Übung 24.1.1

- Untersuchen Sie die vorhandenen Zertifikatvorlagen
- Betrachten Sie die Unterschiede zwischen den Versionen
- Duplizieren Sie die Vorlage „EFS-Wiederherstellungs-Agent“
- Überprüfen Sie, ob Sie von „W11“ als „Karl Klammer“ ein Zertifikat auf Basis dieser neuen Vorlage anfordern können
- Überprüfen Sie, ob Sie von „W11“ als „Meistertraineradministrator“ ein Zertifikat auf Basis dieser neuen Vorlage anfordern können
- Begründen Sie, warum das so ist

Lösung 24.1.1

- Wechseln Sie zur virtuellen Maschine „Server2“
- Tippen Sie unten in der Taskleiste neben der Lupe ein: „MMC“
- Klicken Sie auf „MMC“
- Wählen Sie in der Konsole
    - Datei
    - Snap-In hinzufügen/entfernen
    - Zertifikatvorlage
    - Hinzufügen
    - OK
- Klicken Sie auf der linken Seite des Fensters auf „Zertifikatvorlagen“
- Öffnen Sie eine beliebige Vorlage der Version 1
    - Sie kann nicht verändert werden
    - Sie hat nur wenige Registerkarten (5)
    - Registerkarte Allgemein: kann ab Zertifizierungsstelle Windows 2000 benutzt werden
- Schließen Sie diese Vorlage wieder
- Öffnen Sie eine beliebige Vorlage der Version 2
    - Sie kann verändert werden
    - Sie hat mehr Einstellmöglichkeiten, deswegen auch mehr Registerkarten
    - Registerkarte Kompatibilität:
        - Mindestens Server 2003/Windows XP
- Schließen Sie diese Vorlage wieder
- Öffnen Sie eine beliebige Vorlage der Version 3

    - Sie kann verändert werden
    - Sie hat mehr Einstellmöglichkeiten, deswegen auch mehr Registerkarten
    - Registerkarte Kompatibilität:
        - Mindestens Server 2008R2/Windows Vista
- Schließen Sie diese Vorlage wieder
- Lassen Sie die MMC geöffnet

Duplizieren der Vorlage

- Klicken Sie in der MMC mit der rechten Maustaste auf die Vorlage „EFS-Wiederherstellungs-Agent“
- Wählen Sie
    - Vorlage duplizieren
    - Registerkarte „Allgemein“:
    - Vorlagenanzeigenname „Neuer EFS-Wiederherstellungs-Agent“
    - OK
- Lassen Sie die Konsole geöffnet
- Wählen Sie im Server-Manager
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
    - Zertifikatvorlagen
    - Klicken Sie mit der rechten Maustaste
        - Neu
        - Auszustellende Zertifikatvorlage
        - Neuer EFS-Wiederherstellungs-Agent
        - OK

Überprüfung der Anforderung

- Wechseln Sie zur virtuellen Maschine „W11“
- Melden Sie sich als „Karl Klammer“ an der Maschine an
- Klicken Sie auf „Start“
- Geben Sie oben bei „Suchbegriff hier eingeben“ ein
    - MMC
- Wählen Sie „MMC Befehl ausführen“
- Klicken Sie in der Konsole auf
    - Datei
    - Snap-In hinzufügen/entfernen

- Scrollen Sie auf der linken Seite bei „Verfügbare Snap-Ins“ ganz nach unten und wählen Sie
    - Zertifikate
    - Hinzufügen
    - OK
- Erweitern Sie
    - Zertifikate – Aktueller Benutzer
    - Eigene Zertifikate
    - Zertifikate
- Klicken Sie mit der rechten Maustaste
    - Alle Aufgaben
    - Ein neues Zertifikat anfordern
- Zertifikatregistrierungsassistent
    - Vorbereitung: Weiter
    - Zertifikatregistrierungsrichtlinie auswählen: Weiter
    - Zertifikate anfordern
        - Alle Vorlagen anzeigen
        - Scrollen bis zu „Neuer EFS-Wiederherstellungs-Agent“
    - Brechen Sie an dieser Stelle ab

