eMail Verschlüsselung und TLS/SSL für Einsteiger

1. S/MIME-Verschlüsselung & Alternativen 2. TLS/SSL-Jump-Start

Agenda

- Warum?
- Grundlagen der Verschlüsselung
- eMail-Verschlüsselung im Allgemeinen
- eMail-Verschlüsselung mit LN-Bordmitteln
- Alternativen
- TLS/SSL in Kürze
- Selbsterstelltes SSL-Zertifikat
- Kauf und Installation eines SSL-Zertifikats
- Domino HTTPS-Konfiguration

Warum Verschlüsselung?

- Unsere Privatsphäre schwindet
- Das Bewusstsein f
 ür Geheimhaltung von Unternehmensdaten nimmt ab
- Die Gefährdung von vertraulichen Daten nimmt zu
- IT-Sicherheit wird immer komplexer und damit unbeherrschbarer

Stand der politischen Diskussion

 CCC fordert Ausstieg aus unverschlüsselter Kommunikation, 22. 1. 2015

"Ganz im Gegensatz zu dem von militärischen und politischen Akteuren losgetretenen Kampf gegen Verschlüsselung und für mehr Überwachung setzt sich der Chaos Computer Club (CCC) für zukunftssichere Technologien ein und fordert daher ein Verbot unverschlüsselter Kommunikation."

• Innenminister De Maizière, 21. 1. 2105 "Unter anderem müssen die deutschen Sicherheitsbehörden "befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln"".

Was passiert beim eMail-Senden?

- Analogie zum Fahrradkurier
- MIME-Spezifikation enthält keine Sicherungsfunktionen
- Daten können mitgelesen werden
- Daten können gefälscht werden
- Ein falscher Absender kann vorgetäuscht werden

Was hätten wir gern?

- Vertraulichkeit: nur der gewünschte Empfänger darf den Inhalt lesen
- Authentizität: Sicherstellen der Identität von Sender und Empfänger
- Integrität: keine Verfälschung von Inhalten

Verschlüsselung

- Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text (oder Bilder, Audio, Video) mit Hilfe eines
 Verschlüsselungsverfahrens in eine "unleserliche", das heißt nicht einfach interpretierbare Zeichenfolge umgewandelt wird.
- Parameter der Verschlüsselung sind:
 - ein oder auch mehrere Schlüssel
 - der verwendete Algorithmus

Wie arbeitet Verschlüsselung?

- Mathematisches Verfahren, um die Quelldaten mittels einer Schlüssel-Zeichenkette in ohne Schlüssel unlesbare Zieldaten zu verwandeln
- Rücktransfer ist nur mit dem passenden Schlüssel möglich
- Es gibt Verfahren, die nach dem heutigen Stand der Technik absolut sicher sind

Symmetrische Verschlüsselung

- Verwendung eines einzelnen Schlüssels
- Vorteile:
 - Einfach
 - Verwendung für gemeinsam genutzte Dateien
- Nachteile:
 - Austausch muss organisiert werden
 - Schlüssel darf nicht in unbefugte Hände gelangen
 - Anzahl der Schlüssel bezogen auf die Anzahl der Teilnehmer wächst quadratisch

Asymmetrische Verschlüsselung

- Verwendung von Schlüsselpaaren (öffentlicher und privater Schlüssel)
- Vorteile:
 - Jeder hat nur ein Schlüsselpaar
 - Hohe Sicherheit
 - Kein Schlüsselverteilungsproblem
 - Möglichkeit der Authentifikation durch elektronische Unterschriften (digitale Signaturen)
- Nachteile:
 - komplex
 - Rechenaufwändig (kann auch ein Vorteil sein!)

Digitale Zertifikate

 Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.

Quelle: Wikipedia

Zusammenhang zwischen Schlüssel und digitalem Zertifikat

- Jedes digitale Zertifikat ist mit einem öffentlichen Schlüssel verknüpft, dem ein privater Schlüssel zugeordnet ist. Diesen privaten Schlüssel besitzt nur der Zertifikatsinhaber.
- Das Zertifikat, das den öffentlichen Schlüssel enthält, kann hingegen in einem Verzeichnis publiziert und so jedem zugänglich gemacht werden, der mit dem Inhaber eines Zertifikats sicher kommunizieren möchte.

Public-Key-Infrastruktur

 Mit Public-Key-Infrastruktur (PKI) bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.

Wie prüfe ich die Validität eines Zertifikats?

 Der Browser oder das eMail-Programm machen das f
ür mich [©]

Allgemein Details Zertifizierungspfad		
Zertifizierungspfad TC TrustCenter Universal CA I TC TrustCenter Class 1 L1 CA IX		
	Zertifikat anzeigen	
Zertifizierungsstatus:		
Dieses Zertifikat ist gültig.		Se

Verschlüsselung in Notes Domino

- Verschlüsselung ist integraler Bestandteil des Notes/Domino-Sicherheitskonzepts
- PKI-Infrastruktur
 - Interne Notes-Mails können out-of-the-box signiert und verschlüsselt werden
- Verschlüsselung der Kommunikation zwischen Client und Server
- DBs können auf dem Laptop verschlüsselt werden
- ...und vieles mehr

S/MIME-Verschlüsselung in Notes mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Was brauche ich?

