SSL Installation auf Lotus Domino 8.5

Willkommen zum Domino 8.5 Hands On!

Im Folgenden gibt es einen step-by step guide zur Einrichtung von HTTPS am Domino Server mit einem selbsterstellten Zertifikat.

Danach werden die Schritte gezeigt, die nötig sind, um ein Client-Zertifikat in die Notes-ID zu bringen, die es ermöglicht, verschlüsselte / signierte smtp-mails auszutauschen.

Bernhard Kolb

www.ebe-edv.com

Bernhard.Kolb@ebe-edv.com

Lab 1: SSL via Server Certificate Admin

- 1) Certserv.nsf öffnen
- 2) Create self signed certificate
- 3) Passwort vergeben *lotusnotes*



- 4) Selfcert.kyr und .sth ins Domino Data verzeichnis kopieren
- 5) Im serverdokument unter internet-Protocols SSL Keyfile angeben selfcert.kyr
- 6) https YES
- 7) Serverdoc speichern
- 8) Tell http restart
- 9) Zugriff auf die Webseite via https

Lab 2: Zertifizierungsstelle einrichten

1) Certificate Authority einrichten

am server neue DB von der CCA50 Schablone erstellen

New Applic	ation	? ×
Specify	New Application Name and Location	
<u>S</u> erver	dino/ditech 👻	ОК
<u>T</u> itle	Admincamp CA	Cancel
<u>F</u> ile name	ACCA.nsf	1
	Encryption	
	<u>Create full text index for searching</u>	Ad <u>v</u> anced
Specify	Template for New Application	
Server	dino/ditech 🗨]
Temp <u>l</u> ate	Domino Administrator (8)	
	Domino Blog (8)	1
	Domino Certificate Publication Requ	, ,
	Domino Change Control (6)	
File <u>n</u> ame	cca50.ntf	<u>A</u> bout
	Show advanced templates	
	Inherit future design changes	1.

2) DB schließen und neu öffnen

...sonst sind nicht alle Rollen dem aktuellen User zugeordnet...

🛞 Admincamp CA - CASetup - N	wigator - IBM Lotus Notes	
<u>File Edit View Create Too</u> o	s <u>W</u> indow <u>H</u> elp	
🕒 춝 Home 🛛 🖄 Berr	nar × 🏦 EBE Bri × 🏦 EBE Rec × 💸 Adm ×	×
1 📰 🖌 🕾	🛛 💽 🗸 Search All Mail	2
Address	•	
A	[
ov/vvob.		
Certificate	Certificate Authority Setup	
Authority	1. Create Certificate Authority Key Ring & Certificate	
Certificate	Certificate Authority Profile	
Server	3. Create Server Key Ring & Certificate	-
» •		
	- 🥪 🖧 EBE	•

3) Create Server Certificate & Keyring

Hands On SSL für Domino 8.5



Das Certificate Authority-Keyring-File entspricht der cert.id in der Domino-Welt und wird für die spätere Ausstellung von Zertifikaten benötigt.

Achtung: diese Datei wird lokal auf der Notes-Client Maschine erzeugt!

