Installationsanleitung für digitale Zertifikate

1) die von der BREKOM per Email erhaltene p12-Datei zwischenspeichern

- 2) wählen Sie diese Datei und starten Sie per Doppelklick die Installation des Zertifikats
- 3) es wird ein MS Zertifikatsimport-Assintent gestartet, hier Klicken Sie bitten auf weiter

4) bei dem Punkt Importdateiname, geben Sie den Speicherort und Dateinamen an und gehen Sie auf weiter

5) beim Kennwort geben Sie bitte den PIN, den Sie von der BREKOM bekommen haben,

wichtig ist hier das Kästchen "Schlüssel als exportierbar markieren" auszuwählen:

| Zertifikatsimport-Assistent | \mathbf{X} |
|---|--------------|
| Kennwort Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten. | |
| Geben Sie das Kennwort für den privaten Schlüssel ein. Kennwort: | |
| | |
| Hohe Sicherheit f ür den privaten Schl üssel aktivieren. Immer wenn der private Schl üssel von einer Anwendung verwendet wird, werden Sie zur Eingabe aufgefordert, wenn Sie diese Option aktivieren. | |
| Schüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen. | |
| | _ |
| < Zurück Weiter > Abbrecher | 2 |

Um (wenn es gewünscht ist) die PIN später zu ändern. (wenn man will).

Das andere Kästchen "Hohe Sicherheit …" kann ausgewählt werden (diese Entscheidung muß jeder selber treffen)

6) beim Zertifikatsspeicher bitte Zertifikatsspeicher automatisch wählen nehmen und dann auf weiter gehen.

| Zertifikatsimport-Assistent |
|--|
| Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert |
| Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben. |
| Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend) |
| O Alle Zertifikate in folgendem Speicher speichern |
| Zertifikatspeicher: |
| Durchsuchen |
| |
| |
| |
| |
| |
| < <u>Z</u> urück <u>W</u> eiter > Abbrechen |

7) Zum Schluß wählen Sie bei Fertigstellen des Assistenten den Punkt Fertig stellen aus.

8) Im neuen Fenster Ein neuer privater Austauschschlüssel wird importiert bitte mit OK bestätigen.

| Eine Anwendung erstellt ein geschütztes Objekt. |
|--|
| Privater Schlüssel des Cry |
| Sie haben die mittlere Sicherheitsstufe gewählt Sicherheitsstufe OK Abbrechen Details |

9) mit OK bestätigen Sie auch noch den erfolgreichen Importvorgang.

Ihr Zertifikat wurde somit erfolgreich auf Ihrem Rechner installiert.

| Zertifikat | X |
|---|-------------|
| Allgemein Details Zertifizierungspfad | |
| Zertifizierungspfad | |
| Zertifika | at anzeigen |
| Zertifizierungsstatus: Dieses Zertifikat ist entweder abgelaufen oder noch nicht t | gültig. |
| Weitere Informationen über <u>Zertifizierungspfade</u> | |
| | ОК |
| | - |

Beim Zertifikat kann man die Zertifikatskette/Zertifikatspfad sich ansehen.

Hier ist das Zertifikat selber (Mustermann Erich), das Zertifikat SubCA, das das Zertifikat ausgestellt hat (SubCA-User-01) und das Zertifikat RootCA (RootCA-01), das das SubCA-Zertifikat ausgestellt hat.

Um ein User- oder Maschinen-Zertifikat zu verifizieren, muß man die ganze Zertifikatskette verifizieren.

Also man installiert das User- oder Maschinen-Zertifikat mit dem Installations-Assistenten (also per Doppelklick s.o).

Jetzt muß man ein paar Punkte beachten, (was mühselig ist, und leider nach dem ein paar Trustcenter kompromittiert wurden)unumgänglich ist zu machen:

- 1) Das Zertifikat installieren
- 2) Dann auf start gehen im Suchfeld "mmc" aufrufen
- 3) Dann auf Datei/Snap-In hinzufügen/Zertifikate/Computer

| 🔚 Konsole1 - [Konsolenstamm] | | | |
|---|----------------------------------|------------------|-------|
| Tatei Aktion Ansicht Favoriten Fenster | ? | | _ 8 × |
| (= -) 🖬 🔒 🛛 🖬 | | | |
| Consolenstamm | Name | Aktionen | |
| Zertifikate (Lokaler Computer) | 🐺 Zertifikate (Lokaler Computer) | Konsolenstamm | |
| Zertifikate | | Weitere Aktionen | • |
| a 🚆 Vertrauenswürdige Stammzertifizierungsste | | | |
| Zertifikate | | | |
| Organisationsvertrauen | | | |
| Zwischenzerünzierungsstellen | | | |
| 📔 Zertifikate | | | |
| Vertrauenswürdige Herausgeber | | | |
| Nicht vertrauenswürdige Zertifikate Drittanhieter-Stammzertifizierungsstellen | | | |
| Vertrauenswürdige Personen | | | |
| Andere Personen | | | |
| Remote Desktop | | | |
| Smartcard vertrauenswürdige Stämme | | | |
| Vertrauenswürdige Geräte | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| 1 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| 4 III | | | |
| | | | |

- 4) Unter "eigene Zertifikate" sollte man das User- oder Maschinen-Zertifikat finden
- 5) Unter "Vertrauenswürdige Stammzertifizierungsstellen" muß das Root-Zertifikat (RootCA-01) zu finden sein
- 6) Unter "Zwischenzertifizierungsstellen" das SubCA-Zertifikat (SubCA-User-01) zu finden sein

Sollten die Zertifikate der RootCA und SubCA nicht dort sein, dann muß man diese Zertifikate manuell installieren, und dabei den Speicherort beachten. Oder diese aus der "eigene Zertifikate" dahin verschieben.

| Zertifikat | | | |
|--|--|------|--|
| Allgemein Details Zertifizierungspfad | Zertifikatimport-Assistent | | |
| Zertifikatsinformationen | Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden. | | |
| Dieses Zertifikat ist entweder abgelaufen nicht gültig. | Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben. | | |
| | Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend) | | |
| | Alle Zertifikate in folgendem Speicher speichern Zortifikateneichert | | |
| · · · · · · · · · · · · · · · · · · · | Durchsuchen. | | |
| Ausgestellt für: Mustermann Erich | | | |
| Ausgestellt von: SubCA-User-01 | | | |
| Gültig ab 07. 02. 2013 bis 07. 02. 2 | | | |
| | Weitere Informationen über Zertifikatspeicher | | |
| Zertifikat installieren | | | |
| Weitere Informationen über Zertifikate | < Zurück Weiter > Abbre | chen | |
| | ОК | 1000 | |