Inhaltsverzeichnis

1. EINLEITUNG 11

1.1. Grundsätzliche PKI Alternativen 11

2. VORAUSSETZUNGEN 12

3. RICHTLINIEN UND PKI 12

3.1. Sicherheitsrichtlinie 12

3.2. Zertifikatrichtlinie 13

3.3. Zertifikatsverwendungserklärung (Certificate Practice Statement, CPS) 13

4. ZERTIFIZIERUNGSSTELLEN TYPEN 14

4.1. Unternehmenszertifizierungsstellen 14

4.2. Eigenständige Zertifizierungsstellen 14

4.3. Unternehmens- und eigenständige Zertifizierungsstellen 14

4.4. Stammzertifizierungsstellen 15

4.5. Untergeordnete Zertifizierungsstellen 15

4.6. Zwischenzertifizierungsstellen 15

5. ENTWURF EINER ZERTIFIZIERUNGSSTELLENHIERARCHIE 15

5.1. Eine dreischichtige Hierarchie wird in folgenden Szenarien empfohlen: 16

6. ORGANISATION DER AUSSTELLENDEN ZERTIFIZIERUNGSSTELLEN 16

7. AUSWAHL EINER ARCHITEKTUR 16

7.1. Wie viele Stufen benötigt eine PKI? 16

8. SAMMLUNG DER ERFORDERLICHEN INFORMATIONEN 18

9. IDENTIFIKATION PKI-FÄHIGER ANWENDUNGEN 18

9.1. PKI-fähige Anwendungen 19

9.2. Identifikation von Zertifikatempfängern 19

10. BESTIMMUNG DER SICHERHEITSANFORDERUNGEN 19

10.1. Räumliche Sicherheit der Offline-Zertifizierungsstellen 19

10.2. Zusätzliche Sicherheitsmaßnahmen für Online-Zertifizierungsstellen 19

10.3. Sicherheitsmaßnahmen in der Konfiguration der Zertifizierungsstellen 20

10.3.1. Beschränkung der Serverrollen 20
10.3.2. Absicherung der Server mit Sicherheitskonfigurations-Assistenten 20
10.3.3. Aktivierung aller Überwachungsoptionen einer Zertifizierungsstelle 20
10.3.4. Aktivierung der BitLocker-Datenträgerverschlüsselung 20
10.3.5. Beschränkung der Mitgliedschaft in lokaler Administratorengruppe 20
10.3.6. Durchsetzung der Rollentrennung 20

10.4. Schutz des privaten Schlüssels der Zertifizierungsstelle 20

10.4.1. Verwendung eines Smartcard-Kryptografie-Dienstanbieters 21
10.4.2. Verwendung von Hardwaresicherheitsmodulen 21
10.4.3. Sichere Gehäuse für Zertifizierungsstellencomputer 21

