Technik: Austausch des öffentlichen Schlüssels / Homepage

Austausch des öffentlichen Schlüssels (Public Key)

Die Basis der Verschlüsselung von Daten für Dritte ist der öffentliche Schlüssel (Public Key) dieser Person. Wenn Sie Daten für 'HANS' verschlüsseln wollen, dann müssen Sie erst einmal in den Besitz seines öffentlichen Schlüssels von 'HANS' kommen. Der **abylon protection manager (apm)** bietet dazu eine Reihe von Möglichkeiten an. Diese sollen Ihnen hier vorgestellt werden.

A. Verifizieren einer signierten Datei oder auspacken eine SME-Datei

B. Verwendung des Moduls apm - Public Key Austausch

C. Zugriff auf einen LDAP-Servers

Verifizieren einer signierten Datei oder auspacken einer SME-Datei

Dies ist eine relativ einfache Methode an den öffentlichen Schlüssel einer Person zu gelangen. Lassen Sie sich einfach eine signierte (SGN) oder SME-Datei zuschicken.

1. Klicken Sie doppelt auf die signierte Datei oder SME-Datei.

2. Sollte der entsprechende öffentliche Schlüssel (Public Key) des Absenders noch nicht in Ihrer Zertifikatsdatenbank enthalten sein, so trägt der **abylon protection manager (apm)** diesen automatisch ein.

INFO: Bei SME-Dateien müssen Sie evtl. vorher Ihr Passwort eingeben.

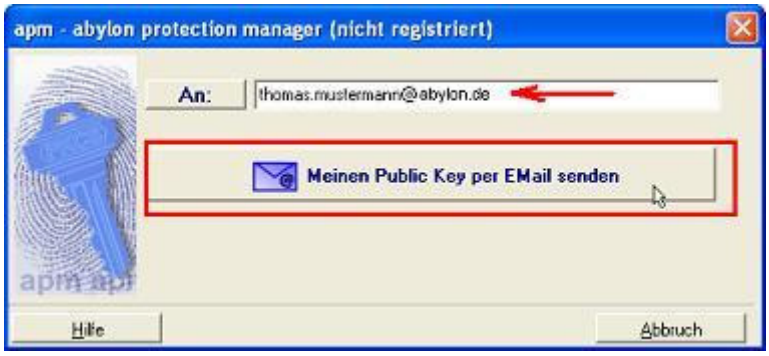
3. Die Zertifikatsinformationen werden in dem folgenden Dialog angezeigt. Hier müssen Sie mit '*OK*' bestätigen. Nun sind Sie im Besitz des entsprechenden öffentlichen Schlüssels. Dieser wird im **apm - Zertifikatsmanager** in der Zertifikatsdatenbank '*My (Private Zertifikate)'* angezeigt und kann in Zukunft zum Bilden von SME's verwendet werden.

Verwendung des Moduls apm - Public Key Austausch

Der **abylon protection manager (apm)** bietet eine komfortabeler Methode zum Versenden Ihres öffentlichen Schlüssels (Public Key) an.

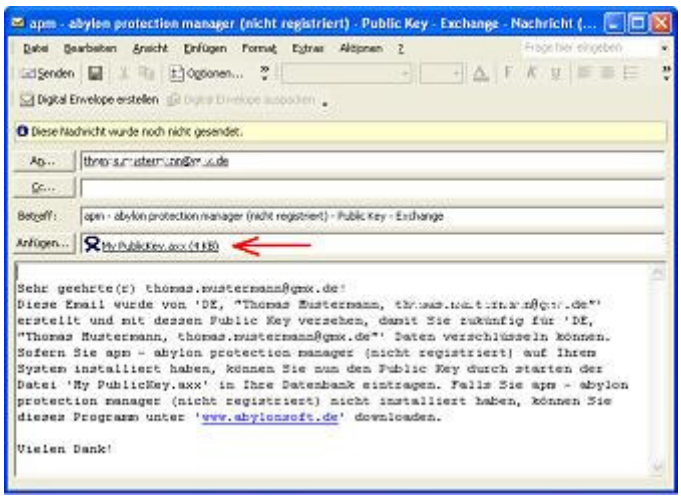
1. Öffnen Sie den **apm - Manager** und Klicken auf folgendes Symbol.

2. Im den Dialog müssen Sie nur noch die Email-Adresse des Empfängers eintragen und auf das Button '*Meinen Public Key per Email senden*' klicken.



3. Wenn Sie ein Zertifikat mit hoher Sicherheit eingestellt haben, dann müssen Sie jetzt Ihr Passwort eingeben.

4. In Ihrem Standardbrowser wird nun eine Email mit der Datei '*My PublicKey.axx*' als Anlage erzeugt. Diese müssen Sie nun nur noch versenden.

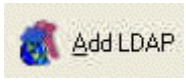


5. Wenn der Empfänger die Anlage ausführt (doppelt klicken) und mindestens die kostenlose Version des **abylon protection managers (apm)** installiert hat, dann trägt das Programm Ihren öffentlichen Schlüssel in seine Zertifikatsdatenbank unter *'My (Private Zertifikate)'* ein. In Zukunft kann der Empfänger Ihnen verschlüsselte Daten zuschicken, die nur Sie wieder Entschlüsseln können.