Überprüfung der Anforderung als Administrator

- Melden Sie sich als „Karl Klammer“ an der Maschine ab
- Melden Sie sich als „Meistertrainer/Administrator“ an der Maschine an
- Klicken Sie auf „Start“
- Geben Sie oben bei „Suchbegriff hier eingeben“ ein
    - MMC
- Wählen Sie „MMC Befehl ausführen“
- Klicken Sie in der Konsole auf
    - Datei
    - Snap-In hinzufügen/entfernen
- Scrollen Sie auf der linken Seite bei „Verfügbare Snap-Ins“ ganz nach unten und wählen Sie
    - Zertifikate
    - Hinzufügen
    - OK
- Erweitern Sie
    - Zertifikate – Aktueller Benutzer
    - Eigene Zertifikate
    - Zertifikate

- Klicken Sie mit der rechten Maustaste
    - Alle Aufgaben
    - Ein neues Zertifikat anfordern
- Zertifikatregistrierungsassistent
    - Vorbereitung: Weiter
    - Zertifikatregistrierungsrichtlinie auswählen: Weiter
    - Zertifikate anfordern
- Sie sehen, dass Sie weitaus mehr verschiedene Zertifikate anfordern können
- Brechen Sie die Registrierung ab
- Melden Sie sich von der Maschine „W11“ ab

Begründung

- Offensichtlich hat der Benutzer „Karl Klammer“ nicht die Rechte, alle Vorlage für die Zertifikatanforderung zu benutzen

Übung 24.1.2

- Bearbeiten Sie die Berechtigungen der Vorlage „Neuer EFS-Wiederherstellungs-Agent“, um einem Standardbenutzer zu erlauben, diese Vorlage zu registrieren
- Überprüfen Sie danach, ob Sie nun von „W11“ als „Karl Klammer“ ein Zertifikat auf Basis dieser neuen Vorlage anfordern können

Lösung 24.1.2

Erteilen der Berechtigungen

- Wechseln Sie zur virtuellen Maschine „Server2“
- Falls Sie die zuvor erstellte MMC noch geöffnet haben, wechseln Sie auf diese
- Sonst erstellen Sie die MMC neu:
- Tippen Sie unten in der Taskleiste neben der Lupe ein: „MMC“
- Klicken Sie auf „MMC“
- Wählen Sie in der Konsole
    - Datei
    - Snap-In hinzufügen/entfernen
    - Zertifikatvorlage
    - Hinzufügen
    - OK

- Klicken Sie auf der linken Seite des Fensters auf „Zertifikatvorlagen“
- Suchen Sie im rechten Fenster nach der Vorlage „Neuer EFS-Wiederherstellungs-Agent“, und öffnen Sie diese
- Wechseln Sie zur Registerkarte „Sicherheit“
- Wählen Sie im oberen Teil die Gruppe „Authentifizierte Benutzer“
- Geben Sie im unteren Teil die Berechtigung „Registrieren-Zulassen“
- Klicken Sie auf „OK“

Überprüfung

- Wechseln Sie zur virtuellen Maschine „W11“
- Melden Sie sich als „Karl Klammer“ an der Maschine an
- Klicken Sie auf „Start“
- Geben Sie oben bei „Suchbegriff hier eingeben“ ein
    - MMC
- Wählen Sie „MMC Befehl ausführen“
- Klicken Sie in der Konsole auf
    - Datei
    - Snap-In hinzufügen/entfernen
- Scrollen Sie auf der linken Seite bei „Verfügbare Snap-Ins“ ganz nach unten und wählen Sie
    - Zertifikate
    - Hinzufügen
    - OK
- Erweitern Sie
    - Zertifikate – Aktueller Benutzer
    - Eigene Zertifikate
    - Zertifikate
- Klicken Sie mit der rechten Maustaste
    - Alle Aufgaben
    - Ein neues Zertifikat anfordern
- Zertifikatregistrierungsassistent
    - Vorbereitung: Weiter
    - Zertifikatregistrierungsrichtlinie auswählen: Weiter
    - Zertifikate anfordern
- Sie sehen, dass nun die Vorlage „Neuer EFS-Wiederherstellungs-Agent“ für Anforderungen benutzt werden kann