10.5. Unterschiedliche Sicherheitsanforderungen für Zertifikate 21

11. BESTIMMUNG DER TECHNISCHEN ANFORDERUNGEN 22

11.1. Die Festlegung der PKI Verwaltungsrollen 22

11.2. Die Minimierung des Ausfallrisikos 22

11.3. Die Festlegung der Gültigkeit von Zertifikaten 22

11.4. Wählen der Schlüssellänge 23
11.5. Festlegung der Veröffentlichungspunkte 23
12. ERMITTLUNG DER BETRIEBLICHEN ANFORDERUNGEN 24
12.1. Minimierung der PKI-bezogenen Kosten 24
12.2. Hohe Verfügbarkeit von Zertifizierungsstellen 24
12.3. Haftung der Teilnehmer 24
13. ERMITTLUNG EXTERNER ANFORDERUNGEN 24
13.1. Externe Organisationen möchten Zertifikate verifizieren können 24
13.2. Zertifikate sollen in einer Partnerorganisation genutzt werden 25
13.3. Gesetze 25
13.4. Überprüfung von Zertifikaten in externen oder Perimeter-Netzwerken 25
14. SAMMELN DER AD DS-ANFORDERUNGEN 25
14.1. Namenskonventionen 25
14.2. Auswahl der Domäne 25
14.3. Definieren der Organisationseinheitsstruktur 25
15. IDENTIFIKATION VON ZERTIFIKATEMPFÄNGERN 25
16. PKI-FÄHIGE ANWENDUNGEN 26
17. SSL-VERSCHLÜSSELUNG FÜR WEBSERVER 26
17.1. Webserverzertifikate von Zertifizierungsstellen im eigenen Netz 26
17.2. Webserverzertifikate von Zertifizierungsstellen kommerzieller Anbieter 27
18. REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE 27
19. SICHERE E-MAIL 28
19.1. S/MIME Zertifikate von Zertifizierungsstellen kommerzieller Anbieter 28
19.2. S/MIME Zertifikate von Zertifizierungsstellen im eigenen Netz 28
20. VIRTUELLE PRIVATE NETZWERKE (VPN) 28
21. 802.1X AUTHENTIFIZIERUNG 29
22. EFS-VERSCHLÜSSELUNG 30
23. CODE-SIGNING 30
24. BEREITSTELLUNG VON SMARTCARDS 31
25. VERSCHLÜSSELUNGSARTEN 32
26. ALGORITHMEN UND SCHLÜSSEL 32
27. DATENVERSCHLÜSSELUNG 33
27.1. Symmetrische Verschlüsselung 33
27.2. Asymmetrische Verschlüsselung 34
27.3. Asymmetrische Signatur 35
27.4. Asymmetrische Algorithmen 36
27.5. Kombination von symmetrischer und asymmetrischer Verschlüsselung 37
27.6. Digitale Signatur von Daten 38
27.7. Der Hashvorgang 39
27.8. Hashalgorithmen 39
27.9. Kombination aus asymmetrischer Signatur und Hashalgorithmus 39
27.10. Cryptography Next Generation (CNG) 40

28. INSTALLATION EINER TESTUMGEBUNG 41
29. PLANUNG DER PKI 41
29.1. Planung einer geeigneten Public Key-Infrastruktur (PKI) 41
29.2. Optionale Bereitstellung eines Hardwaresicherheitsmoduls (HSM) 41
29.3. Erstellung einer geeigneten CAPolicy.inf 42
29.4. Auswahl des Setup-Typs der Zertifizierungsstellen 42
30. SOLLZUSTAND WINDOWS SERVER 2016 ZERTIFIKATSDIENSTE 42
31. INSTALLATION EINER ZWEISCHICHTIGEN ZERTIFIZIERUNGSSTELLENHIERARCHIE 43
32. VORBEREITUNG DES DNS SERVERS AUF DEM DC01 44
33. ANPASSUNG DER STANDARD-INSTALLATIONSEINSTELLUNGEN 45
34. KONFIGURATION NACH DER INSTALLATION 47
35. INSTALLATION DER EIGENSTÄNDIGEN STAMMZERTIFIZIERUNGSSTELLE „ROOT CA“ 50
35.1. Vorarbeiten 50
35.2. Parameter 52
35.3. Installation 53
35.4. Abschlussarbeiten - Post Installation Script 58
36. INSTALLATION DER AUSSTELLENDEN ZERTIFIZIERUNGSSTELLE 59
36.1. Parameter 59
36.2. Installation Part 1 59
36.2.1. Request einreichen 65
36.2.2. CA01 - Zertifikat importieren 70
36.3. Abschlussarbeiten - Post Installation Script 71
36.4. Zertifikatsvorlagen bereitstellen 72
36.5. Weitere Zertifizierungsrollen installieren 80
36.5.1. Schnittstelle für die Webregistrierung 84
36.6. Abschlussarbeiten Internetinformationsdienste (IIS) 85
36.7. Installation Part 2 86
36.7.1. Installation des Online-Responders 86
1.1.1. Installation des Registrierungsdienstes für Netzwerkgeräte 93
37. INSTALLATION DES NETWORK POLICY SERVERS (NPS) / RADIUS 100
38. INSTALLATION EINES EXTERNEN WEBSERVERS IN DER DMZ 104
38.1. Erweiterung der Firewall Regeln für den Web01 in der DMZ 105
38.1.1. Installation des IIS 105
38.1.2. Web Server Zertifikat für den Web01 implementieren 106
7.2.3 Verzeichnis für die Zertifizierungsstellen Zertifikate erstellen 118
7.2.4 Automatisierung der Veröffentlichung der Zertifikate und Sperrlisten auf dem Web01 120
39. INSTALLATION EINES KERIO CONNECT MAILSERVERS IN DER DMZ 125
39.1. MX-Eintrag für den Mailserver 126
39.2. Erweiterung der Firewall Regeln für den Mail01 in der DMZ 126
39.3. Windows Firewall konfigurieren 127
39.4. Kerio Connect Schemaerweiterung für den Domian Controllers DC01 130
39.5. Einrichtung des Kerio Connect Mailservers 130

