrische Signatur	44
27.4.	Asymmetrische Algorithmen	45
27.5.	Kombination von symmetrischer und asymmetrischer Verschlüsselung.....	45
27.6.	Digitale Signatur von Daten	46
27.7.	Der Hashvorgang	47
27.8.	Hashalgorithmen.....	47
27.9.	Kombination aus asymmetrischer Signatur und Hashalgorithmus.....	47
27.10.	Cryptography Next Generation (CNG).....	48
28.	INSTALLATION EINER PKI-TESTUMGEBUNG	49
29.	PLANUNG DER PKI.....	49
29.1.	Planung einer geeigneten Public Key-Infrastruktur (PKI).....	49
29.2.	Optionale Bereitstellung eines Hardwaresicherheitsmoduls (HSM).....	49
29.3.	Erstellung einer geeigneten CAPolicy.inf	50
29.4.	Auswahl des Setup-Typs der Zertifizierungsstellen	50
30.	SOLLZUSTAND WINDOWS SERVER 2016 ZERTIFIKATSDIENSTE	50
31.	INSTALLATION EINER ZWEISCHICHTIGEN ZERTIFIZIERUNGSSTELLENHIERARCHIE	51
32.	VORBEREITUNG DES DNS-SERVERS AUF DEM DC01	52
33.	ANPASSUNG DER STANDARD-INSTALLATIONSEINSTELLUNGEN	53
34.	KONFIGURATION NACH DER INSTALLATION.....	55
35.	INSTALLATION DER EIGENSTÄNDIGEN STAMMZERTIFIZIERUNGSSTELLE „ROOT CA“	57
35.1.	Vorarbeiten.....	57
35.2.	Parameter	59
35.3.	Installation	60
35.4.	Abschlussarbeiten - Post Installation Script.....	65
35.5.	Publish Root CA Cert und CRL.....	65
36.	INSTALLATION DER AUSSTELLENDEN ZERTIFIZIERUNGSSTELLE ...	66
36.1.	Parameter	66
36.2.	Installation Part 1.....	66
36.2.1.	Request einreichen.....	72
36.2.2.	CA01 - Zertifikat importieren.....	77
36.3.	Abschlussarbeiten - Post Installation Script.....	78
36.4.	Zertifikatsvorlagen bereitstellen.....	79
36.5.	Weitere Zertifizierungsrollen installieren	87
36.5.1.	Schnittstelle für die Webregistrierung.....	91
36.6.	Abschlussarbeiten Internetinformationsdienste (IIS)	92
36.7.	Petit-Potam Workaround.....	93
36.7.1.	Schadensbegrenzung	94
36.8.	Installation Part 2.....	97
36.8.1.	Installation des Online-Responders	97
1.1.1.	Installation des Registrierungsdienstes für Netzwerkgeräte	102
37.	INSTALLATION DES NETWORK POLICY SERVERS (NPS) / RADIUS	110
38.	INSTALLATION EINES EXTERNEN WEBSERVERS IN DER DMZ	114

38.1.	Erweiterung der Firewall Regeln für den Web01 in der DMZ	115
38.1.1.	Installation des IIS	115
38.1.2.	Web Server Zertifikat für den Web01 implementieren	116
7.2.3	Verzeichnis für die Zertifizierungsstellen Zertifikate erstellen.....	128
7.2.4	Automatisierung der Veröffentlichung der Zertifikate und Sperrlisten auf dem Web01.....	130
39.	INSTALLATION EINES KERIO CONNECT MAILSERVERS IN DER DMZ	
	135	
39.1.	MX-Eintrag für den Mailserver	136
39.2.	Erweiterung der Firewall Regeln für den Mail01 in der DMZ	136
39.3.	Windows Firewall konfigurieren.....	138
39.4.	Kerio Connect Schemaerweiterung für den Domian Controllers DC01	140
39.5.	Einrichtung des Kerio Connect Mailservers	140
39.5.1.	SSL Zertifikat von der Zertifizierungsstelle CA01 installieren.....	141
39.5.2.	Deaktivierung nicht benötigter und unsicherer Dienste	147
39.5.3.	Konfiguration der Anbindung an die Active Directory Domäne	149
39.5.4.	Test der Active Directory Anbindung	151
40.	INSTALLATION EINES VPN-SERVERS IN DER DMZ.....	152
40.1.	Erweiterung der Firewall Regeln für die fw01 in der DMZ	153