- Mein Schlüsselpaar (privater und öffentlicher Schlüssel)
- Den öffentlichen Schlüssel des Empfängers
- Die richtigen Einstellungen am Notes-Client

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Was braucht die Gegenseite?

- Ihr/sein Schlüsselpaar (privater und öffentlicher Schlüssel)
- meinen öffentlichen Schlüssel (Schlüssel des Empfängers)
- Die richtigen Einstellungen in seinem Mail-Client

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 19

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Wie richte ich meinen Notes-Client ein?

- Arbeitsumgebung einstellen
- Personendokument konfigurieren
- Zertifikat mit privatem Schlüssel in Notes-ID importieren
- Öffentliche Schlüssel der Mail-Empfänger in Adressbuch einfügen

 Um SHA-2-Zertifikate zu unterstützen, werden die "FIPS 140-2"-Algorithmen benötigt! (Admin-9-Hilfe)

Arbeitsumgebung einstellen

Diese Einstellung sorgt dafür, dass der Client die MIME-Konvertierung vornimmt. Das ist nötig, weil nur der Client den Schlüssel hat.

Arbeitsumgebung: ITEE Office (Network)

Entwic

Allgemein	Server	Ports	Mail	Internet-Browser	Replizierung	Erweitert	Administration	
-----------	--------	-------	------	------------------	--------------	-----------	----------------	--

Speicherort der Maildatei:Lokal I I Lokal I I Lokal I I Lokal I I I I I I I I I I I I I I I I I I I	Mail		
Maildatei:「maillykunert」Domino-Maildomäne:「ITEE」Domino-Maildomäne für Notes-Adressen, wenn direkte Verbindung zum Internet besteht:「ITEE」Schnelladressierung:Erst lokal dann Server」Schnelladressierung:Erst lokal dann Server」Schnelladressierung:Bei jedem Zeichen」Bei jedem Zeichen」Stopp nach der ersten Übereinstimmung」Mailadressierung:Nur lokal IMailadressierung:Uber Domino-Server」Sormat für Nachrichten übertragen, wenn:IMIME-FormationAusgehende Mail übertragen, wenn:Imiter warten	Speicherort der Maildatei:	CLokal	
Domino-Maildomäne: ITEE _ Internetdomäne für Notes-Adressen, wenn direkte Verbindung zum Internet besteht: IEst lokal dann Server _ Schnelladressierung: Erst lokal dann Server _ Schnelladressierung: Bei jedem Zeichen _ Schnelladressierung: Bei jedem Zeichen _ Schnelladressierung: Stopp nach der ersten Übereinstimmung _ Mailadressierung: Nur lokal _ Ausgehende Mail Ober Domino-Server _ Format für Nachrichten 	Maildatei:	^r mail\jkunert_	
Internetdomäne für Notes-Adressen, wenn direkte Verbindung zum 	Domino-Maildomäne:	^C ITEE	
Schnelladressierung:Erst lokal dann Server •Schnelladressierung aktivieren:Bei jedem Zeichen •Empfänger nachschlagen:Stopp nach der ersten Übereinstimmung •Mailadressierung:Nur lokal •Ausgehende Mail senden:Über Domino-Server •Format für Nachrichten an Internetadressen:IMIME-Format •Ausgehende Mail übertragen, wenn:Nachrichten warten	Internetdomäne für Notes-Adressen, wenn direkte Verbindung zum Internet besteht:		
Schnelladressierung Bei jedem Zeichen] • Ausgehende Mail Stopp nach der ersten Übereinstimmung] • Mailadressierung: Nur lokal] • Ausgehende Mail Über Domino-Server] • Format für Nachrichten an Internetadressen: MIME-Format] • Ausgehende Mail Image: Ima	Schnelladressierung:	🖥 Erst lokal dann Server 🛛 💌	
Empfänger nachschlagen:Stopp nach der ersten ÜbereinstimmungMailadressierung:Nur lokalAusgehende Mail senden:Über Domino-ServerFormat für Nachrichten an Internetadressen:MIME-FormatAusgehende Mail übertragen, wenn:Inachrichten warten	Schnelladressierung aktivieren:	^r Bei jedem Zeichen 🛛 💌	
Mailadressierung: Nur lokal • Ausgehende Mail senden: Über Domino-Server • Format für Nachrichten an Internetadressen: MIME-Format • Ausgehende Mail übertragen, wenn: • Nachrichten warten	Empfänger nachschlagen:	🖥 Stopp nach der ersten Übereinstimmung 🛛 💌	
Ausgehende Mail senden:Über Domino-Server]Format für Nachrichten an Internetadressen:MIME-Format]Ausgehende Mail übertragen, wenn:Inachrichten warten	Mailadressierung:	🖥 Nur lokal 🛛 💌	
Format für Nachrichten Image: Milde-Formation an Internetadressen: Ausgehende Mail übertragen, wenn:	Ausgehende Mail senden:	[╔] Über Domino-Server 』 ▼	
Ausgehende Mail übertragen, wenn:	Format für Nachrichten an Internetadressen:	[™] MIME-Format _a ▼	
	Ausgehende Mail übertragen, wenn:	ິ _ Nachrichten warten	\leq