Übung 24.2

- Sie möchten, dass sich Ihre Benutzer per Smartcard anmelden, und dafür sollen Zertifikate automatisch erteilt werden
- Stellen Sie alle Schritte anhand der Beschreibungen und Abbildungen im Buch nach

Lösung 24.2

Erstellen der Sicherheitsgruppe

- Wechseln Sie zur virtuellen Maschine „DC“
- Wählen Sie
    - Tools
    - Active Directory-Benutzer und –Computer
- Wählen Sie auf der linken Seite
    - Meistertrainer.info
    - Users
- Klicken Sie mit der rechten Maustaste und wählen Sie
    - Neu
    - Gruppe
    - Nennen Sie die Gruppe „Smartcardanmeldung“
    - Lassen Sie „Globale Gruppe“
    - OK
- Klicken Sie doppelt auf die eben erstellte Gruppe und wechseln Sie zur Registerkarte „Mitglieder“
- Fügen Sie hinzu
    - Domänen-Admins
    - Domänen-Benutzer
    - OK

Erstellen der Zertifikatvorlage

- Wechseln Sie zur virtuellen Maschine „Server2“
- Falls Sie die zuvor erstellte MMC noch geöffnet haben, wechseln Sie auf diese
- Sonst erstellen Sie die MMC neu:
- Tippen Sie unten in der Taskleiste neben der Lupe ein: „MMC“
- Klicken Sie auf „MMC“
- Wählen Sie in der Konsole
    - Datei

    - Snap-In hinzufügen/entfernen
    - Zertifikatvorlage
    - Hinzufügen
    - OK
- Klicken Sie auf der linken Seite des Fensters auf „Zertifikatvorlagen“
- Wählen Sie auf der rechten Seite die Vorlage „Smartcard-Benutzer“ aus und klicken Sie mit der rechten Maustaste
    - Vorlage duplizieren
- Registerkarte „Allgemein“
    - Vorlagenanzeigenamen: Smartcard-Benutzer-Autoenrollment
- Registerkarte „Sicherheit“
    - Hinzufügen: Gruppe Smartcardanmeldung
- Ändern der Berechtigungen für diese Gruppe
    - Lesen
    - Registrieren
    - Automatisch registrieren
    - OK

Veröffentlichen der Zertifikatvorlage

- Wählen Sie im Server-Manager von Server2
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
    - Zertifikatvorlagen
    - Klicken Sie mit der rechten Maustaste
        - Neu
        - Auszustellende Zertifikatvorlage
        - Smartcard-Benutzer-Autoenrollment
        - OK

Konfigurieren der Gruppenrichtlinie

- Wechseln Sie zur virtuellen Maschine „DC“
- Wählen Sie
    - Tools
    - Gruppenrichtlinienverwaltung
- Navigieren Sie zu

    - Domänen
    - Meistertrainer.info
    - Default Domain Policy
- Klicken Sie mit der rechten Maustaste und wählen Sie „Bearbeiten“
- Navigieren Sie zu
    - Benutzerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Richtlinien für öffentliche Schlüssel
- Klicken Sie auf der rechten Seite auf „Zertifikatdienstclient –Automatische Registrierung“
    - Eigenschaften
    - Konfigurationsmodell: Aktiviert
    - OK

Übung 24.3

- Sichern Sie die Zertifikatdatenbank mithilfe des Sicherungsprogramms der CA

Lösung 24.3

- Wechseln Sie zur virtuellen Maschine „Server2“
- Erstellen Sie im Windows Explorer auf Laufwerl C:\ einen Ordner mit Namen „Certbackup“

- Wählen Sie im Server-Manager
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
- Klicken Sie mit der rechten Maustaste
    - Alle Aufgaben
    - Zertifizierungsstelle sichern
- Folgen Sie dem Assistenten
    - Willkommen: Weiter
    - Zu sichernde Elemente
        - Privater Schlüssel und Zertifizierungsstellenzertifikat
        - Zertifikatdatenbank und Zertifikatdatenbankprotokoll