39.5.1. SSL Zertifikat von der Zertifizierungsstelle CA01 installieren 131
39.5.2. Deaktivierung nicht benötigter und unsicherer Diensten 137
39.5.3. Konfiguration der Anbindung an die Active Directory Domäne 139
39.5.4. Test der Active Directory Anbindung 141
40. INSTALLATION EINES VPN-SERVERS IN DER DMZ 142
40.1. Erweiterung der Firewall Regeln für die fw01 in der DMZ 143
40.2. Sicherheitsgruppen für die VPN Clients erstellen 144
40.3. Zertifikatvorlage für den VPN-Server erstellen 144
40.4. Installation der Zertifikate der Stammzertifizierungsstelle (RootCA) und der ausstellenden Zertifizierungsstelle CA01 156
40.5. Konfiguration des Netzwerkrichtlinienservers (RADIUS) 161
40.6. Konfiguration des Rolle Remotezugriff auf dem VPN-Server 163
40.6.1. Eigenschaften Routing und RAS 167
40.7. Konfiguration der lokalen Firewall für die Verwendung von IPsec 170
40.7.1. Globale Einstellungen 170
40.7.2. Verbindunssicherheitsregel (Connection Security Rule) 174
40.7.3. Die Überwachung der IPsec Verbindung 178
40.8. Protokollierung und Firewall-Log 180
41. BEREITSTELLUNG WEITERER ZERTIFIKATE 181
41.1. Zertifikate für Domänencontroller 181
41.2. Zertifikate für Computer 183
41.3. Zertifikat für Benutzer 186
41.4. Zertifikate für Remote Desktop Services 189
42. KONFIGURATION ACCESS POINT (AP01) 192
43. KONFIGURATION RADIUS NAS (SWITCH01) 195
43.1. Die Konfiguration des 802.1X-fähigen Switches erfordert folgende Werte 195
43.2. NPS-Serverkonfiguration auf einen anderen NPS-Server kopieren. 196
43.3. RADIUS-Attribute für VLANs 196
44. IMPLEMENTIERUNG UND KONFIGURATION DER FIREWALL (FW01) 198
44.1. Das Regelwerk 199
44.2. Die Konfiguration als Textdatei 199
45. WINDOWS ENTERPRISE ZERTIFIKATSDIENSTE NUTZEN 207
45.1. Server Manager 207
45.2. Management der Zertifizierungsstelle 210
45.3. Zertifikatvorlagen 210
45.4. Ausrollen und automatisches Registrieren der Zertifikate 212
45.5. OCSP 214
45.6. Schnittstelle für die Webregistrierung 215
45.7. Erstellung eines Benutzer Zertifikats 217
45.8. Zertifikat der Zertifizierungsstelle *(RootCA Certificate)* 219
45.9. Verwaltung von Client Zertifikaten 221
45.10. Zertifikate exportieren 222

45.11. Zertifikate sperren und freigeben 224

45.12. Backup 227
45.12.1. Manuelle Sicherung mit der Konsole Zertifizierungsstelle 227
45.12.2. Automatische Sicherung mittels Certutil-Befehl 229

45.13. Certutil - Zertifikate löschen und verwalten 230
46. KEY RECOVERY AGENT 231

46.1. Schlüssel mit dem Key Recovery Agent wiederherstellen 238
47. REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE 239
48. WIFI MIT 802.1X AUTHENTIFIZIERUNG 241