40.2.	Sicherheitsgruppen für die VPN-Clients erstellen.....	154
40.3.	Zertifikatvorlage für den VPN-Server erstellen	154
40.4.	Installation der Zertifikate der Stammzertifizierungsstelle (RootCA) und der ausstellenden Zertifizierungsstelle CA01	166
40.5.	Konfiguration des Netzwerkrichtlinienservers (RADIUS)	171
40.6.	Konfiguration des Rolle Remotezugriff auf dem VPN-Server	173
40.6.1.	Eigenschaften Routing und RAS.....	177
40.7.	Konfiguration der lokalen Firewall für die Verwendung von IPsec	180
40.7.1.	Globale Einstellungen.....	180
40.7.2.	Verbindunsicherheitsregel (Connection Security Rule)	184
40.7.3.	Die Überwachung der IPsec Verbindung	188
40.8.	Protokollierung und Firewall-Log.....	190
41.	BEREITSTELLUNG WEITERER ZERTIFIKATE	191
41.1.	Zertifikate für Domänencontroller.....	191
41.2.	Zertifikate für Computer	193
41.3.	Zertifikat für Benutzer	196
41.4.	Zertifikate für Remote Desktop Services.....	199
42.	KONFIGURATION ACCESS POINT (AP01)	203
43.	KONFIGURATION RADIUS NAS (SWITCH01)	206
43.1.	Die Konfiguration des 802.1X-fähigen Switches erfordert folgende Werte	206
43.2.	Alternativ: Konfiguration eine HP Procurve Switches	207
43.2.1.	Konfiguration der benötigten Parameter an der Console des Switches.....	208
44.	IMPLEMENTIERUNG UND KONFIGURATION DER FIREWALL (FW01)	
	209	
44.1.	Das Regelwerk.....	209
44.2.	Die Konfiguration als Textdatei.....	209
45.	WINDOWS ZERTIFIKATSDIENSTE NUTZEN.....	218
45.1.	Server Manager.....	218

45.2.	Management der Zertifizierungsstelle	218
45.3.	Zertifikatvorlagen	219
45.4.	Ausrollen und automatisches Registrieren der Zertifikate.....	221
45.5.	OCSP	222
45.6.	Schnittstelle für die Webregistrierung.....	223
45.7.	Erstellung eines Benutzer Zertifikats.....	225
45.8.	Zertifikat der Zertifizierungsstelle (<i>RootCA Certificate</i>)	227
45.9.	Verwaltung von Client Zertifikaten	229
45.10.	Zertifikate exportieren	230
45.11.	Zertifikate sperren und freigeben	232
45.12.	Backup	235
45.12.1.	Manuelle Sicherung mit der Konsole Zertifizierungsstelle	235
45.12.2.	Automatische Sicherung mittels Certutil-Befehl.....	237
45.13.	Certutil - Zertifikate löschen und verwalten.....	238
46.	KEY RECOVERY AGENT	239
46.1.	Schlüssel mit dem Key Recovery Agent wiederherstellen.....	246
47.	REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE	247
48.	WIFI MIT 802.1X AUTHENTIFIZIERUNG	249
48.1.	EAP-TLS-Authentifizierung	249
48.2.	PEAP-Authentifizierung	250
48.3.	Funktionsweise der 802.1x Authentifizierung.....	250
48.4.	Zusammenfassung des Prozesses zum Einbuchen in das WLAN.....	252
48.5.	Sicherheitsbedenken	253
48.5.1.	EAP-TLS (Transport Layer Security)	253
48.5.2.	EAP-PEAP (Protected EAP)	253
48.6.	Bereitstellung der benötigten Zertifikate.....	253
48.7.	Externe Wifi-Devices	253
48.7.1.	Manuelle Verwaltung und Konfiguration.....	254
48.7.2.	Registrierungsdienst für Netzwerkgeräte	254
48.7.3.	Mobile-Device-Management (MDM).....	255
49.	IMPLEMENTIERUNG 802.1X - WIFI FÜR AD-DS-INTEGRIERTE CLIENTS 255	
49.1.	Konfiguration der Wifi-Devices (EAP-TLS).....	255
49.2.	Computer-Zertifikat für das Wifi-Device.....	255
