Hilfe: Installation eines Zertifikates / Homepage

Notwendigkeit eines Zertifikates

Die asymmetrische Verschlüsselung beruht auf der Verwendung von X.509 Zertifikaten mit einem öffentlichen (Public Key) und eine privaten Schlüssel (Private Key). Ohne dieses Zertifikat funktioniert auch der **abylon protection manager (apm)** nicht.

Erstellung eines Zertifikates

ACHTUNG: Bei den durch **abylon protection manager (apm)** erstellten Zertifikaten handelt es sich um selbstsignierte Zertifikate. Diese sind damit nicht authentisch, das heißt sie sind nicht durch eine öffentliche Zertifizierungsstelle bestätigt und können nur im privaten Umfeld eingesetzt werden. Für ein authentisches Zertifikat wenden Sie sich bitte an ein öffentliche Zertifizierungsstelle, wie z. B. <u>TC Trustcenter</u> oder <u>D-Trust</u>.

1. Ein selbstsigniertes Zertifikat können Sie mit wenigen Klicks über das Modul <u>apm - Selbstsignierte</u> Zertifikate erstellen. Klicken Sie einfach auf das folgende Icon.



2. Danach müssen Sie noch bestätigen, dass Sie die erstellten selbstsignierten Zertifikate nicht missbrauchen und nur privat nutzen.

apm - Warnung!
Ich bin mir darüber im Klaren, dass das in Folge erstellte selbstsignlerte Zertifikat nur zur privaten Verwendung benutzt werden darf und jeder Missbrauch verboten ist! Ich oder Dritte werden für etwaige Schäden die entstehen abylonsoft oder andere Lizenznehmer NICHT haftbar machen. Akzeptleren?
🔽 Dialog nächstes mal anzeigen!
Nein

3. Im Dialog **apm - Selbstsignierte Zertifikate erstellen** geben Sie nun Ihren Namen, Ihre Email-Adresse, die Schlüssellänge und die Laufzeit ein.

00100011	1 Zertifikatsinhaber:	Frank Muster	
abylons	2 Emailadresse:	fm@musterfirma.de	7
sig finto	3 Seriennummer:	66575638 RSA Schlüsselstärke: 1024 4 💌	<u>E</u> rstellen
10001	5 Laufzeit (Tagen):	730 Alias: fm 6	

4. Das Zertifikat können Sie vor einer unberechtigten Installation durch ein Passwort schützen. Dieses Passwort hat nichts mit dem Kennwort zu tun, welches Sie später für Ihre Datenverschlüsselung und Signatur verwenden. Dieses wird am Ende der Zertifikatsinstallation festgelegt.



5. Das erstellte Zertifikat wird in Form einer PFX-Datei gespeichert. Sichern Sie diese Datei vor unberechtigten Zugriffen und legen Sie sich **unbedingt** eine Sicherheitskopie auf Diskette an. ACHTUNG: Bei einer Neuinstallation Ihres Rechners, einem harten Systemcrash oder einem versehentlichen Löschen des Zertifikats ist eine Entschlüsselung Ihrer Daten nur mit diesem Originalzertifikat möglich. Das erneute Erstellen eines gleichnamigen Zertifikates hilft Ihnen in diesem Fall nicht weiter, weil der entsprechende Schlüssel durch interne Zufallsgeneratoren immer wieder neu generiert wird und sich niemals wiederholt.

apm - selbs	stsignierte Zertifikate erste	ellen	? 🔀
Speichern	DEMP		
Stest_xp.p tom-xp.pl	fx 'x		

6. Nun können Sie das erstellte Zertifikat direkt in Ihre Zertifikatsdatenbank importieren. Dazu sehen Sie sich die Anleitung zur <u>Installation eines Zertifikates</u> an.



Installation eines Zertifikates

1. Zur Installation eines Zertifikates müssen Sie nur ein doppelt auf eine Zertifikatsdatei klicken. Diese haben die Dateiendung PFX oder P12.

🚳 test_xp.pfx 🚳 tom-xp.pfx

Wenn Sie sich vorher mit **apm** ein selbstsigniertes Zertifikat erstellt haben, den letzten Dialog mit '*Ja*' bestätigt haben, dann startet die Installationsroutine automatisch.

2. Auf der 2. Seite des Installationsassistenten wird noch einmal das zu installierende Zertifikat angezeigt.

3. Auf der 3. Seite müssen Sie das Passwort eingeben, mit dem das Zertifikat geschützt ist. Sinnvoll ist es auch, die beiden Punkte '*Hohe Sicherheit*' und '*Exportierbarkeit*' zu aktivieren. Dadurch können Sie am Ende der Installation den Zugriff auf Ihr Zertifikat mit einem Passwort schützen und später auch wieder mit privaten Schlüssel exportieren.

