Michael Buth
it berater

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 19

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. Wahl der Schlüssellänge 23
11.5. Ausstellung von Zertifikaten 24
11.6. Festlegung der Veröffentlichungspunkte 24
12. ERMITTLUNG DER BETRIEBLICHEN ANFORDERUNGEN 24
12.1. Minimierung der PKI-bezogenen Kosten 25
12.2. Hohe Verfügbarkeit von Zertifizierungsstellen 25
12.3. Haftung der Teilnehmer 25
13. ERMITTLUNG EXTERNER ANFORDERUNGEN 25
13.1. Externe Organisationen möchten Zertifikate verifizieren können 25
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 26
14.1. Namenskonventionen 26
14.2. Auswahl der Domäne 26
14.3. Definieren der Organisationseinheitsstruktur 26
15. IDENTIFIKATION VON ZERTIFIKATEMPFÄNGERN 26
16. PKI-FÄHIGE ANWENDUNGEN 26
17. SSL-VERSCHLÜSSELUNG FÜR WEBSERVER 27
17.1. Webserverzertifikate von Zertifizierungsstellen im eigenen Netz 27
17.2. Webserverzertifikate von Zertifizierungsstellen kommerzieller Anbieter 27
18. REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE 28
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 29
20. VIRTUELLE PRIVATE NETZWERKE (VPN) 29
21. 802.1X AUTHENTIFIZIERUNG 29
22. EFS-VERSCHLÜSSELUNG 30
23. CODE-SIGNING 30
24. BEREITSTELLUNG VON SMARTCARDS 32
25. VERSCHLÜSSELUNGSARTEN 32
26. ALGORITHMEN UND SCHLÜSSEL 33
27. DATENVERSCHLÜSSELUNG 34
27.1. Symmetrische Verschlüsselung 34
27.2. Asymmetrische Verschlüsselung 35
27.3. Asymmetrische Signatur 36
27.4. Asymmetrische Algorithmen 37
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 PKI 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“ 49
35.1. Vorarbeiten 49
35.2. Parameter 51
35.3. Installation 52
35.4. Abschlussarbeiten - Post Installation Script 57
35.5. Publish Root CA Cert und CRL 57
36. INSTALLATION DER AUSSTELLENDEN ZERTIFIZIERUNGSSTELLE 58
36.1. Parameter 58
36.2. Installation Part 1 58
36.2.1. Request einreichen 64
36.2.2. CA01 - Zertifikat importieren 69
36.3. Abschlussarbeiten - Post Installation Script 70
36.4. Zertifikatsvorlagen bereitstellen 71
36.5. Weitere Zertifizierungsrollen installieren 79
36.5.1. Schnittstelle für die Webregistrierung 83
36.6. Abschlussarbeiten Internetinformationsdienste (IIS) 84
36.7. Installation Part 2 85
36.7.1. Installation des Online-Responders 85
1.1.1. Installation des Registrierungsdienstes für Netzwerkgeräte 92
37. INSTALLATION DES NETWORK POLICY SERVERS (NPS) / RADIUS 99
38. INSTALLATION EINES EXTERNEN WEBSERVERS IN DER DMZ 103
38.1. Erweiterung der Firewall Regeln für den Web01 in der DMZ 104
38.1.1. Installation des IIS 104
38.1.2. Web Server Zertifikat für den Web01 implementieren 105
7.2.3 Verzeichnis für die Zertifizierungsstellen Zertifikate erstellen 117
7.2.4 Automatisierung der Veröffentlichung der Zertifikate und Sperrlisten auf dem Web01 119
39. INSTALLATION EINES KERIO CONNECT MAILSERVERS IN DER DMZ 124
39.1. MX-Eintrag für den Mailserver 125
39.2. Erweiterung der Firewall Regeln für den Mail01 in der DMZ 125
39.3. Windows Firewall konfigurieren 126

39.4. Kerio Connect Schemaerweiterung für den Domian Controllers DC01 129

39.5. Einrichtung des Kerio Connect Mailservers 129
39.5.1. SSL Zertifikat von der Zertifizierungsstelle CA01 installieren 130
39.5.2. Deaktivierung nicht benötigter und unsicherer Diensten 136
39.5.3. Konfiguration der Anbindung an die Active Directory Domäne 138
39.5.4. Test der Active Directory Anbindung 140