49.3.	Sicherheitsgruppen erstellen.....	257
49.4.	GPOs erstellen	257
49.5.	Netzwerkrichtlinienserver NPS (RADIUS)	265
49.6.	Konfiguration weiterer Bedingungen für die Verbindungsanforderung	270
49.7.	Test eines AD-DS-integrierten Wifi-Devices	272
50.	IMPLEMENTIERUNG 802.1X – WIFI FÜR NICHT-AD-DS-INTEGRIERTE CLIENTS	273
50.1.	PEAP	273
50.1.1.	Sicherheitsgruppe erstellen.....	273

50.1.2.	Netzwerkrichtlinienserver NPS (RADIUS).....	274
50.1.3.	Konfiguration weiterer Bedingungen für die Verbindungsanforderung	276
50.1.4.	Test eines Nicht-AD-DS-integrierten Wifi-Devices	276
50.2.	EAP (TLS) und PEAP	278
50.3.	iPhone Enterprise Integration mit EAP-TLS.....	279
50.3.1.	Benutzer-Zertifikat für das externe Device (EAP-TLS).....	279
50.3.2.	iPhone Configuration Utility 3.6.2 for Windows	286
50.3.3.	Test der iPhone EAP (TLS) Verbindung.....	289
51.	WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG	292
51.1.	Sicherheitsbedenken	295
52.	IMPLEMENTIERUNG WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG FÜR AD-DS-INTEGRIERTE CLIENTS	295
52.1.	Konfiguration der Wired-Access-Devices (EAP-TLS)	295
52.2.	Computer-Zertifikat für das Wired-Access-Devices	295
52.3.	Sicherheitsgruppe erstellen	296
52.4.	GPOs erstellen	297
52.5.	Netzwerkrichtlinienserver NPS (RADIUS)	300
52.6.	NPS-Serverkonfiguration auf einen anderen NPS-Server kopieren.....	306
52.7.	RADIUS-Attribute für VLANs.....	307
52.8.	Test	308
53.	TRIUMPF ADLER (KYOCERA) DRUCKER MIT 802.1X AUTHENTIFIZIERUNG	309
53.1.	IEEE 802.1X-Authentifizierungseinstellung	309
53.2.	Zertifikat der Zertifizierungsstelle importieren.....	310
53.3.	Benutzerzertifikat anfordern und importieren.....	313
54.	WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG FÜR EXTERNE CLIENTS	322
54.1.	Konfiguration externer Wired-Access-Clients (PEAP).....	322
54.1.1.	Netzwerkrichtlinienserver NPS (RADIUS).....	322
54.1.2.	Test	322
54.2.	Konfiguration externer Wired-Access Clients EAP (TLS)	324
54.2.1.	Benutzer-Zertifikat für das externe Device	324
54.2.2.	Netzwerkrichtlinienserver NPS (RADIUS).....	331
54.2.3.	Test	331
55.	NDES-KONFIGURATION FÜR SCEP (CISCO ASA SCEP PROXY).....	332
55.1.	Windows Server Konfiguration	332
55.2.	Cisco ASA Konfiguration per ASDM	335
55.1.	Cisco ASA Konfiguration per Command-Line Interface (CLI) für AnyConnect	342
56.	EFS-VERSCHLÜSSELUNG	348
56.1.	Zertifikatvorlagen für die EFS-Verschlüsselung	348
56.2.	Das EFS-Verschlüsselungszertifikat	348
56.3.	Lokale EFS-Verschlüsselung	348
56.4.	Remoteverschlüsselung.....	349
56.5.	EFS-Entschlüsselung	350

56.6.	EFS-Datenwiederherstellung	350
56.7.	Wiederherstellungsmethoden	351
56.7.1.	Datenwiederherstellung	352
56.7.2.	Sichern des privaten Schlüssels	360
56.7.3.	Schlüsselwiederherstellung	361
56.8.	Aktivierung und Deaktivierung von EFS	361
56.9.	Ausrollen der EFS-Benutzerzertifikate	363
57.	SICHERE E-MAIL	369
57.1.	Secure/Multipose Internet Mail Extensions (S/MIME).....	369
57.2.	Verschlüsselung von E-Mail.....	370
57.3.	SSL für Internetprotokolle.....	371
57.3.1.	SSL-Ports für E-Mail Protokolle	372
57.4.	E-Mail-Server Zertifikat	372