        - Sicherungspfad: C:\CertBackup
        - Weiter
    - Kennwort auswählen:
        - Kennw0rt!
        - Bestätigen
        - Weiter
    - Fertigstellen des Assistenten:
        - Fertig stellen

Übung 24.3.1

- Richten Sie die Schlüsselarchivierung ein
- Stellen Sie alle Schritte anhand der Beschreibungen und Abbildungen im Buch nach
- Setzen Sie alle virtuellen Maschinen auf den Prüfpunkt „Basis“ zurück

Lösung 24.3.1

Erstellen der Gruppe „Schluesselarchivierungsgruppe“

- Wechseln Sie zur virtuellen Maschine „DC“
- Wählen Sie
    - Tools
    - Active Directory-Benutzer und –Computer
- Wählen Sie auf der linken Seite
    - Meistertrainer.info
    - Users
- Klicken Sie mit der rechten Maustaste und wählen Sie
    - Neu
    - Gruppe
    - Nennen Sie die Gruppe „Schluesselarchivierungsgruppe“
    - Lassen Sie „Globale Gruppe“
    - OK
- Klicken Sie doppelt auf die eben erstellte Gruppe und wechseln Sie zur Registerkarte „Mitglieder“
- Fügen Sie hinzu
    - Domänen-Admins
    - OK

Berechtigungsvergabe für die Zertifikatvorlage „Schlüsselwiederherstellungsagent“

- Wechseln Sie zur virtuellen Maschine „Server2“
- Falls Sie die zuvor erstellte MMC noch geöffnet haben, wechseln Sie auf diese
- Sonst erstellen Sie die MMC neu:
- Tippen Sie unten in der Taskleiste neben der Lupe ein: „MMC“
- Klicken Sie auf „MMC“
- Wählen Sie in der Konsole
    - Datei
    - Snap-In hinzufügen/entfernen
    - Zertifikatvorlage
    - Hinzufügen
    - OK
- Klicken Sie auf der linken Seite des Fensters auf „Zertifikatvorlagen“
- Wählen Sie auf der rechten Seite die Vorlage „Key Recovery Agent“ aus und klicken Sie mit der rechten Maustaste
    - Eigenschaften
- Registerkarte „Sicherheit“
    - Hinzufügen: Gruppe Schluesselarchivierungsgruppe
- Ändern der Berechtigungen für diese Gruppe
    - Lesen
    - Registrieren
    - OK

Veröffentlichen der Zertifikatvorlage

- Wählen Sie im Server-Manager von Server2
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
    - Zertifikatvorlagen
    - Klicken Sie mit der rechten Maustaste
        - Neu
        - Auszustellende Zertifikatvorlage
        - Key Recovery Agent
        - OK

Zertifikatanforderung

- Wechseln Sie zur virtuellen Maschine „W11“
- Melden Sie sich als „Meistertrainer/Administrator“ an der Maschine an
- Klicken Sie auf „Start“
- Geben Sie oben bei „Suchbegriff hier eingeben“ ein
    - MMC
- Wählen Sie „MMC Befehl ausführen“
- Klicken Sie in der Konsole auf
    - Datei
    - Snap-In hinzufügen/entfernen
- Scrollen Sie auf der linken Seite bei „Verfügbare Snap-Ins“ ganz nach unten und wählen Sie
    - Zertifikate
    - Hinzufügen
    - Eigenes Benutzerkonto
    - Fertigstellen
    - OK
- Erweitern Sie
    - Zertifikate – Aktueller Benutzer
    - Eigene Zertifikate
- Klicken Sie mit der rechten Maustaste
    - Alle Aufgaben
    - Ein neues Zertifikat anfordern
- Zertifikatregistrierungsassistent
    - Vorbereitung: Weiter
    - Zertifikatregistrierungsrichtlinie auswählen: Weiter
    - Zertifikate anfordern
    - Key Recovery Agent
    - Registrieren
    - Fertig stellen
- Lassen Sie die MMC offen