Problem! Herausforderung

- Wenn die MIME-Einstellung in der Arbeitsumgebung falsch ist, wird gar nicht signiert/verschlüsselt, ohne Fehlermeldung!
- Achtung: Policies!

Personendokument konfigurieren

Im Personendokument des Domino Directory:

Person: Dirk Nowitzki/ITEE/De DirkNowitzki@itee.de

Allgemein Büro/Privat Andere Verschiedenes Zertifikate Roaming Administration

Allgemein	
Vorname:	^r Dirk_
2. Vorname:	Г J
Nachname:	[⊯] Nowitzki ⊒
Benutzername:	[©] Dirk Nowitzki/ITEE/De Dirk Nowitzki dirk@ite2.de ⊫

Alternative Namen:

Kurzname/BenutzerID:	🖥 DNowitzki 🗉
Anrede:	ſ
Generationskennung:	ſ. •

Mail

dem Speichern in Maildatei verschlüsseln:

Mailsystem:	^r Notes 」 ▼
Domäne:	『ITEE 』
Mail-Server:	『ITEENS03/ITEE/De』
Maildatei:	[©] mail\dnowitzk_
Weiterleitungsadresse:	Г
Internetadresse:	^ℤ DirkNowitzki@itee.de <u>』</u>
Bevorzugtes Format für eingehende Mail:	[₡] Format des Absenders beibehalten _
Eingehende unverschlüsselte Mail vor	r

r Jaur 🗸

Guten Tag Juergen Kunert,

Sie haben eine TC Internet ID mit den folgenden Daten beantragt:

Name:.....Juergen Kunert Land:..... Deutschland

Wir bestätigen Ihren Antrag mit der Antragsnummer 404159485.

Ausstellung des Zertifikates

Damit wir Ihr Zertifikat ausstellen können, müssen Sie zunächst auf der Antragsstatusseite ein Schlüsselpaar erzeugen.

Das erforderliche Passwort für den Zugang zu der Antragsstatusseite erhalten Sie gesondert per E-Mail oder SMS (entsprechend der Auswahl bei der Antragsstellung).

Antragsstatusseite:

https://www.trustcenter.de/RetailStore/cid/Login.action?loginName=fOKFsgGHUWgQDS Nach der Schlüsselerzeugung erfolgen unmittelbar die Ausstellung Ihres Zertifikates sowie die Installation des Zertifikates in Ihrem Browser.

HINWEIS: Wir empfehlen Ihnen, sich eine Sicherheitskopie Ihres privaten Schlüssels und des Zertifikates zu erstellen. Sollte zu einem späteren Zeitpunkt, z.B. nach Verlust des privaten Schlüssels, ein Ersatzzertifikat benötigt werden und keine Sicherheitskopie vorliegen, muss ein neues Zertifikat zu dem dann aktuell gültigen Preis beantragt werden.

Sperrung Ihres Zertifikats

Zum Sperren Ihres Zertifikates rufen Sie bitte folgende URL auf: http://www.trustcenter.de/sperren

Sollten Sie auf Ihr Zertifikat keinen Zugriff mehr haben, können Sie die Sperrung auch telefonisch unter +49 40 / 80 80 26-113 veranlassen. Bei Nennung Ihres –bei der Antragsstellung von Ihnen angegebenen –Notfallpasswortes wird die sofortige Sperrung Ihres Zertifikats veranlasst.

Support

Bei technischen Fragen wenden Sie sich bitte an den Support: https://www.verisign.de/support/contact-support/index.html

Vielen Dank, dass Sie sich für TC TrustCenter entschieden haben.

🔰 trustcenter.de | https://www.trustcenter.de/RetailStore/cid/SelfService!reload.action?refId=ca157671f4cb3b656e2d534959e52a0437b31084

🏠 マ C 🚼 - tc tru:

