Erledigt Schlüsselbund, Zertificate und SSH

Beitrag von „ryder“ vom 7. Mai 2014, 16:28

Hallo Gemeinde,

ich verstehe nicht die Technik rund um den Schlüsselbund. Ich habe mir eine USB-SmartCard besorgt und diese mit einem Zertifikat betankt.
Der Schlüsselbund dient ja "angeblich" dazu ein einheitliches Interface auf alle Zertificate und Credentials zu bieten.
Soweit funktioniert das auch, wenn ich die USB-SmartCard einstecke, erscheint das Zertifikat im Schlüsselbund. Ich kann dann dieses Zertifikat
nutzen, z.B. in Outlook2011.
Nun gut, aber wie bringe ich nun dem SSH-Client bei auf dieses Zertifikat zuzugreifen und es für eine Authentifizierung beim Verbindungsaufbau zu verwenden?

Wer weiß wie das funktioniert?

ciao
ryder

Beitrag von „ich777“ vom 8. Mai 2014, 16:41

Welchen SSH Client willst du benutzen bzw benutzt du?

Beitrag von „ryder“ vom 12. Mai 2014, 08:35

den openssh, der im OS dabei ist.

Beitrag von „Griven“ vom 13. Mai 2014, 23:03

Nur, damit ich das verstehe du möchtest Dich über den SSH Client über einen Schlüssel, der auf Deinem USB Stick enthalten ist auf einem entfetten Rechner anmelden, richtig? Ich gehe davon aus, dass Du Dir ein Schlüsselpaar erstellt hast bestehend aus einen privaten und einem öffentlichen Key, richtig? Falls nicht kannst Du das erreichen indem Du wie folgt vorgehst:

1. Terminal öffnen
2. ssh-keygen eingeben und mit Enter bestätigen
3. den Anweisungen auf dem Bildschirm folgen

Wenn das erledigt ist geht es weiter mit der Konfiguration des entfernten Rechners, hierzu wird zunächst der öffentliche Schlüssel auf den entfernten Rechner hochgeladen.

Code

```
1. scp /Pfad/Auf/Dem/Stick/.ssh/id_rsa.pub DEINUSERNAME@ihrserver.de:authorized_keys
```

Ist der Key einmal hochgeladen meldest Du Dich einmalig via ssh mit Passwort Authorisation am Server an

Code

```
1. ssh -l user deinserver
```

und gehst dann im Falle eine Linux Servers wie folgt weiter vor:

1. Im Homeverzeichnis des Users, der sich automatisch mit dem Key einloggen können soll erstellen wir ein Verzeichnis

Code

```
1. mkdir -p .ssh
```

2. Als nächstes verschieben wir auf dem Server die Datei authorized_keys in den eben

erstellten Ordner .ssh

Code

```
1. mv authorized_keys .ssh/authorized_keys
```

3. Jetzt noch die Berechtigungen richtig setzen

Code

```
1. chmod 600 .ssh/authorized_keys
```

und das war es schon. Haben wir alles richtig gemacht und der Stick ist gesteckt sollte ein

Code

```
1. ssh -l user deinserver
```

Dich direkt auf die shell bringen, ist der Stick nicht gesteckt erfolgt die Abfrage des Passworts.

&Voila, Ziel erreicht 

Beitrag von „ryder“ vom 14. Mai 2014, 08:49

griven,

nicht, ganz der Anfang von dir ist leider falsch geschildert. Ich habe einen privat/Public Key auf einem USB-Stick. Das ist aber kein herkömmlicher USB-Stick sondern eine SmarCard
(siehe z.B. hier http://www.safenet-inc.com/mul...uthentication/etoken-pro/)

Der Unterschied zu solch einem Token ist, dass er NICHT wie ein herkömmlicher USB-Stick angesprochen werden kann. Ich sehe den Schlüssel vom Stick im Schlüsselbund, kann mir dort das Zertifikat anzeigen.
Ich weiß aber nicht, wie ich dem SSH-Client sage, bitte benutze diesen Key aus dem Schlüsselbund.
Outlook 2011 kann das z.B., wenn ich hier Email-Verschlüsselung konfiguriere, dann zeigt er

mir alle Schlüssel vom Schlüsselbund an, auch den, der auf dem Stick ist.

So ich hoffe, nun ist es klarer.

ciao
ryder

Beitrag von „Dr. Ukeman“ vom 14. Mai 2014, 09:38

Naja du musst ja trotzdem ZUgriff auf deinen öffentlichen Schlüssel haben. Evtl bekommst du diesen auch auf der Homepage des Anbieters.
Denn der öffentliche Schlüssel muss ja definitiv auf den Zielrechner.

Beitrag von „ryder“ vom 14. Mai 2014, 12:14

Nicht der öffentliche Schlüssel ist das Problem, den kann man einfach vom Stick exportieren, der ist auch schon auf dem Server.
Ich muss jedoch dem ssh-client normalerweise sagen, welchen privaten Schlüssel er verwenden soll. Das kann ich tun, in dem ich den Schlüssel in die Standarddatei kopieren (kann ich aber nicht)
oder in dem ich mit ssh -i <schlüsseldatei> arbeite. Aber was muss ich machen wenn eben der Schlüssel im Schlüsselbund, wie "sage" ich das dem ssh-client?

ciao
ryder

Beitrag von „Griven“ vom 14. Mai 2014, 13:38

Schau Dir mal das Tool ssh keychain an, das sollte so ziemlich genau das umsetzen, was Duvor hast.