4)	Configure	Certificate	Authority
----	-----------	-------------	-----------

😧 Ce File	ertificate Authority Prof Edit View Create Acti	î ile - IBM Lotus Notes ons Text Tools Window Help			
		a Admincamp 2010 - CASetup - Navig 🗴	🚯 Certificate Authority Profile 🛛 🗙		
1 28] 🕀 🐵 📃	💌 💌 b i 😐 🛛 🔛 🗴	🛚 🚺 👻 Search All Mail	Q
1 -	🖌 🔑 👀 🔤	> ⋒ √			
A	Use this form to co	onfigure settings needed by the Certificate Auth	ority application.		
	CA Cottings		Quick Hole		
	CA Settings CA Key File	『C:1Program Files (x86)\IBM\Lotus\Notes\Data\ACCAKey.kyr』	- The name of the CA key ring file is stored here automatically when you create it. If you move the CA key ring file, you must update the path here so the application can find it		
	Certificate Server DNS Name	^{I7} www.admincamp.local_	- The DNS for the server is needed for the automatic generation of the e-mail that is sent to users for certificate pickup.		
	Use SSL for certificate transactions?	Ves Yes	If this is selected, the automatically generated e-mail will contain a reference to the SSL port for secure certificate pick-up		
() () () () () () () () () () () () () (Certificate Server Port Number	^{[7} 80]	- The port number is also needed for the automatic generation of the e-mail that is sent to users for certificate pickup. This is the TCP/IP port on which the Certificate Server will be running		
	Mail confirmation of signed certificate to requestor?		Selecting this default option is for an e-mail confirmation of a signed certificate request		
	Submit signed certificates to AdminP for addition to the Directory?	T Yes	Selecting this default option is for the signed certificate request to be submitted to the Administration Process for storage of the certificate in		T
				a 🥪 🖓	AC2010 +

Achtung: üblicherweise wird Mailconfirmation auf YES gesetzt! Nur hier im Lab wird auf Mail Benachrichtigung verzichtet.

5) Create Server KeyRing

🛞 Ci	reat	e Key Ring - IBM Lo	tus Notes			
Eile	Edit	t ⊻iew <u>⊂</u> reate <u>A</u> cti	ions <u>T</u> ext T <u>o</u> ols <u>W</u> indow <u>H</u> elp			
Ð		🎙 Home 🛛 🐝 c:	a Admincamp 2010 - CASetup - Navig 🗙 😤 🤇	Create Key Ring ×		
1 %	P) 💼 🔄 🕈 🖡		💽 b i 😐 🛛 🗱 🗧	🛛 🔀 🔻 Search All Mail	٩)
1 👁	1		🔨 🕼 🗸			
			Create CA Server Key Ring			
		Use this form to cr carry out all the int signing it with the the server key ring	eate the server key ring for the CA server. When yo ternal steps of creating the server key ring, creating CA certificate, then installing the CA certificate and	u submit the form, Domino will the server certificate request, the signed server certificate into		
		Note : Once the se application to view	erver key ring has been created, you should use the v and manage the server key ring contents.	e Server Certificate Admin		
۱ ۵ ۰		Server Key Ring	Information			
		Key Ring File Name: Key Ring Password:	^e keyfile.kyr <u>a</u>	Specify the name and password for the server key ring file you are creating.		
*		Password Verify:	ra			Sidebar
2	L	Key Size				
⊕ ⊚ ☆		Key Size:	[@] 1024 ⊒ ▼	Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength.		
				Note: With International Editions of the Domino server, the 1024 bit key size can only be used if you qualify for and have purchased a Verisign Global Server ID		
		CA Certificate Label	[©] Admincamp 2010 _	This label identifies the CA Trusted Root certificate that is automatically installed in the server key ring you are creating.		T
				*	a 🕹 🖓	AC2010 +

6) Die beiden Dateien **Keyfile.kyr** und **Keyfile.sth** aus dem lokalen Notes Data Verzeichnis ins Data Verzeichnis am Domino Server kopieren 7) Im Serverdokument des Domino Directories unter Ports – Internet Ports SSL aktivieren