	TRUSTCENTER
14	Now part of Symantec

Zertifika TC Inter Antr

Now part of Symantec											Unser Supj
rtifikatsantrag Einternet ID											
Antragsstatus					Einstellunger	n					×
Übersicht						۵. چ		00		\bigcirc	i i i i i i i i i i i i i i i i i i i
Antragsnummer: Referenznummer: Produkt: Gültigkeit: Bearbeitungsstatus des Zertifikatantrags:	4041 ca15767114cb3b656e2d534959e52a0437t TC Inte 1 Jahr Q	159485 b31084 ernetID -0,00€ Zertifika	at-Manager		Allgemein Net	Tabs Inhai	t Anwendungen Verschlüsselung		Sicherheit	Sync	Erweitert
		Ihre Zertifik	kate Personen Serv	er Zertifizierun	gsstellen Andere	1					
Ihr Zertifikat		Sie haber Zertifika	n Zertifikate dieser Or atsname	ganisationen, d Kryptograf	lie Sie identifizierer phie-Modul	n: Serier	nummer	Läuft ab ar	n	Ę	
Ihr Zerlifikat kann installiert werden.		🖃 TC Tru Ju	ustCenter GmbH Iergen Kunert	Software-Si	cherheitsmodul	00:D6:	50:00:01:00:02:1E:0	DE 25.04.2013			
	Zertifikat in:		Wählen Sie Das Zertifika erstellen. Sie Zertifikats-B: Zertifikats-B: Wichtig: We	ein Zertifika ts-Backup-Passi müssen dieses ackup-Passwort ackup-Passwort	Ats-Backup-Pas wort, das Sie hier Passwort festlege : (nochmals):	sswort festlegen, schüt: en, um mit dem B	zt die Backup-Datei, ackup fortzufahren.	die Sie im Momeni			
			Passwort-Qu	ilen. Bitte schre	iben Sie es an ein	em sicheren Plat:	nieder.	Abbrech	en		

Ansehen...

Sichern...

Alle sichern...

Löschen...

Importieren...

Seite 26

OK

- Nach Anmeldung auf Webseite wird das Zertifikat in den Zertifikatsspeicher des Betriebssystems/Browsers gespeichert
- Zugriff über Internet Explorer/Internetoptionen
- von dort exportieren
- Ggf. Häkchen bei "privaten Schlüssel exportieren" setzen

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

nternetoptione	n				?			
Verbindung	en	Pro	gramme		Erweitert			
Allgemein	Sich	erheit	Datensc	hutz	Inhalte			
Inhaltsratgeber Filter helfen Ihnen bei der Kontrolle der Internetinhalte, die auf diesem Computer angezeigt werden können.								
Zertifikate Zertifikate werden für verschlüsselte Verbindungen und zur Identifizierung verwendet.								
SSL-Status löschen Zertifikate Herausgeber								
Auto vorhi und s	Vervollstär erige Einga schlägt Üb	ndigen speid aben auf We ereinstimmu	hert ebseiten ngen vor.	Eins	tellungen			

27

 von dort exportieren in eine .p12-, .p7b oder .cer-Datei

🕮 Zertifikate											
Datei Aktion Ansicht ?											
🗐 Zertifikate - Aktueller Benutzer	Ausgestellt für 🔥	Ausgestellt von	Gültig bis	Beabsichtigte Zwecke	Angezeigter Name	Statu:					
M:\ITEE\JUERGENKUNERT_TC_!	🔛 Juergen Kunert	TC TrustCenter	25.04.2013	Clientauthentifizieru	<keine></keine>	R					
	🔤 Juergen Kunert	TC TrustCenter	25.04.2013	Clientauthentifizieru	<keine></keine>	R					
	🖼 TC TrustCenter Class 1 L1 CA IX	TC TrustCenter	31.12.2025	<alle></alle>	<keine></keine>	R					
	🔤 TC TrustCenter Class 1 L1 CA IX	TC TrustCenter	31.12.2025	<alle></alle>	<keine></keine>	R					
	🖼 TC TrustCenter Universal CA I	TC TrustCenter	31.12.2025	<alle></alle>	<keine></keine>	R					
	🕮 TC TrustCenter Universal CA I	TC TrustCenter	31.12.2025	<alle></alle>	<keine></keine>	R					
< · · · · · · · · · · · · · · · · · · ·	<					>					
Der Speicher "M:\ITEE\JUERGENKUNERT_	TC_SMIME.P7S" 6 Zertifikate.										

Seite 28

- Alternativen:
- <u>https://www.instantssl.com/ssl-certificate-</u> products/free-email-certificate.html
- oder selber machen mit openssl: <u>https://gist.github.com/richieforeman/3166</u> 387