57.5.	Auswahl der Zertifikatvorlagen	372
57.5.1.	Eine Zertifikatvorlage für Signatur und Verschlüsselung	372
57.5.1.	Separate Zertifikatvorlage für Signatur und Verschlüsselung.....	375
57.6.	Aktivierung von Outlook 2016.....	379
57.6.1.	Einrichtung des Kerio Outlook Connector (Offline Edition)	379
57.6.2.	Anforderung des S/MIME Zertifikats	381
57.6.3.	Einbindung des Zertifikats in Outlook	386
57.6.4.	Einbindung des Zertifikats in Kerio Web Frontend	391
57.6.5.	Funktionstest.....	394
58.	VPN-INFRASTRUKTUR MIT WINDOWS SERVER.....	397
58.1.	L2TP/IPsec.....	398
58.2.	IPsec (IKEv2).....	400
58.3.	Konfiguration des VPN-Clients für IKEv2 / IPsec	401
58.3.1.	Erstellung der Zertifikatvorlage für den VPN-Clientcomputer	402
58.3.2.	Gruppenrichtlinie für die automatische Registrierung erstellen	405
58.3.3.	DNS Auflösung des Common Name (CN) des VPN-Servers.....	406
58.3.4.	IKEv2 VPN-Verbindung am Client einrichten	407
58.4.	Deployment / Rollout der VPN Client Konfiguration	413
58.4.1.	Connection Manager Administration Kit (CMAK).....	413
58.5.	NPS-Zertifikatssperrlistenprüfungen.....	417
58.5.1.	Registrierungseinstellungen.....	419
58.5.2.	Standardkonfiguration der Zertifikatssperrlistenpfade	420
59.	SMARTCARD	421
59.1.	Voraussetzungen für Smartcard-Zertifikate.....	422
59.1.1.	Anforderungen vor Windows Vista.....	422
59.1.2.	Anforderungen ab Windows Vista	422
59.1.3.	Verhaltensänderung bei der Smartcard-Anmeldung ab Windows Vista	422
59.2.	Planung der Smartcard-Bereitstellung	423
59.3.	Bereitstellung von Smartcards ab Windows Vista.....	423
59.4.	Zertifikatvorlagen für Smartcards.....	423
59.4.1.	Anforderungen an die Registrierungsagent-Zertifikate	423
59.4.2.	Anforderungen an die Smartcard-Zertifikatvorlage	427
59.4.3.	Anforderungen an die Smartcard-Zertifikate	432
59.4.4.	Beschränkung der Registrierungsagenten	432
59.5.	Bereitstellungsprozeduren.....	433
59.5.1.	Bereitstellung des Registrierungsagent-Zertifikats	433

59.5.2.	Bereitstellung eines Smartcard-Benutzerzertifikats	436
59.6.	Überlegungen zu diesem Prozess der Smartcard-Bereitstellung.....	440
59.7.	Test Smartcard-Anmeldung.....	441
60.	ZERTIFIKATE FÜR LINUX APACHE WEBSERVER.....	442
60.1.	Zertifikatanforderung erstellen	442
60.2.	Zertifikat anfordern.....	442
60.3.	SAN (Subject Alternative Name).....	443
60.4.	Konvertieren von PFX-Dateien in PEM-Dateien unter Windows	443
60.4.1.	Konvertierung in eine kombinierte PEM-Datei.....	444
60.4.2.	Konvertierung in separate PEM-Dateien.....	444
60.4.3.	Entfernen des Kennworts vom extrahierten privaten Schlüssel	444
60.4.4.	Export des des Zertifikats ohne Schlüssel	444
61.	ANHANG	445
61.1.	Technische Richtlinie – Kryptographische Algorithmen und Schlüssellängen nach BSI 445	
61.2.	Common PKI Spezifikation V2.0 (früher ISIS-MTT).....	447
61.3.	Anforderungen an eine unternehmensinterne PKI	447
61.3.1.	Sicherheitsanforderungen	448
61.3.2.	Technische Anforderungen.....	448
61.4.	Anforderungen an eine unternehmensübergreifende PKI-Architektur.....	448
61.4.1.	Richtlinien und PKI.....	448
61.4.2.	Sicherheitsanforderungen	448
61.4.3.	Technische Anforderungen.....	449