<mark>@</mark> 50	erver: Domino/kolb - IBM Lotus Notes	
File	Edit View Greate Actions Lext Tools Window Help	
L I	A Home × 😡 kolb's Directory - Server/Servers × 🖓 Server: Domino/kolb ×	
18	, 🕒 💼 🖆 - 🔚 🖴 🔕 🛛 👘 🕹 💈 🛛 🕹 Search All Mail	<u></u>
1 🤊	🖌 🔗 🐽 🔤 🥆 👘 🗸	
A	Save & Close Create Web Examine Notes Certificate(s)	
	Basics Security Ports Server Tasks Internet Protocols MTAs Miscellaneous Transactional L	
	Notes Network Ports Internet Ports Proxies	
	SSL settings	
	SSL key file name: [©] keyfile.kyr ₌	
ø	SSL protocol version (for use with all protocols except HTTP):	
•	Accept SSL site certificates: O Yes 💿 No	
<u>₽</u> 3 +	Accept expired SSL certificates:	
	SSL ciphers: RC4 encryption with 128-bit key and MD5 MAC Modify RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC DES encryption with 56-bit key and SHA-1 MAC DES encryption with 28-bit key and SHA-1 MAC	
	Enable SSL V2:	
	(SSL V3 is always enabled)	
⑧ ☆	Web Directory Mail DIIOP Remote Debug Manager Server Controller	
	Web (HTTP/HTTPS)	
	TCP/IP port number: [©] 80 _	
	TCP/IP port status: Enabled .	
	Enforce server access 『No 』 settings:	
	Authentication options:	
	Name & password: Ves J	
	Anonymous: Yes V	
	SSL port number: 443 g	
	Authentication options:	-
	Client certificate:	
	Name & password: [©] Yes I V	
	Anonymous:	
	Fritantha name of the COL law view the Dawine Web and recommendation of the Col	
	Enter the name of the SSL key ring the Domino Web server uses for encryption activities.	
	- 😽 🛹 🔏 A	02010 🔺

auf der Serverconsole mit **tell http restart** den http Task neu starten bzw mit load http starten falls er noch nicht läuft

Lab 3: Cerifier migrieren

1) Migrate certifier

Admin Client – configuration – Migrate Certifier

Migrate Ce	rtifier	×
.	Migrate certifier file to Certificate Authority Process:	OK
	Please select either a Lotus Notes certifier ID file or a certifier keyring file:	Cancel
	Select	
Migrating Domino /) the certifier to CA process provides several key benefits. For more info Administration Help.	rmation, see the

2) Select Keyring File -> ICL DB anlegen

Migrate CN=Admincamp 2010/0=BKH/ST=vienna/C=AT	? ×
Basics Certificates Misc.	
Migrate certifier with id/keyring: C:\Program Files (x86)\IBM\Lotus\Notes\Data\ACCA	Key.kyr
Select the server on which this certifier will run: Domino/kolb	-
Name of ICL database to be created: icl\Admincamp 2010.nsf	
How this certifier is protected	
Encrypt certifier ID with: O Locking ID	
Server ID	
Require password to activate	
Password: Re-enter Password:	
Administrator(s)	
CAA RA Name	<u>A</u> dd
🗹 🗹 Notes Admin/kolb	Delete
	Loioto
	List of administrators
ОК	Cancel

3) Certreq.nsf anlegen

File – Application new (certreq.ntf)

New Applica	ation	2 X
Specify I	New Application Name and Location	
<u>S</u> erver	Domino/kolb	ОК
<u>T</u> itle	Admincamp Certificate Requests	Cancel
<u>F</u> ile name	Admincamp\ACR.nsf	
	Encryption	
	Create full text index for searching	Ad <u>v</u> anced
Specify	Cemplate for New Application	
Se <u>r</u> ver	Local	
Template	Bookmarks (8.5)	
	🔁 Certificate Requests (8)	
	Cluster Analysis (6)	
	Core Elements	
	Database Analysis	
File <u>n</u> ame	certreq.ntf	<u>A</u> bout
	Show advanced templates	
	Inherit future design changes	11.

