## Automatische Zertifikatssuche in Thunderbird einrichten

Verwenden des LDAP-Verzeichnisdienstes der DFN-PKI ©UHH-CA, Version2.0, 10.02.2011

Für den täglichen Gebrauch ist die manuelle Suche nach Zertifikaten ungeeignet. Vielmehr benötigt man einen Automatismus, der bei Eingabe der eMail-Adresse eines Empfängers automatisch von einem Verzeichnisdienst ein geeignetes Zertifikat für die Verschlüsselung auswählt und für zukünftige eMails an den selben Empfänger im eMail-Programm installiert.

Im Rahmen der DFN-PKI ist dies bereits vorgesehen. Das Häkchen "Veröffentlichen" auf dem Zertifikatsantrag sorgt dafür, dass das eigene Zertifikat im Verzeichnisdienst der DFN-PKI abgelegt wird und somit für andere automatisch über Ihre eMail-Adresse gefunden werden kann. Damit ist es anderen Personen möglich, Ihnen verschlüsselte eMails zu senden und ihnen ist es möglich, eMails an andere im Verzeichnis geführte Personen zu verschlüsseln.

Um den Verzeichnisdienst der DFN-PKI in Ihrem Thunderbird-eMail-Programm zu verwenden, gehen Sie bitte folgendermaßen vor:

- 1. Klicken Sie auf **Adressbuch** in der Symbolleiste. Es erscheint das Fenster mit den bisher eingerichteten Adressbüchern.
- 2. Wählen im Menü des Adressbuchfensters: **Datei->Neu->LDAP-Verzeichnis...** . Es erscheint das Fenster "LDAP-Verzeichnisserver bearbeiten".
- 3. Tragen Sie die folgenden Informationen in der Rubrik "Allgemein" ein:
  - a. Name: DFN-PKI
  - b. Serveradresse: Idap.pca.dfn.de
  - c. Basis-DN: ou=DFN-PKI,o=DFN-Verein,c=de
  - d. Port-Nummer: 389

LD	AP-Verzeichnissen	ver bearbeiten	×
	Allgemein Offlin	ne Erweitert	
	<u>N</u> ame:	DFN-PKI	
	Server <u>a</u> dresse:	ldap.pca.dfn.de	
	<u>B</u> asis-DN:	ou=DFN-PKI,o=DFN-Verein,c=de	<u>S</u> uchen
	<u>P</u> ort-Nummer:	389	
	B <u>i</u> nd-DN:		
	🔲 Verschlüssel	te Verbindung (SS <u>L</u> ) verwenden	
		ОК	Abbrechen

4. Speichern Sie das neue Adressbuch mit **OK** ab. Wählen Sie das neue Adressbuch mit einem Mausklick aus und geben Sie zum Testen im Suchfeld "uhh-ra" ein. Es sollten Informationen zum Zertifikat der UHH-RA wie im folgenden Bild angezeigt werden:

Adressbuch			_ <b>_ X</b>
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsio	:ht E <u>x</u> tras <u>H</u> ilfe		
🐣 Neuer Kontakt 🛛 🔩 P	Jeue Liste 🕕 Eigenschaften 📑	🛛 Verfassen 🛛 🗙 Löschen	uhh-ra ×
Adressbücher	Name 🔺 E-Mail-Adresse 🛛 🕅	Messenger-Name Organisa	tion 🛛 Tel. dienstlich 🛛 🖽
Persönlicdressbuch	🔒 GRP: UHH-RA@uni-ha		
🔮 DFN-PKI			
📗 Gesammelte Adressen			
Ein Treffer gefunden			1.

Damit steht das neu eingerichtete Adressbuch allen eMail-Konten zur Verfügung. Damit das neue Adressbuch bei der Eingabe von eMail-Adressen beim Schreiben von neuen eMails auch verwendet wird, müssen Sie es noch mit dem jeweiligen Konto verknüpfen. Gehen Sie dazu folgendermaßen vor:

 Wählen Sie im Hauptfenster von Thunderbird Ihr eMail-Konto aus und wählen Sie anschließend Konten-Einstellungen bearbeiten. Es erscheint das Fenster "Konten-Einstellungen". 2. Wählen Sie die Rubrik Verfassen & Adressieren aus. Im Bereich "Adressieren" wählen Sie nun Einen anderen LDAP-Verzeichnisserver verwenden: und anschließend im Auswahlfeld DFN-PKI.