40. INSTALLATION EINES VPN-SERVERS IN DER DMZ 141

40.1. Erweiterung der Firewall Regeln für die fw01 in der DMZ 142

40.2. Sicherheitsgruppen für die VPN Clients erstellen 143

40.3. Zertifikatvorlage für den VPN-Server erstellen 143

40.4. Installation der Zertifikate der Stammzertifizierungsstelle (RootCA) und der ausstellenden Zertifizierungsstelle CA01 155

40.5. Konfiguration des Netzwerkrichtlinienservers (RADIUS) 160

40.6. Konfiguration des Rolle Remotezugriff auf dem VPN-Server 162
40.6.1. Eigenschaften Routing und RAS 166

40.7. Konfiguration der lokalen Firewall für die Verwendung von IPsec 169
40.7.1. Globale Einstellungen 169
40.7.2. Verbindunssicherheitsregel (Connection Security Rule) 173
40.7.3. Die Überwachung der IPsec Verbindung 177

40.8. Protokollierung und Firewall-Log 179

41. BEREITSTELLUNG WEITERER ZERTIFIKATE 180

41.1. Zertifikate für Domänencontroller 180

41.2. Zertifikate für Computer 182

41.3. Zertifikat für Benutzer 185

41.4. Zertifikate für Remote Desktop Services 188

42. KONFIGURATION ACCESS POINT (AP01) 191

43. KONFIGURATION RADIUS NAS (SWITCH01) 194

43.1. Die Konfiguration des 802.1X-fähigen Switches erfordert folgende Werte 194

43.2. Alternativ: Konfiguration eine HP Procurve Switches 195
43.2.1. Konfiguration der benötigten Parameter an der Console des Switches 196

44. IMPLEMENTIERUNG UND KONFIGURATION DER FIREWALL (FW01) 197

44.1. Das Regelwerk 197

44.2. Die Konfiguration als Textdatei 197

45. WINDOWS ZERTIFIKATSDIENSTE NUTZEN 206

45.1. Server Manager 206

45.2. Management der Zertifizierungsstelle 206

45.3. Zertifikatvorlagen 207

45.4. Ausrollen und automatisches Registrieren der Zertifikate 209

45.5. OCSP 210

45.6. Schnittstelle für die Webregistrierung 211

45.7. Erstellung eines Benutzer Zertifikats 213

45.8. Zertifikat der Zertifizierungsstelle *(RootCA Certificate)* 215

45.9. Verwaltung von Client Zertifikaten 217

45.10. Zertifikate exportieren 218
45.11. Zertifikate sperren und freigeben 220
45.12. Backup 223
45.12.1. Manuelle Sicherung mit der Konsole Zertifizierungsstelle 223
45.12.2. Automatische Sicherung mittels Certutil-Befehl 225
45.13. Certutil - Zertifikate löschen und verwalten 226
46. KEY RECOVERY AGENT 227
46.1. Schlüssel mit dem Key Recovery Agent wiederherstellen 234
47. REGISTRIERUNGSDIENST FÜR NETZWERKGERÄTE 235
48. WIFI MIT 802.1X AUTHENTIFIZIERUNG 237
48.1. EAP-TLS-Authentifizierung 237
48.2. PEAP-Authentifizierung 238
48.3. Funktionsweise der 802.1x Authentifizierung 238
48.4. Zusammenfassung des Prozesses zum Einbuchen in das WLAN. 240
48.5. Sicherheitsbedenken 241
48.5.1. EAP-TLS (Transport Layer Security) 241
48.5.2. EAP-PEAP (Protected EAP) 241
48.6. Bereitstellung der benötigten Zertifikate 241
48.7. Externe Wifi-Devices 241
48.7.1. Manuelle Verwaltung und Konfiguration 242
48.7.2. Registrierungsdienst für Netzwerkgeräte 242
48.7.3. Mobile-Device-Management (MDM) 243
49. IMPLEMENTIERUNG 802.1X - WIFI FÜR AD-DS-INTEGRIERTE CLIENTS 243
49.1. Konfiguration der Wifi-Devices (EAP-TLS) 243
49.2. Computer-Zertifikat für das Wifi-Device 243
49.3. Sicherheitsgruppen erstellen 245
49.4. GPOs erstellen 245
49.5. Netzwerkrichtlinienserver NPS (RADIUS) 253
49.6. Konfiguration weiterer Bedingungen für die Verbindungsanforderung 258
49.7. Test eines AD-DS-integrierten Wifi-Devices 260
50. IMPLEMENTIERUNG 802.1X – WIFI FÜR NICHT-AD-DS-INTEGRIERTE CLIENTS 261
50.1. PEAP 261
50.1.1. Sicherheitsgruppe erstellen 261
50.1.2. Netzwerkrichtlinienserver NPS (RADIUS) 262
50.1.3. Konfiguration weiterer Bedingungen für die Verbindungsanforderung 264
50.1.4. Test eines Nicht-AD-DS-integrierten Wifi-Devices 264
50.2. EAP (TLS) und PEAP 266
50.3. iPhone Enterprise Integration mit EAP-TLS 267
50.3.1. Benutzer-Zertifikat für das externe Device (EAP-TLS) 267
50.3.2. iPhone Configuration Utility 3.6.2 for Windows 274
50.3.3. Test der iPhone EAP (TLS) Verbindung 277
51. WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG 280
51.1. Sicherheitsbedenken 283