4) Konfiguration

Database Administration	:
Supported CA:	Server: 🖁 Domino/kolb 🛛 💌
	Certifier: [₽] CN=Admincamp 2010/O=BKH/ST=vi€
Supported Certificate Types:	O Client Certificates Only
	O Server Certificates Only
	Both Client and Server Certificates
Client Request Customiza	tion:
Validity Period:	[©] 2₂years
Key Usages:	[®] Digital Signature, Key Encipherment
no, cougo.	bigital bigitatale, itey Encipiterinenta E
Extended Key Usages:	[®] Client Authentication, EMail Protection, 1×1
Server Request Customiza	ation:
Server Request Customiza Validity Period:	ation: 『1』years
Server Request Customiza Validity Period:	ation: 『1』years
Server Request Customiza Validity Period:	ation: 『1』years
Server Request Customiza Validity Period: Key Usages:	ation: 『1』years 『Digital Signature, Key Encipherment』▼
Server Request Customiza Validity Period: Key Usages:	ation: 『1』years 『Digital Signature, Key Encipherment』▼
Server Request Customiza Validity Period: Key Usages:	ation: 『1』years 『Digital Signature, Key Encipherment』▼
Server Request Customiza Validity Period: Key Usages:	ation: 『1』years 『Digital Signature, Key Encipherment』▼
Server Request Customiza Validity Period: Key Usages: Extended Key Usages:	ation: 『1 _ years 『Digital Signature, Key Encipherment 』 • 『Server Authentication 』 •
Server Request Customiza Validity Period: Key Usages: Extended Key Usages:	ation: 『1 _ years 『Digital Signature, Key Encipherment 』▼ 『Server Authentication 』▼
Server Request Customiza Validity Period: Key Usages: Extended Key Usages:	ation: 『1years 『Digital Signature, Key Encipherment 』 • 『Server Authentication 』 •
Server Request Customiza Validity Period: Key Usages: Extended Key Usages: Request Processing:	ation: [®] 1 gyears [®] Digital Signature, Key Encipherment 1 [®] Server Authentication 1
Server Request Customize Validity Period: Key Usages: Extended Key Usages: Request Processing: Processing Method:	ation: [®] 1 gyears [®] Digital Signature, Key Enciphermentge [®] Server Authenticationge [®] Manualge
Server Request Customize Validity Period: Key Usages: Extended Key Usages: Request Processing: Processing Method:	ation: [®] 1 gyears [®] Digital Signature, Key Encipherment * [®] Server Authentication * [®] Manual *
Server Request Customize Validity Period: Key Usages: Extended Key Usages: Request Processing: Processing Method:	ation: [®] 1 gyears [®] Digital Signature, Key Encipherment [®] Server Authentication [®] Manual [®] Manual [®]
Server Request Customiza Validity Period: Key Usages: Extended Key Usages: Request Processing: Processing Method:	ation: [®] 1 gyears [®] Digital Signature, Key Encipherment R [®] Server Authentication R [®] Manual R
Server Request Customize Validity Period: Key Usages: Extended Key Usages: Request Processing: Processing Method: Mail Notification:	ation: [®] 1years [®] Digital Signature, Key Encipherment _ • [®] Server Authentication _ • [®] Manual _ •
Server Request Customiza Validity Period: Key Usages: Extended Key Usages: Request Processing: Processing Method: Mail Notification: Mail confirmation of handled request to requestor?	ation: 『1years 『Digital Signature, Key Encipherment 』 ▼ 『Server Authentication 』 ▼ 『Manual 』 ▼

Achtung: auch hier normalerweise Mail confirmation -> YES. Nur hier im Lab werden keine Mails versendet