Genehmigung der Anforderung

- Wechseln Sie zur virtuellen Maschine „Server2“
- Wählen Sie im Server-Manager
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA

    - Ausstehende Anforderungen
- Wählen Sie die Anfrage im rechten Bereich des Fensters aus
- Klicken Sie mit der rechten Maustaste und wählen Sie
    - Alle Aufgaben
    - Ausstellen

Zertifikat exportieren, importieren und registrieren

- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
    - Ausgestellte Zertifikate
    - Wählen Sie das ausgestellte Zertifikat aus und doppelklicken Sie
    - Registerkarte „Details“
    - In Datei kopieren
- Wählen Sie im Zertifikatexport-Assistenten
    - Willkommen: Weiter
    - Format der zu exportierenden Datei: DER-codiert-binär X.509 (.cer)
    - Weiter
    - Erstellen Sie einen Ordner mit Namen „Cert“ und speichern Sie das Zertifikat dort unter dem Namen „Schluesselwiederherstellung“
- Kopieren Sie die Datei von „Server2“ auf „W11“ in den vorhandenen Ordner „Cert“

Importieren des Zertifikats

- Wechseln Sie zur virtuellen Maschine „W11“
- Kehren Sie zur zuvor geöffneten MMC zurück
- Erweitern Sie
    - Zertifikate – Aktueller Benutzer
    - Eigene Zertifikate
- Klicken Sie mit der rechten Maustaste
    - Alle Aufgaben
    - Importieren
- Zertifikatimport-Assistent
    - Willkommen: Weiter
    - Zu importierende Datei
        - Durchsuchen
        - Auswahl Ordner Cert\Schluesselwiederherstellung.cer
        - Weiter
        - Zertifikatspeicher: Weiter
        - Fertigstellen des Assistenten: Fertigstellen

Konfigurieren der Zertifizierungsstelle für den Schlüsselwiederherstellungsagenten

- Wechseln Sie zur virtuellen Maschine „Server2“
- Wählen Sie im Server-Manager
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
- Registerkarte „Wiederherstellungs-Agents“
    - Wählen Sie „Schlüssel archivieren“
    - Fügen Sie im unteren Bereich das Zertifikat des Administrators hinzu
    - OK
- Bestätigen Sie den Neustart des Dienstes

Erstellen einer neuen Vorlage für zukünftige Zertifikate

- Klicken Sie in der MMC mit der rechten Maustaste auf die Vorlage „Benutzer“
- Wählen Sie
    - Vorlage duplizieren
    - Registerkarte „Allgemein:
    - Vorlagenanzeigenname „Benutzer mit archiviertem Schlüssel“
    - Registerkarte „Anforderungsverarbeitung“
    - Haken setzen bei „Privaten Schlüssel für die Verschlüsselung archivieren“
    - OK
    - Bestätigen Sie die Warnmeldung
- Wählen Sie im Server-Manager
    - Tools
    - Zertifizierungsstelle
- Klicken Sie auf der linken Seite mit der rechten Maustaste auf
    - Meistertrainer-Server2-CA
    - Zertifikatvorlagen
    - Klicken Sie mit der rechten Maustaste
        - Neu
        - Auszustellende Zertifikatvorlage
        - Benutzer mit archiviertem Schlüssel
        - OK

Zurücksetzen der virtuellen Maschinen

- Wechseln Sie auf Ihre Hostmaschine

- Öffnen Sie den Hyper-V-Manager
- Klicken Sie im mittleren Fenster mit der rechten Maustaste auf die virtuelle Maschine „DC“
- Wechseln Sie auf das Fenster „Prüfpunkte“
- Wählen Sie den Prüfpunkt „Basis“ aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Anwenden“
- In der Abfrage wählen Sie „Anwenden“
- Warten Sie, bis der Prüfpunkt angewendet ist, dann können Sie die virtuelle Maschine neu starten
- Verfahren Sie für alle anderen virtuellen Maschinen genauso