Zugriff auf einen LDAP-Servers

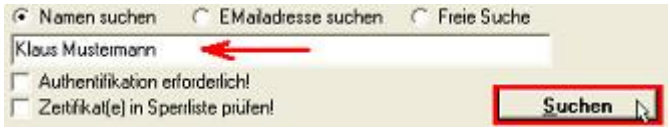
Firmen und Trustcenter bieten eine so genannte Public Key Infrastructure PKI an, über welche öffentlichen Schlüssel (Public Keys) online abgerufen werden können. Dadurch kann direkt für eine Person verschlüsselt werden, ohne vorher den öffentlichen Schlüssels auszutauschen. Der **abylon protection manager (apm)** bietet in der Pro-Version die Möglichkeit auf diese Server zuzugreifen und nach Zertifikaten zu suchen.

1. Beim Bilden eine SME öffnet sich der **apm - Zertifikatsmanager** zum Selektieren des öffentlichen Schlüssels (Public Keys). Nun können Sie den Dialog zum Durchsuchen eines LDAP-Servers öffnen.



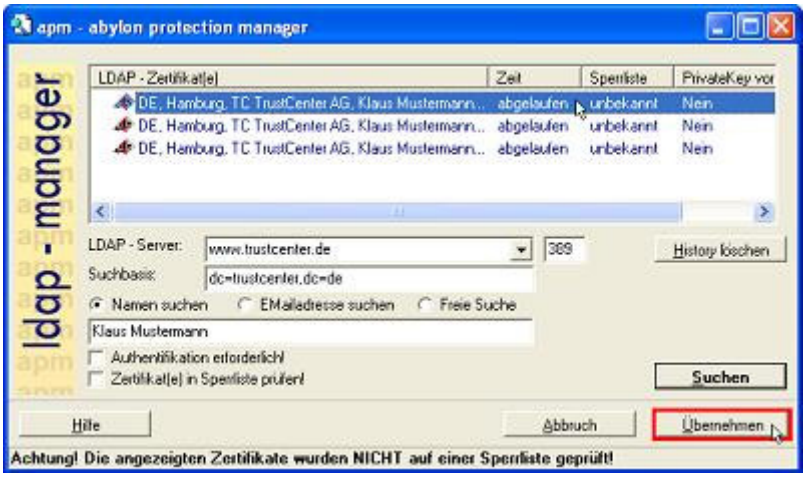
2. In diesem Dialog sind einige Angaben zum LDAP-Server und der Suchbasis einzugeben. Alternativ können Sie einen der vorgegebenen LDAP-Server (z. B. TC Trustcenter oder D-Trust) verwenden.

3. Geben Sie die den zu suchenden Namen oder die Email-Adresse an und drücken das Button '*Suchen*'.

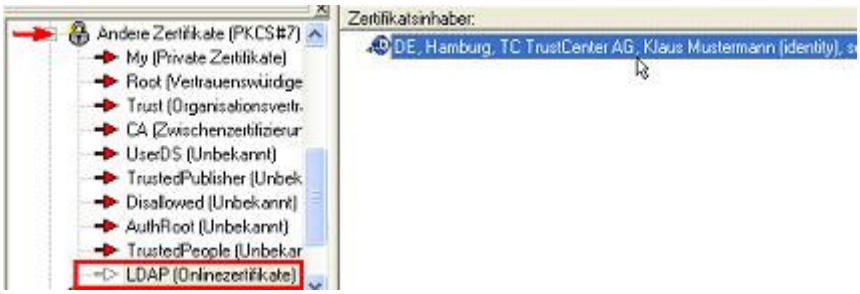


INFO: Es können Wildcards (Sternchen *) verwendet werden, jedoch bricht der LDAP-Server bei einem Überschreiten einer maximalen Anzahl an gefundenen Einträgen mit einer Fehlermeldung ab. In diesem Fall müssen Sie das Suchkriterium weiter eingrenzen.

4. Im oberen Feld werden alle Suchergebnisse angezeigt. Die selektierten Einträge werden durch das Button '*Übernehmen*' in den Zertifikatsmanager übertragen.



5. Die selektierten Einträge finden Sie nun in der Zertifikatsdatenbank '*LDAP (Onlinezertifikate)*'. Diesen können sie nun zum Verschlüsseln verwenden. Der öffentliche Schlüssel bleibt Ihnen für die nächsten Verschlüsselungen erhalten, sodass Sie nicht erneut auf dem LDAP-Server suchen müssen. Sie können auch jederzeit ein LDAP-Zertifikat Offline verfügbar machen, indem Sie dieses von der Datenbank '*LDAP*' in die Datenbank '*MY*' kopieren.



INFO: Mit öffentlichen Schlüsseln (PKCS#7-Zertifikaten) verschlüsselte Daten können nur von dem Besitzer des privaten Schlüssels (PKCS#12-Zertifikaten) wieder entschlüsselt werden.

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

Web: http://www.abylonsoft.de
Kontakt: mail@abylonsoft.de