5) CA Servertask starten

Auf der Sevrerconsole: load ca

6) Im Browser einen Request erstellen

Mit dem Firefox auf http:/127.0.0.1/Admincamp/ACR.nsf

🥹 Mozilla Firefox		
<u>File Edit View History Bookmar</u>	ks <u>T</u> ools <u>H</u> elp	
🔇 💽 C 🗙 🏠 🛛	http://www.admincamp.local/cei	rtreq.nsf 🔗 - Google 🔎 S -
🧕 Most Visited 🌮 Getting Started 🔒	🖌 Latest Headlines	
💼 http://www.admincamp.local/acca.r	nsf 🛛 🗙 👘 http://www.adminca	local/certreq.nsf 🗙 🛞 http://www.admical/certreq.nsf 🗙 🔄
.dom/wo	Request a Clie	ent Certificate for Netscape Navigator or Compatible
Certificate	Use this form to enter the inf	ormation required for your client certificate request.
Authority	Certificate Info: The following information will	be included in your client certificate.
	Your Full Name:	Thomas Bahn e.g. John Doe
<u>Request Server</u> <u>Certificate</u>	Organizational Unit(s):	
<u>Pick Up Server</u> <u>Certificate</u>		
Accept This Authority In Your	Organization:	assono
<u>Server</u>	City/Locality:	
	State/Province:	Schleswig-Holsteir No abbreviations
Accept This Authority In Your	Country:	DE 2 letter country code, e.g. us
DIOWSEI	E-Mail Address:	thomas.bahn@assono.de
Request Client Certificate		four e-mail address is required if you will be using this certificate
Pick Up Client Certificate	Contact Information:	
	Provide the following informat	tion in case the Certificate Authority needs to contact you.
	Return E-Mail:	thomas.bahn@assono.de
		Directions for picking up your certificate will be sent to this email
Done	1	

Damit ist der Request in der certreq.nsf

Dort selektieren und -> Submit to adminP

7) Im Administrationsprozeß freigeben

in der Admin4.nsf in der view Certificate Requests

🛞 A	dministration Requests - Certificate Request	ts - IBM Lotus Notes	
Eile	<u>E</u> dit <u>V</u> iew <u>C</u> reate <u>A</u> ctions T <u>o</u> ols <u>W</u> indow <u></u>	Help	
Ð	😚 Home 🔹 🄏 Administration Reques	sts - Certifica 🗙 🖼 Certificate Requests - Pending/Subm 🗙	
1 🔁	- 🕂 😣 🍫 🍫 🗢 🖬 🛱 🧭 1	🐻 🏠 🖴 🖪 🛛	
1 👁	🖌 🖧 🖛 🔤 🥆 🕼 🗸		
A	Administration Requests	U Help	
	Administrative Attention Required Pending Administrator Approval Individual Approval Required Pending by Age Pending by Server All Activity by Server All Activity by Server All Errors by Date All Errors by Server Administration Requests	CA State Modified Subject Name CN=Admincamp 2010/0=BKH/ST=vienna/C=AT New 09/2012:34 EMAIL=thomas.bahn@assono.de/CN=Thomas.Bahn/0=assono/ST=Sc Issued by Certification Authority 09/2011:32 EMAIL=Bernhard@kolb.cc/CN=Bernhard Kolb/0=EBE/ST=vienna/C=AT 09/2011:11 EMAIL=mm@test.local/CN=Max.Muster/0=BKH/L=vienna/ST=vienna/C	
	Using application on Domino/kolb	🔺 🧠 🔏 AC20'	10 🔺

Eintrag editieren

optional: Zuordnung zu einem Personendokument (oder Not Published auswählen)

8) Zertifikat zum download bereitstellen

In der certreq.nsf den Eintrag selektieren – Pull request

😡 Certificate Requests - Pending/Submitted Requests - IBM Lotus Notes								
Eile	Edit View Create Actions Tools Window H	elp.						
Ð	😚 Home 🛛 🗶 Administration Request	s - Certific	a ×	📑 Certificate Reque	ests - Pending/Subm ×			
1 2	👌 - 😓 🔕 🗞 🍫 🖶 📼 📓 🛱 🎯 🐻 🏠 🚔 🖪							
) 🦔 🖌 🔑 🚥 🛲 🛰 📦 🗸								
A	Certificate Requests	ᆚ Submi	t Selecter	d Requests 🛛 🚑 Pull Sel	ected Requests			
	2010/O=BKH/ST=vienna/C=AT	CA	State	Modified	Request Information			
1 1			N=Admi	incamp 2010/0=BK	H/ST=vienna/C=AT			
			🔻 Subi	mitted to Administra	ntion Process			
la l	🗉 Pending/Submitted Requests 🛛 🔺	~ 		20.09 12:34	Client Request from Thomas	<u>Bahn (thomas.bahn@assono.c</u>	ie) 🧮	
	🎟 Pendina/Submitted Email Reque			20.09 11:10	Client Request from Max Mus	ter (mm@test.local)		
~	Database: Certificate Requests	•					• 🔊	
	1 document selected				*		AC2010 🔺	