48.1. EAP-TLS-Authentifizierung 241

48.2. PEAP-Authentifizierung 242

48.3. Funktionsweise der 802.1x Authentifizierung 242

48.4. Zusammenfassung des Prozesses zum Einbuchen in das WLAN. 244

48.5. Sicherheitsbedenken 245
48.5.1. EAP-TLS (Transport Layer Security) 245
48.5.2. EAP-PEAP (Protected EAP) 245

48.6. Bereitstellung der benötigten Zertifikate 245

48.7. Externe Wifi-Devices 245
48.7.1. Manuelle Verwaltung und Konfiguration 246
48.7.2. Registrierungsdienst für Netzwerkgeräte 246
48.7.3. Mobile-Device-Management (MDM) 247
49. IMPLEMENTIERUNG 802.1X - WIFI FÜR AD-DS-INTEGRIERTE CLIENTS 247

49.1. Konfiguration der Wifi-Devices (EAP-TLS) 247

49.2. Computer-Zertifikat für das Wifi-Device 247

49.3. Sicherheitsgruppen erstellen 249

49.4. GPOs erstellen 249

49.5. Netzwerkrichtlinienserver NPS (RADIUS) 257

49.6. Konfiguration weiterer Bedingungen für die Verbindungsanforderung 262

49.7. Test eines AD-DS-integrierten Wifi-Devices 264
50. IMPLEMENTIERUNG 802.1X – WIFI FÜR NICHT-AD-DS-INTEGRIERTE CLIENTS 265

50.1. PEAP 265
50.1.1. Sicherheitsgruppe erstellen 265
50.1.2. Netzwerkrichtlinienserver NPS (RADIUS) 266
50.1.3. Konfiguration weiterer Bedingungen für die Verbindungsanforderung 268
50.1.4. Test eines Nicht-AD-DS-integrierten Wifi-Devices 268

50.2. EAP (TLS) und PEAP 270

50.3. iPhone Enterprise Integration mit EAP-TLS 271
50.3.1. Benutzer-Zertifikat für das externe Device (EAP-TLS) 271
50.3.2. iPhone Configuration Utility 3.6.2 for Windows 278
50.3.3. Test der iPhone EAP (TLS) Verbindung 281
51. WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG 284

51.1. Sicherheitsbedenken 287
52. IMPLEMENTIERUNG WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG FÜR AD-DS-INTEGRIERTE CLIENTS 287

52.1. Konfiguration der Wired-Access-Devices (EAP-TLS) 287
52.2. Computer-Zertifikat für das Wired-Access-Devices 287
52.3. Sicherheitsgruppe erstellen 288
52.4. GPOs erstellen 289
52.5. Netzwerkrichtlinienserver NPS (RADIUS) 292
52.6. Beispiel NAS (Switch) Konfiguration 299
52.7. Test 300
53. WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG FÜR EXTERNE CLIENTS 301
53.1. Konfiguration externer Wired-Access-Clients (PEAP) 301
53.1.1. Netzwerkrichtlinienserver NPS (RADIUS) 301
53.1.2. Test 302
53.2. Konfiguration externer Wired-Access Clients EAP (TLS) 303
53.2.1. Benutzer-Zertifikat für das externe Device 303
53.2.2. Netzwerkrichtlinienserver NPS (RADIUS) 311
53.2.3. Test 311
54. NDES KONFIGURATION FÜR SCEP (CISCO ASA SCEP PROXY) 312
54.1. Windows Server Konfiguration 312
54.2. Cisco ASA Konfiguration per ASDM 315
54.1. Cisco ASA Konfiguration per Command-Line Interface (CLI) für AnyConnect 322
55. EFS-VERSCHLÜSSELUNG 328
55.1. Zertifikatvorlagen für die EFS-Verschlüsselung 328
55.2. Das EFS-Verschlüsselungszertifikat 328
55.3. Lokale EFS-Verschlüsselung 328
55.4. Remoteverschlüsselung 329
55.5. EFS-Entschlüsselung 330
55.6. EFS-Datenwiederherstellung 330
55.7. Wiederherstellungsmethoden 331
55.7.1. Datenwiederherstellung 332
55.7.2. Sichern des privaten Schlüssels 340
55.7.3. Schlüsselwiederherstellung 341
55.8. Aktivierung und Deaktivierung von EFS 341
55.9. Ausrollen der EFS-Benutzerzertifikate 343
56. SICHERE E-MAIL 349
56.1. Secure/Multipose Internet Mail Extensions (S/MIME) 349
56.2. Verschlüsselung von E-Mail 350
56.3. SSL für Internetprotokolle 351
56.3.1. SSL-Ports für E-Mail Protokolle 352
56.4. E-Mail Server Zertifikat 352
56.5. Auswahl der Zertifikatvorlagen 352
56.5.1. Eine Zertifikatvorlage für Signatur und Verschlüsselung 352
56.5.1. Separate Zertifikatvorlage für Signatur und Verschlüsselung 355
56.6. Aktivierung von Outlook 2016 359
56.6.1. Einrichtung des Kerio Outlook Connector (Offline Edition) 359