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 29

- Datei\Sicherheit\Benutzersicherheit
- Ihre Identität\Ihre Zertifikate

Benutzersicherheit

		Zertifikate in	Ihrer ID-Datei									
6 77	Sicherheit allgemein	Ihre Zertifikate	hre Zertifikate identifizieren Sie sicher gegenüber Notes und anderen Programmen. Ihre ID kann sowohl									
🧟 E	Ihre Identität	Zertifikate zur :	Zertifikate zur sicheren Kommunikation in Notes als auch Zertifikate für das Internet enthalten.									
	Ihre Namen											
	Ihre Zertifikate	Alle Zertifikate		Umfasst Ihre In Zertifizierungsst	ternet- und Notes-Zertifik ellen, die Ihre Zertifikate	ate und 2 ausgeste	Zertifikate für die ellt haben.					
	Ihre Smartcard			_								
🕭 E	Identität anderer	Typ Ausgeste	ellt auf 🗘	Ausgest	ellt von 🌣		Zertifikate abrufen 🕶					
🧏 E	Tätigkeiten anderer	🙀 Juergen	Kunert/ITEE/De	/ITEE/D	e	^	Notes-Zertifikate importieren (in ID aufnehmen)					
		🖳 🕅 Juergen	Kunert/ITEE/De	/ITEE/D	/ITEE/De		Neues nicht hierarchisches Notes-Zertifikat anfordern					
📚 🗄	Notes-Daten	🛛 🖳 /ITEE/D	e	/ITEE/D	e		Internetzertifikate importieren					
2	Mail	💽 TC Trust	Center Class 1 L1	CAIX TC Trus	Center Universal CA I	Neues Internetzertifikat anfordern						
		🚺 🚺 TC Trust	Center Universal C	AI TC Trust	Center Universal CA I	~	Internetzertifikat von einer Smartcard importieren					
		Ausgewähltes	Element									
		Ausgestellt auf	Juergen Kunert/I	ITEE/De								
		Ausgestellt von	/ITEE/De									
		Aktiviert	04.08.2010	Тур	Notes - Internationale V	selung						
		Ablaufdatum	05.02.2013	Schlüsselbezeichner	17N9F QWXQ6 JDEU?	61WX2 F84D7						
		Erweiter	te Details									

Zertifikate abrufen ▼	Datei mit den l	nternetzertifika	ıten angeben			? 🗙
Notes-Zertifikate importieren (in ID aufnehmen) Neues nicht hierarchisches Notes-Zertifikat anfordern	Suchen in:	20120427	~	G 🕫	• 🖽 🥙	
Internetzertifikate importieren Internetzertifikat von einer Smartcard importieren Thermetzertifikat von einer Smartcard importieren Thermetzertifikat von einer Smartcard importieren Thermetzertifikat von einer Smartcard importieren	Zuletzt Verwendete D Desktop Eigene Dateien Arbeitsplatz Netzwerkumgeb	Dateiname: Dateityp:	PKCS12-Dateien (*.p12, *.pfx) PKCS12-Dateien (*.p12, *.pfx) PKCS7-Dateien (*.p7b, *.p7c) Binäre und Base64-Dateien (*.cer Alle Dateien	, *.der)		Öffnen Abbrechen Hilfe

Importdateiformat auswählen	? ×	Kennwort eingeben		? ×		
In welchem Format ist Ihr Zertifikat in der Datei gespei	chert?	Geben Sie das Kennwo	ort für die Datei ein, die d	ie Internetzertifi		
O Binär X.509		Kennwort				
O Base 64 X.509			ОК	Abbrechen		
PKCS 12						
O PKCS 7	Internetz	ertifikate importieren		? ×		
	Möchten	Sie folgende Zertifikate anne	hmen und in Ihre ID-Date	i aufnehmen?		
Weiter Abbre	che Alle Interne	etzertifikate 😽 😽]			
	Typ Aus	Typ Ausgestellt auf ♀ Ausgestellt von ♀				
	💽 ТС	TrustCenter Class 1 L1 CA IX	TC TrustCenter Ur	niversal CA I		
	TC 💽	TC TrustCenter Universal CA I TC TrustCenter Universal CA I				
	🚺 🚺 Jue	rgen Kunert	TC TrustCenter Cla	ass 1 L1 CA IX		
Ausgewähltes Element:						
	Ausgestellt	auf Juergen Kunert	(E-Mail)	Juergen.Kunert@itee.de		
		von TC TrustCenter Class 1 L1 CA	IX (E-Mail)			
	Aktiviert	24.04.2012 Тур	Internet - Mehrzweck			
	Ablaufdatur	m 25.04.2013 Digest	B9E8 9254 3009 2687 AE	2E 34CF DA61 CC26		
ntwicklerCamp 2015 - Jürgen Kunert - I		veiterte Details Zu diesem Ze	rtifikat gehört ein privater Schlu	issel.		
			Alle an	nehmen Abbrechen		

 Sicherheit allgemein 	Ihre Zertifikate identifizieren Sie sicher geger Zertifikate zur sicheren Kommunikation in No	nüber Notes und anderen Programmen. Ihre ID kann sowohl otes als auch Zertifikate für das Internet enthalten.	
Ihre Namen Ihre Zertifikate Ihre Smartcard	Alle Zertifikate Vm Zer	fasst Ihre Internet- und Notes-Zertifikate und Zertifikate für die tifizierungsstellen, die Ihre Zertifikate ausgestellt haben.	
👧 🗉 Identität anderer	Typ Ausgestellt auf ≎	Ausgestellt von ≎	1
😤 🗉 Tätigkeiten anderer	Juergen Kunert/ITEE/De		1
💝 🗉 Notes-Daten	TC TrustCenter Class 1 L1 CA IX	TC TrustCenter Universal CA I]
🖄 Mail	TC TrustCenter Universal CA I Juergen Kunert	TC TrustCenter Universal CA I	
	Ausgewähltes Element Ausgestellt auf Juergen Kunert/ITEE/De Ausgestellt von /ITEE/De Aktiviert 07.11.2012 Typ Ablaufdatum 08.11.2014 Schlüsse Erweiterte Details Schlüsse	Notes - Internationale Verschlüsselung Hbezeichner 17N9F QWXQ6 JDEU7 K81S5 61WX2 F84D7	
		OK Schließen	-

Was habe ich davon?