Der Request liegt nun in der View Issued Certificate Requests

Dort den Eintrag öffnen ind die Pickup ID kopieren

Lab 4: Client Zertifikat installieren

1) Im Firefox das Zertifikat abholen und akzeptieren

🍪 Mozilla Firefox	
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarl	ය <u>T</u> ools <u>H</u> elp
🔇 🔊 C 🗙 🏠	🐌 http://www.admincamp.local/certreq.nsf 🛛 🖓 🗸 Google 🔎 🗴 -
🔊 Most Visited 🌮 Getting Started 🔊	Latest Headlines
\bigcirc http://www.admilocal/acca.nsf \times	💮 http://www.admial/certreq.nsf 🗙 👘 http://www.a/certreq.nsf 🗙 🔄 🚽
Authority	Pick Up Client Certificate When your certificate has been signed by the Certificate Authority and is ready for pickup, you will usually receive an e-mail containing the URL where you can pick up the certificate. If you do not receive an e-mail, you can use this form to pick up your certificate by providing the Pickup ID in the field below. Contact your Certificate Authority to obtain the Pickup ID. Enter the Certificate Pickup ID below:
<u>Request Server</u> <u>Certificate</u> Pick Up Server	Pickup ID: Pick Up Client Certificate
Certificate	
Done	D 🗡 👻 🖬 😓 🍼 📈 🛠 💽 💞 🎵

Damit ist das Zertifikat dann im Firefox

instellungen	_					×
	_				-	47.4
		5		90		ĘŎź
Allgemein	Tabs	Inhalt	Anwendunge	n Datenschu	tz Sicherheit	Erweitert
Allgemein Ne	atzwerk Un	date Ver	schlüsselung			
Aligement	erswerk op	uate	semassenang			
Protokolle						
✓ SSL <u>3.0</u>) verwender)		TLS <u>1</u> .0 verw	/enden	
Zertifikate						
Wenn eine	e Website na	ch dem j	persönlichen Sic	herheitszertifika	at verlangt:	
Autom	natisch eins	<u>w</u> ählen	<u>J</u> edes Mal f	ragen		
				-		
Zertifikat	e anzeigen	Zertif	ikatsperrliste	Validierung	<u>K</u> ryptographie	-Module
				ОК	Abbrechen	Hilfe

2) Exportieren via: Extras – Einstellungen

Zertifikate anzeigen -> Sichern

🥹 Z	Zertifikat-Manager	elacape Browner			
I	hre Zertifikate Personen	Server Zertifizierungsstellen And	lere		
	Sie haben Zertifikate dies	er Organisationen, die Sie identifi	zieren:		
	Zertifikatsname	Kryptographie-Modul	Seriennummer	Läuft ab am	Ę
	⊿BKH				
	Bernhard Kolb	Software-Sicherheitsmodul	4C:73:99:FE	23.08.2012	
	Ansehen Sicher	n Alle sichern	tieren		
					UK
	Terror Concerns of				

damit wird das Zertifikat (public und Private Key) in eine Datei exportiert

3) Im Internet Explorer der Ausstellungsstelle vertrauen mit dem IE die ACCA.nsf öffnen und "Accept This Authority in your Browser"





ternetoptionen	-		-		? <mark>x</mark>			
Verbindunger	Programme			Erweitert				
Allgemein	Siche	erheit	Datenso	hutz	Inhalte			
Inhaltsratgeber Filter helfen Ihnen bei der Kontrolle der Internetinhalte, die auf diesem Computer angezeigt werden können. Reference								
Zertifikate								
Zertifik Identif	ate werd izierung v	len für vers verwendet.	schlüsselte Ve	rbindunge	en und zur			
SSL-Status	öschen	<u>Z</u> ert	tifikate	<u>H</u> era	ausgeber			
SSL-Status löschen Zertifikate Herausgeber AutoVervollständigen AutoVervollständigen speichert vorherige Eingaben auf Webseiten und schlägt Übereinstimmungen vor. Einstellungen Feeds und Web Slices Einstellungen Einstellungen Feeds und Web Slices Einstellungen Freeds und Web Slices bieten aktualisierte Inhalte von Websites, die in Internet Explorer und anderen Programmen gelesen werden können. Einstellungen								
		0	K Ab	brechen	Ü <u>b</u> ernehmen			

4) In den Internet Explorer importieren

Es müssen die Attribute gesetzt werden – das geht im IE...