nten-Einstellungen	<u>د</u>
A Server-Finstellungen	Verfassen & Adressieren
Kopien & Ordner	_ Verfassen
Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz Empfangsbestätigungen (MDN) S/MIME-Sicherheit #Lokale Ordner Junk-Filter Speicherplatz Postausgang-Server (SMTP)	<ul> <li>Nachrichten im HTML-Format verfassen</li> <li>Original-Nachricht beim Antworten automatisch zitieren</li> <li>Dabei meine Antwort unter dem Zitat beginnen </li> <li>und meine Signatur unter das Zitat platzieren. (empfohlen)</li> <li>Signatur beim Antworten beifügen</li> <li>Signatur beim Weiterleiten beifügen</li> </ul>
Konten-Aktionen •	
	OK Abbrechen

Anschließend wird beim Verfassen einer neuen eMail bereits beim Eintippen der Anfangsbuchstaben im Empfängerfeld im DFN-PKI-Verzeichnis nach passenden eMail-Adressen gesucht, zu denen es ein gültiges Zertifikat gibt. Sie erkennen dies daran, dass Sie bereits beim Tippen der eMail-Adresse Vorschläge von Thunderbird angezeigt bekommen. In der Folgenden Abbildung wurde im Empfänger-Feld lediglich der Präfix **mey** eingetippt und sofort erscheint eine Auswahlliste mit dazu passenden eMail-Adressen, zu denen es ein Zertifikat gibt.

🗠 Verfassen: Testnachrich mit LDAP-Verzeichnis	_ 🗆 X					
Datei Bearbeiten Ansicht Einfügen Format Einstellungen Extras Hilfe						
📰 Senden 🏻 🎐 Rechtschr 👂 Anhang - 🔒 S/MIME - 🔜 Speichern -						
Von:	•					
An: An: Meyer <meyerk@tu-cottbus.de></meyerk@tu-cottbus.de>						
Kirstin Meyer <meyerk@tu-cottbus.de></meyerk@tu-cottbus.de>						
"Dr. Henning Meyer" <henning.meyer@charite.de></henning.meyer@charite.de>						
Angelika Meyer <angelika.meyer@charite.de></angelika.meyer@charite.de>						
Betreff: Test						
Normaler Text ▼ Variable Breite ▼ ■ A' A' A A A I = 1 = 4 = 4 = - ■ - ◎ -						

Zum Verschlüsseln der Nachricht an den ausgewählten Empfänger drücken Sie die Schaltfläche **S/MIME**. Wählen Sie dann die Einstellung **Nachricht verschlüsseln** wie in der folgenden Abbildung dargestellt. Beim Versenden wird die Nachricht nun mit Hilfe des im Adressbuch gefundenen Zertifikats an den Empfänger verschlüsselt, so dass nur die Empfängerin die Nachricht wieder entschlüsseln kann.

🗠 Verfassen: Test	_ 🗆 🗙
Datei Bearbeiten Ansicht Einfügen Format Einstellungen Extras Hilfe	
📰 Senden aby Rechtschr 👂 Anhang - 🔒 S/MIME - 🔜 Speichern -	
Von: Vachricht verschlüsseln	-
✓ Nachricht <u>unterschreiben</u>	
Sicherheitsinformationen anzeigen	
Betreff: Test Normaler Text Variable Breite $\mathbf{v} = \mathbf{A}^{\mathbf{v}} \mathbf{A}^{\mathbf{A}} \mathbf{A} \mathbf{A}$ $\mathbf{A} = 1^{-} \mathbf{A}^{\mathbf{v}} \mathbf{A}^{\mathbf{v}} = \mathbf{A}^{\mathbf{v}} \mathbf{A}^{\mathbf$	
Sehr geehrte Damen und Herren,	

Wird wie im obigen Beispiel zusätzlich **Nachricht unterschreiben** ausgewählt, fügt Thunderbird eine digitale Signatur mit Hilfe Ihres Zertifikats an die eMail an. Damit ist es der Empfängerin dann auch möglich zu verifizieren,

- dass die eMail tatsächlich von Ihnen (und nicht von jemand anderem in Ihrem Namen) gesendet wurde und
- dass die eMail während der Übertragung nicht verfälscht (geändert, manipuliert) wurde.