52. IMPLEMENTIERUNG WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG FÜR AD-DS-INTEGRIERTE CLIENTS 283

52.1. Konfiguration der Wired-Access-Devices (EAP-TLS) 283

52.2. Computer-Zertifikat für das Wired-Access-Devices 283

52.3. Sicherheitsgruppe erstellen 284

52.4. GPOs erstellen 285

52.5. Netzwerkrichtlinienserver NPS (RADIUS) 288

52.6. NPS-Serverkonfiguration auf einen anderen NPS-Server kopieren. 294

52.7. RADIUS-Attribute für VLANs 295

52.8. Test 296

53. TRIUMPF ADLER (KYOCERA) DRUCKER MIT 802.1X AUTHENTIFIZIERUNG 297

53.1. EEE 802.1X-Authentifizierungseinstellung 297

53.2. Zertifikat der Zertifizierungsstelle importieren 298

53.3. Benutzerzertifikat anfordern und importieren 301

54. WIRED ACCESS MIT 802.1X AUTHENTIFIZIERUNG FÜR EXTERNE CLIENTS 310

54.1. Konfiguration externer Wired-Access-Clients (PEAP) 310

54.1.1. Netzwerkrichtlinienserver NPS (RADIUS) 310

54.1.2. Test 310

54.2. Konfiguration externer Wired-Access Clients EAP (TLS) 312

54.2.1. Benutzer-Zertifikat für das externe Device 312

54.2.2. Netzwerkrichtlinienserver NPS (RADIUS) 319

54.2.3. Test 319

55. NDES KONFIGURATION FÜR SCEP (CISCO ASA SCEP PROXY) 320

55.1. Windows Server Konfiguration 320

55.2. Cisco ASA Konfiguration per ASDM 323

55.1. Cisco ASA Konfiguration per Command-Line Interface (CLI) für AnyConnect 330

56. EFS-VERSCHLÜSSELUNG 336

56.1. Zertifikatvorlagen für die EFS-Verschlüsselung 336

56.2. Das EFS-Verschlüsselungszertifikat 336

56.3. Lokale EFS-Verschlüsselung 336

56.4. Remoteverschlüsselung 337

56.5. EFS-Entschlüsselung 338

56.6. EFS-Datenwiederherstellung 338

56.7. Wiederherstellungsmethoden 339

56.7.1. Datenwiederherstellung 340

56.7.2. Sichern des privaten Schlüssels 348

56.7.3. Schlüsselwiederherstellung 349

56.8. Aktivierung und Deaktivierung von EFS 349

56.9. Ausrollen der EFS-Benutzerzertifikate 351

57. SICHERE E-MAIL 357

57.1. Secure/Multipose Internet Mail Extensions (S/MIME) 357

57.2. Verschlüsselung von E-Mail 358

57.3. SSL für Internetprotokolle 359
57.3.1. SSL-Ports für E-Mail Protokolle 360

57.4. E-Mail Server Zertifikat 360

57.5. Auswahl der Zertifikatvorlagen 360
57.5.1. Eine Zertifikatvorlage für Signatur und Verschlüsselung 360
57.5.1. Separate Zertifikatvorlage für Signatur und Verschlüsselung 363