Hands On SSL für Domino 8.5

Zertifikate	in second		— X—					
Beabsichtigter Zweck: <	:>		•					
Eigene Zertifikate Andere	Personen Zwischenzert	ifizierungsstellen	Vertrauenswürdige					
Ausgestellt für	Ausgestellt von	Ablaufda	Anzeigename					
Bernhard Kolb	EBE-EDV CA	04.06.2011	<keine></keine>					
Importieren Exportiere	n] <u>E</u> ntfernen		Erweitert					
Beabsichtigte Zwecke des Z	ertifikats							
Antoine								
			Anceigen					
Weitere Informationen über Zertifikate								

importieren...

wichtig: Schlüssel als exportierbar markieren!

Zertifikatimport-Assistent
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 für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert. Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen. Alle erweiterten Eigenschaften mit einbeziehen.
Weitere Informationen über <u>das Sichern privater Schlüssel</u>
< <u>Z</u> urück Weiter > Abbrechen

Dann das Zertifikat auswählen – erweitert

Erweiterte Optionen								
Zertifikatzweck Wählen Sie mindestens einen Zweck, der als "Erweiterter Zweck" aufgeführt werden soll.								
Zertifikatzwecke:								
Serverauthentifizierung Clientauthentifizierung Codesignatur Sichere E-Mail Zeitstempel Microsoft-Vertrauenslistensionatur								
Exportformat								
das Ziehen eines Zertifikats in einen Dateiordner.								
Exportformat: DER-codiertes binäres X.509 (*.CER) -								
Alle Zertifikate im Zertifizierungspfad einbeziehen								
OK Abbrechen								

Clientauthentifizierung auswählen und Sichere-email Dann wieder exportieren.

ertifikatexport-Assistent	×
Privaten Schlüssel exportieren Sie können den privaten Sch	ılüssel mit dem Zertifikat exportieren.
Private Schlüssel sind kennw ausgewählten Zertifikat exp Seiten ein Kennwort eingebe	ortgeschützt. Wenn Sie den privaten Schlüssel mit dem ortieren möchten, müssen Sie auf einer der folgenden
Möchten Sie mit dem Zertifik	at auch den privaten Schlüssel exportieren?
Ia, privaten Schlüss	el exportieren
🔘 <u>N</u> ein, privaten Schlü	ssel nicht exportieren
Weitere Informationen über das	Exportieren privater Schlüssel
	< Zurück Weiter > Abbrechen

Wichtig: privaten Schlüssel exportieren!

ertifikatexport-Assistent Format der zu exportierenden Datei Zertifikate können in verschiedenen Dateiformaten exportiert werden.					
Wählen Sie das gewünschte Format:					
DER-codiert-binär X.509 (.CER)					
<u>Base-64-codiert X.509 (.CER)</u>					
Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B) Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen					
Privater Informationsaustausch - PKCS #12 (.PFX) Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen					
 Privaten Schlüssel nach erfolgreichem Export löschen Alle erweiterten Eigenschaften exportieren 					
O Microsoft Serieller Zertifikatspeicher (.SST)					
Weitere Informationen über Zertifikatdateiformate					
< <u>Z</u> urück Weiter > Abb	rechen				

- 5) Optional: Nun kann der Key in den Notes Client importiert werden
 - File Security User Security