Kennwort	
Der private Schlüs gewährleisten.	sel wurde mit einem Kennwort geschützt, um die Sicherheit zu
Geben Sie das Ker	nwart für den privaten Schlüssel ein.
Kennwort:	
->	
-> 🖓 Hohe Sicher	heit für den privaten Schlüssel aktivieren. Immer wenn der private
Hohe Sicher Schlüssel vo aufgeforder	heit für den privaten Schlüssel aktivieren. Immer wenn der private n einer Anwendung verwendet wird, werden Sie zur Eingabe t, wenn Sie diese Option aktivieren.
Hohe Sicher Schlüssel vo aufgeforder	heit für den privaten Schlüssel aktivieren. Immer wenn der private n einer Anwendung verwendet wird, werden Sie zur Eingabe t, wenn Sie diese Option aktivieren. sexportierbar markieren. Dadurch können Sie Ihre Schlüssel zu ren Zeitpunkt sichern bzw. überführen.
Hohe Sicher Schlüssel vo aufgeforder Schlüssel al: einem späte	heit für den privaten Schlüssel aktivieren. Immer wenn der private n einer Anwendung verwendet wird, werden Sie zur Eingabe t, wenn Sie diese Option aktivieren. s exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu ren Zeitpunkt sichern bzw. überführen.

4. Auf der 4. Seite müssen Sie die Zertifikatsdatenbank auswählen, in dem das Zertifikat gespeichert werden soll. Dazu wird der Punkt '*Alle Zertifikate in folgendem Speicher speichern'* ausgewählt. Über das Button '*Durchsuchen...'* öffnet sich der Dialog zum Auswählen des Zertifikatsspeichers. Hier ist der erste Punkt '*Eigene Zertifikate'* zu wählen. Nach dem Bestätigen mit dem Button '*OK'* schließt sich der Dialog wieder und in dem Feld Zertifikatsspeicher steht nun die Zertifikatsdatenbank '*Eigene Zertifikate'*.

Zertifikatsimport-Assistent	
Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert	
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einer Pfad für die Zertifikate angeben. Ozertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)	n
O Alle Zertifikate in folgendem Speicher speichern Zertifikatspeicher: Durchsucher	
Vertifikatspeicher auswählen	
	echen)
Physikalischen Speicher anzeigen	In

5. Auf der letzten Seite werden noch einmal alle relevanten Daten angezeigt. Den Installationsassistenten schließen Sie mit dem Button '*Fertig stellen*'.

6. Zum Schluss muss noch die Sicherheitsstufe festgelegt werden. Klicken Sie dazu auf das Button '*Sicherheitsstufe.*'.

tin neder pri	Eine Anwendung erstellt ein geschütztes Objekt.	
	Privater Schliterel der Cru	
	Sie haben die mittlere Sicherheitsstufe gewählt OK Abbrechen Details	

7. Hier sollten Sie die Stufe '*Hoch*' wählen, damit Sie bei jeder Signier- oder Entschlüsselungsaktion nach dem Passwort gefragt werden.

Ein neuer privater Au	stauschschlüssel wird importiert. 🛛 🛛 🔀
	 Wählen Sie eine passende Sicherheitsstufe für dieses Objekt. Hoch Bevor Objekt verwendet werden kann, muss meine Zustimmung mit einem Kennwort eingeholt werden. Mittel Bevor Objekt verwendet werden kann, muss meine Zustimmung eingeholt werden.
	<zuruck weiter=""> Abbrechen</zuruck>

8. Danach müssen Sie noch ein Passwort eingeben und das Button '*Fertig stellen"* klicken.

in neuer privater Au	istauschschlüssel Erstellen Sie ein Ker schützen.	wird importiert. nnwort, um dieses Objekt zu
	Neues Kennwort für Kennwort für:	r dieses Objekt erstellen Privater Schlüssel des Cr
	Kennwort 🛁 Bestätigen 🛁	•••••
	< Zurüc	K Fertig stellen Abbrechen

9. Nun müssen Sie nur noch den Dialog (siehe Punkt 5) mit 'OK' bestätigen. Damit ist die Installation des Zertifikates abgeschlossen und Sie finden Ihr Zertifikat im <u>apm - Zertifikatsmanager</u> in der Datenbank 'My

(Private Zertifikate)'. Über das Button 'Aktivieren' können Sie dieses Zertifikat als Ihr 'Eigenes Zertifikat' (gelb hinterlegter Schlüssel) festlegen. In Zukunft werden alle Signier- und Verschlüsselungsoperationen mit Hilfe dieses Zertifikates durchgeführt. 🚯 apm - Zertifikatsmanager (nicht registriert) - uwe Add LDAP an Importieren **E**rstellen <u> Löschen</u> 🐔 Info <u> S</u>enden Aktivieren × Zertiříkatsinhaber: Zeit Sp 🔦 Aktueller User: uwe e 🛷 DE, "Thomas Mustermann, thomas mustermann@abyl0f1_guilig 白 🛞 Eigene Zertifikate (PKC: 0 -> My (Private Zertifika 1 O 🔶 Root (Vertrauenswi.

(c) 2001-2003 abylonsoft - created 17.09.2002 - Last Update / Stand 25.09.2003

abylonsoft - Dr. Thomas Klabunde GbR Amselweg 18 D-55442 Stromberg

Web: <u>http://www.abylonsoft.de</u> Kontakt: <u>mail@abylonsoft.de</u>