- Ich kann signierte Mails verschicken
- Ich kann Mails lesen, die mit meinem Public Key verschlüsselt sind
- Geht auch in iNotes, wenn ID-Datei in Maildatei importiert ist
- Geht auch in Traveler (Android)/CompanionLink (iPhone), wenn ID-Datei in Maildatei importiert ist

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Betreff/Subject einer Mail

- wird nicht verschlüsselt

 weder in interner eMail
 noch bei S/MIME
- "Anfrage nach Suchtberatung"

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 36
Wenn eine signierte Mail ankommt

Was habe ich davon?

- Die eMail wurde von jemandem versendet, der Zugriff auf den privaten Schlüssel hatte
- Wenn die Signatur intakt ist, wurde die eMail nicht verändert
- So sieht das dann aus:

Dieses Dokument wurde nach dem Signieren geändert! Möglicherweise wurde eine absichtliche Manipulation vorgenommen.

Wenn eine signierte Mail ankommt

- Gegenzertifikat im lokalen Adressbuch erstellen, nachdem man geprüft hat dass die Mail authentisch ist
- Künftig wird dann dieser Signatur vertraut

EntwicklerCamp 2015 - Jürgen Kur

Gegenzertifikat auss	tellen ? 🗙
<u>Z</u> ertifizierer <u>S</u> erver	Anne Wiesmann/Notes-Werkstatt Local
S <u>u</u> bjekt	EMAIL=gschrod@web.de/CN=Gerald Peters/L=Ham 🔽
Alternativer Subjektname	
Fingerabdruck	8DFD 29C3 A1F8 2973 E35F 8B44 6749 7CAF
<u>A</u> blaufdatum	31.07.2022 19:28:18
	Gegenzertifizieren Abbrechen

Praxis: Schlüsselaustausch Empfänger Notes 1

- Ich habe eine signierte Mail bekommen
- Mail mit Signatur markieren

▶ •	B •	Û	Mehr +	Q	Q •		
			Vorga Abwe	aben. senh	 eit		
			Коріе	ren ir	n neue(n) 🕨	
			Abse	nder :	zur Kor	taktliste hinzufügen	
			Mail von Absender in den Ordner für unerwünschte Mail				
log4': ?	berpr?	'ft]	Bespr	rechu	ng plar	ien	
udemirer's glass		Neue Doku Quick Mailee	Nach ment Rule	als 'Ab erstelle	it Vorlage gelaufen' markieren/Markierung aufheben en		
20308	001):1	kurz	Maiire	syein			

Praxis: Schlüsselaustausch Empfänger Notes 2 Absender hinzufügen

Häkchen setzen: Gegebenenfalls X.509-Zertifikate aufnehmen

EntwicklerCam

Absender zur Kont	aktliste hinzufügen	? ×
All		ОК
Aligemein		
Titel:	▲	Abbrechen
Vorname:	tephan	
2. Vorname:		
Nachname: E	rnst	
Namenszusatz:	✓	
Erweitert		
Mailsystem: 🔍	Internet 💙	
Routing-Domäne(n):	
E-Mail-Adresse:	Stephan Ernst <stephan.ernst@trigonum.de></stephan.ernst@trigonum.de>	
🔽 Gegebenenfall	s X.509-Zertifikate aufnehmen 🔹	
K		
	•	

Praxis: Schlüsselaustausch Empfänger Notes 3 Kontakt ansehen

<u>Kategorie:</u>

Kommentare Angaben zum Namen Zertifikate

Internetzertifikate:

Internetzertifikat: Aussteller des Internetzertifikats:

Vorhanden

1. CN=www.magical.de/O=magical Workflow GmbH/ST=Hamburg/C=DE

Notes-Zertifikate:

Zertifizierter öffentlicher Schlüssel:	
Schlüssel für einfachen Namen:	

Praxis: Schlüsselaustausch Empfänger Notes: Kontakt ansehen

- Email-Adresse darf nur im RFC821-Format dort stehen:
- Juergen.Kunert@itee.de
- Nicht im erweiterten RFC822:
- "Jürgen Kunert" <<u>Juergen.Kunert@itee.de</u>>
- RFC 821 definiert die Standardkonvention f
 ür die Namensgebung von Mailbox-Adressen, z. B. "user@domain", bekannt als RFC 821-Adressierung.
- Nachfolger: RFC 822 im Format "Phrase" <localpart@domainpart>
- Ein optionaler Anzeigename zeigt den Namen des Empfängers an, wie er in der Mail-Anwendung des Benutzers angezeigt wird, z. B. "Jürgen Kunert" <Juergen.Kunert@itee.de>.