57.6. Aktivierung von Outlook 2016 367
57.6.1. Einrichtung des Kerio Outlook Connector (Offline Edition) 367
57.6.2. Anforderung des S/MIME Zertifikats 369
57.6.3. Einbindung des Zertifikats in Outlook 374
57.6.4. Einbindung des Zertifikats in Kerio Web Frontend 379
57.6.5. Funktionstest 382

58. VPN INFRASTRUKTUR MIT WINDOWS SERVER 385

58.1. L2TP/IPsec 386

58.2. IPsec (IKEv2) 388

58.3. Konfiguration des VPN Clients für IKEv2 / IPsec 389
58.3.1. Erstellung der Zertifikatvorlage für den VPN-Clientcomputer 390
58.3.2. Gruppenrichtlinie für die automatische Registrierung erstellen 393
58.3.3. DNS Auflösung des Common Name (CN) des VPN-Servers 394
58.3.4. IKEv2 VPN-Verbindung am Client einrichten 395

58.4. Deployment / Rollout der VPN Client Konfiguration 401
58.4.1. Connection Manager Administration Kit (CMAK) 401

58.5. NPS-Zertifikatsperrlistenprüfungen 405
58.5.1. Registrierungseinstellungen 407
58.5.2. Standardkonfiguration der Zertifikatssperrlistenpfade 408

59. SMARTCARD 409

59.1. Voraussetzungen für Smartcard-Zertifikate 410
59.1.1. Anforderungen vor Windows Vista 410
59.1.2. Anforderungen ab Windows Vista 410
59.1.3. Verhaltensänderung bei der Smartcard-Anmeldung ab Windows Vista 410

59.2. Planung der Smartcard-Bereitstellung 411

59.3. Bereitstellung von Smartcards ab Windows Vista 411

59.4. Zertifikatvorlagen für Smartcards 411
59.4.1. Anforderungen an die Registrierungsagent-Zertifikate 411
59.4.2. Anforderungen an die Smartcard-Zertifikatvorlage 415
59.4.3. Anforderungen an die Smartcard-Zertifikate 420
59.4.4. Beschränkung der Registrierungsagenten 420

59.5. Bereitstellungsprozeduren 421
59.5.1. Bereitstellung des Registrierungsagent-Zertifikats 421
59.5.2. Bereitstellung eines Smartcard-Benutzerzertifikats 424

59.6. Überlegungen zu diesem Prozess der Smartcard-Bereitstellung 428

59.7. Test Smartcard-Anmeldung 429

60. ZERTIFIKATE FÜR LINUX APACHE WEBSERVER 430

60.1. Zertifikatanforderung erstellen 430

60.2. Zertifikat anfordern 430

60.3. SAN (Subject Alternative Name) 431

60.4. Konvertieren von PFX-Dateien in PEM-Dateien unter Windows 431

60.4.1. Konvertierung in eine kombinierte PEM-Datei 432
60.4.2. Konvertierung in separate PEM-Dateien 432
60.4.3. Entfernen des Kennworts vom extrahierten privaten Schlüssel 432
60.4.4. Export des des Zertifikats ohne Schlüssel 432
61. ANHANG 433
61.1. Technische Richtlinie – Kryptographische Algorithmen und Schlüssellängen nach BSI 433
61.2. Common PKI Spezifikation V2.0 (früher ISIS-MTT) 435
61.3. Anforderungen an eine unternehmensinterne PKI 435
61.3.1. Sicherheitsanforderungen 436
61.3.2. Technische Anforderungen 436
61.4. Anforderungen an eine unternehmensübergreifende PKI-Architekturen 436
61.4.1. Richtlinien und PKI 436
61.4.2. Sicherheitsanforderungen 436
61.4.3. Technische Anforderungen 437