56.6.2. Anforderung des S/MIME Zertifikats 361
56.6.3. Einbindung des Zertifikats in Outlook 366
56.6.4. Einbindung des Zertifikats in Kerio Web Frontend 371
56.6.5. Funktionstest 374
57. VPN INFRASTRUKTUR MIT WINDOWS SERVER 377
57.1. L2TP/IPsec 378
57.2. IPsec (IKEv2) 380
57.3. Konfiguration des VPN Clients für IKEv2 / IPsec 381
57.3.1. Erstellung der Zertifikatvorlage für den VPN-Clientcomputer 382
57.3.2. Gruppenrichtlinie für die automatische Registrierung erstellen 385
57.3.3. DNS Auflösung des Common Name (CN) des VPN-Servers 386
57.3.4. IKEv2 VPN-Verbindung am Client einrichten 387
57.4. Deployment / Rollout der VPN Client Konfiguration 393
57.4.1. Connection Manager Administration Kit (CMAK) 393
57.5. NPS-Zertifikatsperrlistenprüfungen 397
57.5.1. Registrierungseinstellungen 399
57.5.2. Standardkonfiguration der Zertifikatssperrlistenpfade 400
58. SMARTCARD 401
58.1. Voraussetzungen für Smartcard-Zertifikate 402
58.1.1. Anforderungen vor Windows Vista 402
58.1.2. Anforderungen ab Windows Vista 402
58.1.3. Verhaltensänderung bei der Smartcard-Anmeldung ab Windows Vista 402
58.2. Planung der Smartcard-Bereitstellung 403
58.3. Bereitstellung von Smartcards ab Windows Vista 403
58.4. Zertifikatvorlagen für Smartcards 403
58.4.1. Anforderungen an die Registrierungsagent-Zertifikate 403
58.4.2. Anforderungen an die Smartcard-Zertifikatvorlage 407
58.4.3. Anforderungen an die Smartcard-Zertifikate 412
58.4.4. Beschränkung der Registrierungsagenten 412
58.5. Bereitstellungsprozeduren 413
58.5.1. Bereitstellung des Registrierungsagent-Zertifikats 413
58.5.2. Bereitstellung eines Smartcard-Benutzerzertifikats 416
58.6. Überlegungen zu diesem Prozess der Smartcard-Bereitstellung 420
58.7. Test Smartcard-Anmeldung 421
59. ZERTIFIKATE FÜR LINUX APACHE WEBSERVER 422
59.1. Zertifikatanforderung erstellen 422
59.2. Zertifikat anfordern 422
59.3. SAN (Subject Alternative Name) 423
59.4. Konvertieren von PFX-Dateien in PEM-Dateien unter Windows 423
59.4.1. Konvertierung in eine kombinierte PEM-Datei 424
59.4.2. Konvertierung in separate PEM-Dateien 424
59.4.3. Entfernen des Kennworts vom extrahierten privaten Schlüssel 424
59.4.4. Export des des Zertifikats ohne Schlüssel 424
60. ANHANG 425
60.1. Common PKI Spezifikation V2.0 (früher ISIS-MTT) 425
60.2. Anforderungen an eine unternehmensinterne PKI 425
60.2.1. Sicherheitsanforderungen 425
60.2.2. Technische Anforderungen 426
60.3. Anforderungen an eine unternehmensübergreifende PKI-Architekturen 426