Manuell Zertifikat zu einer Adresse hinzufügen

 Wenn Konvertierung falsch eingestellt war, sieht man einen Anhang:

Signierte Mail

gerald - smime.p7s

- Anhang abhängen
- Dann Personendokument öffnen, hinzufügen:

	Aktionen	Werkzeuge	Fenster	Hilfe
	Weiterl	leiten		🗶 📑 Christian Wetien - Kontak
	In Ordr	her verschiebe	en	
	Aus Or	dner entferne	n	
	Bearbe	iten		
	vCard	weiterleiten		
1	Bespre	chung planen		
	Nachrio	ht senden:		
	Chatte	n		
q	In Papi	erkorb versch	ieben	
	Zertifik	ate	۱.	Gegenzertifikat erstellen
	Vorsch	au im Wab-Bro	weer b	Notes-Zertifikate überprüfen
l	vorsch	au iin web-bru	Jwser 🕨	Internetzertifikate überprüfen
e	erald Peters" <gschrod@web.d< td=""><td>Internetzertifikate importieren</td></gschrod@web.d<>			Internetzertifikate importieren
				Internetzertifikate exportieren

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

S	ian	iert	e M	lail	ser	nden

nden Sen	den und ableg	gen Als Entwurf speichern Zustelloptionen 🕨 🔻 🔗 🐻 Anzeigen
	I	🗌 Hohe Dringlichkeit 🔲 Empfangsbestätigung 🔽 Signieren 🔲 Verschl
	<u>An</u> :	Dirk.Nowitzki@itee.de
	Kopie:	
1000	Blindkopie:	
	Betreff:	Einladung zum Basketball-Turnier
	Diese Nachric	ht wird mit einer digitalen Signatur gesendet.

Lieber Dirk,

Falsch geschriebenes Wort suchen... Nachricht wird signiert... Mail wurde zur Zustellung abgegeben. (1 Person/Gruppe).

Probleme

 Wenn kein privater Schlüssel des Absenders da ist:

OK

IBM Lotus Notes



Sie haben angefordert, diese Internetnachricht zu signieren, aber Ihre aktuelle ID enthält bzw. verweist auf kein Internetzertifikat. Wenn die Nachricht trotzdem gesendet werden soll, wählen Sie 'OK', andernfalls 'Abbrechen'.

Abbrechen

 Wenn die MIME-Einstellung in der Arbeitsumgebung falsch ist, wird gar nicht signiert/verschlüsselt, ohne Fehlermeldung!

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Empfangen einer verschlüsselten Mail

Überprüfung auf neuen Maileingang... Sie haben neue Mail auf 'ITEENS01/ITEE/De' erhalten Dokument wird entschlüsselt...

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Senden einer verschlüsselten Mail

Senden	Senden und able	gen Als Entwurf speichern Zustelloptionen 🕨 🔻 🖉 🐻 Anzeigen 🕶 Mehr 🕶 🧖
		🗆 Hohe Dringlichkeit 🗖 Empfangsbestätigung 🗖 Signieren 🔽 Verschlüsseln 🗖
	<u>An</u> :	Dirk.Nowitzki@itee.de,
	Kopie:	
	Blindkopie:	
	Betreff:	Einladung zum Frühsport
	Diese Nachrid	sht wird verschlüsselt gesendet.
Lieber	Dirk, Falsch ges Mail wurde Dokument	thriebenes Wort suchen zur Zustellung abgegeben. (1 Person/Gruppe). wird verschlüsselt
	Verschlüss	Falsch: "mit ihrem privaten Schlüssel Falsch: "mit ihrem privaten Schlüssel"
vvenn	es nicht (jekiappi nai, ienit die ietzte Zelle!

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden
- Troubleshooting

Troubleshooting

- Ist das Zertifikat valide?
 - Zertifikatskette überprüfen
 - Zertifikat abgelaufen?
- Beim Import
 - Ist das zu importierende Zertifikat das richtige, habe ich das Richtige bestellt, das Richtige heruntergeladen?

Nachteile der Verschlüsselung mit Bordmitteln

- 1. Erklärungsbedarf
- 2. Administrativer Aufwand (Client)
- 3. Die User sind verantwortlich
- 4. Mail-Journaling funktioniert nicht mehr für diese Mails
- 5. Was macht der Virenscanner, das Signaturprogramm, etc. mit der signierten oder verschlüsselten Mail?

eMail-Verschlüsselung

- Einführung in die Verschlüsselung
- eMail-Verschlüsselung
- eMail-Verschlüsselung mit Bordmitteln
- Alternativen

PGP

- steht f
 ür Pretty Good Privacy
- von Phil Zimmermann entwickelt
- ebenso wie S/MIME Internet-Standard
- Plug-Ins/Zusatzprogramme f
 ür den Mail-Client n
 ötig, auch f
 ür Notes: PGPNotes
- genauso sicher wie S/MIME



- GNUPG: Kommandozeilenprogramm
- GPGWin, Download unter http://slproweb.com/products/Win32Open SSL.html
- Kleopatra: Schlüsselmanager
- etc.