User S	ecurity							<u>?</u> ×		
		Certifi	Certificates in your ID file							
	Security Basics	Your	certifica	tes provide a secure	e way to identify you t	o Notes and other pro	grams. Your I	D may contain		
6 E	Your Identity	certifi	cates u	sed to secure Notes	communications as t	well as certificates use	d with the Inte	emet.		
	Your Names									
	Your Certificates	Your N	otes Ce	rtificates _	 May be used to lo secure mail with or 	May be used to login to Notes, to access Notes databases, and to excha				
	Your Smartcard									
🎊 +	Identity of Others	Туре	Issued	d To ≎	Issue	d By ≎		Get Certificates 🔻		
🥵 ±	What Others Do	R	Bemh	ard Kolb/ebe	/ebe					
🂝 ±	Notes Data	L R	Bemh	ard Kolb/ebe	/ebe	/ebe				
2	Mail							Other Actions		
		 ⊢Select	ted item	I						
		Issue	ed to	Bernhard Kolb/eb	e					
		Issue	ed by	/ebe						
	Activated 21.02.2010			Туре	Notes international e	ncryption				
Expires 22.02.2012			Key identifier 1ETPT T4D31 6R7EJ TU2U5 U6RZF U34F1							
<u>A</u> dvanced Details										
							ОК	Close		

Get CertificatesIm	ort Internet Certificate
--------------------	--------------------------

Imp	oort I	nterne	t Certificates					? ×
D	o you	u wani	t to accept th	e following ce	rtificates	; into y	our ID?	
Δ	lat a r		1:0t	_				
	Inten	net Cer						
L I	Type Issued To ♀ Issued By ♀ Image: Second			Issued By ♀				
	Admincamp Admincamp							
		1						
Sel	ected	d item:						
	lssue	d to	bernhard.Kolb	@ebe-edv.com			(Email)	bernhard.Kolb@ebe-edv.cc
	lssue	d by	Admincamp				(Email)	
	Activ	ated	23.08.2010	Туре	Internet	multi-pu	urpose	
	Expire	es	23.08.2012	Fingerprint	D95F C	F10 C9	40 5A52 23	96 994E 2808 78B2
	1	Advanc	ed <u>D</u> etails	There is a privat	te key cor	respond	ding to this (certificate.
				_			Acce	ept All Cancel

Accept all -> übernimmt das Zertifikat in die Notes ID

6) Tadaa – fertig! Nun kann man Mails an Internetuser signieren

Delivery Options				? ×
Basic Advanced				ОК
Delivery Options				Cancel
Importance:	Normal	•	Return receipt	
Delivery report:	Only on failure	•	Prevent copying	
Delivery priority:	Normal	•	Auto spellcheck	
			🗌 Mark Subject Confidential	
 Do not notify me if recipe Do not expand person Security Options Sign Encrypt Save these security options 	ipient(s) are running Out of Office nal groups otions as the default		Mood Stamp Normal	

Dadurch wird der eigene public Key mitgesendet – der Empfänger muß das Zertifikat akzeptieren und den Absender ins Adreßbuch aufnehmen. Damit können dann verschlüsselte Nachrichten über SMTP ausgetauscht werden!

7) Umgekehrt muß man im Notes Client den **Absender** einer unterzeichneten email ins **lokale Adreßbuch** aufnehmen um seinen public Key zu speichern!

Issue Cross Certificate	? 🗙
Certifier	Bemhard Kolb/ebe
<u>S</u> erver	Local
Subject name	EMAIL=bemhard@bkolb.at/CN=Bemhard Kolb/O=EE
Subject alternate names	
Fingerprint	992E A9EF ABC9 79A0 A793 EE71 68F4 7655
Expiration date	24.08.2020 18:51:27
	Cross certify Cancel

		ОК
Basics		
Title:		Cancel
First name: Berr	hard	
Middle name:		
Last name: Kolb	•	
Suffix:	•	
Advanced		
Mail system:	Lotus Notes	
Routing domain(s):		
E-mail address:	Bernhard Kolb/ebe	
Include X.509 ce	rtificates when encountered 🔹	

Wichtig: include X.509 certificates!