Schlüssel erstellen in Kleopatra

🔁 Kleopatra		
Datei Ansicht Zertifikate Extras Einstellu	ngen Fenster Hilfe	
Neues Zertifikat	Strg+N	ren 🐼 Vorgang abbrechen 🛛 👋
AS Zertifikate auf Server suchen	Strg+Umschalt+I	Alle Zertifikate
ன Zertifikate importieren	Strg+I	te Importierte Zertifikate
🥁 Zertifikate exportieren	Strg+E	is Details 🛆 Schlüssel-Kennung
👔 Geheime Schlüssel exportieren		OpenPGP 01C9CCA0 OpenPGP 125624C9
Zertifikate zu einem Server exportieren	Strg+Umschalt+E	OpenPGP 817F20A3
🙀 Dateien entschlüsseln/überprüfen		3 OpenPGP 999E3E4B
🛃 Dateien signieren/verschlüsseln		
Prüfsummendateien erstellen		·
Prüfsummen-Dateien verifizieren		
😣 Schließen	Strg+W	
🔀 Beenden	Strg+Q	

🗖 Assistent zur Erstellung des Zertifikats

Format des Zertifikates wählen

Bitte wählen Sie den Typ des zu erstellenden Zertifikates.

- Persönliches OpenPGP-Schlüsselpaar erzeugen OpenPGP-Schlüsselpaare werden lokal auf Ihrem Rechner erstellt und von Ihren Freunden und Bekannten beglaubigt. Es gibt keine zentrale Beglaubigungsinstanz; jer er Anwender erstellt ein persönliches Netz des Vertrauens durch die Beglaubigung der Schlüsselpaare anderer durch sein eigenes Zertifikat.
- Persönliches X.509-Schlüsselpaar und Beglaubigungs-Anfrage erstellen X.509-Schlüsselpaare werden lokal erstellt, aber zentral durch eine Beglaubigungsinstanz (Certificate Authority, CA) beglaubigt. CAs können andere CAs beglaubigen, dadurch entsteht eine hierarchische Vertrauenskette.

Abbrechen

Weiter

2

X

5

👩 Assistent zur Erstellung des Zertifikats

Details eingeben

Bitte tragen Sie Angaben zu Ihrer Person ein. Für mehr Kontrolle über die Zertifikatseinstellungen wählen Sie bitte "Erweiterte Einstellungen".

?

х

<u>N</u> ame:	Dirk Nowitzki	(benötigt)
<u>E</u> -Mail:	Dirk.Nowitzki@itee.de	(benötigt)
Kommentar:		(optional)
	Dirk Nowitzki <dirk.nowitzki@itee.de></dirk.nowitzki@itee.de>	
	E <u>r</u> weiterte Einste	llungen
	<u>W</u> eiter <u>A</u> b	brechen
)



Zertifikat-Einstellungen überprüfen

Bitte überprüfen Sie vor der Zertifikatserstellung noch einmal Ihre Angaben.

 Name:
 Dirk Nowitzki

 E-Mail-Adresse:
 Dirk.Nowitzki@itee.de

 Schlüsseltyp:
 RSA

 Schlüsselstärke:
 2,048 Bits

 Verwendung des Zertifikats: Signieren, Verschlüsseln

5

Alle Details anzeigen

Schlüssel erzeugen Abbrechen

2

X

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 60

2

Abbrechen

einmal ein:

Bitte geben Sie die Passphrase noch

Passphrase ••••••••

OK

X

Abbrechen

Seite 61

X

Assistent zur Erstellung des Zertifikats

Geben Sie die Passphrase ein

Passphrase •••••••

OK

90%

Abbrechen

Qualität:

Schlüssel wird erzeugt ...

Ihr Schlüssel wird erstellt.

pinentry

Die Erzeugung eines Schlüssels benötigt sehr viele Zufallszahlen. Sie können diesen Vorgang unterstützen, indem sie im unten stehenden Eingabefeld irgendetwas beliebiges eingeben. Der Text selbst hat nichts weiter zu bedeuten, nur die Zeitspannen zwischen den einzelnen Tastendrücken. Sie können auch dieses Fenster hier mit der Maus hin- und herbewegen oder eine Festplatten-Intensive Anwendung starten.

23

Weiter

pinentry

EntwicklerCamp 2015	- Jürgen Kunert - ITEE

Assistent zur Erstellung des Zertifikats

Schlüsselpaar erfolgreich erzeugt.

Ihr neues Schlüsselpaar wurde erfolgreich erzeugt. Details und Vorschläge für weitere Schritte finden Sie weiter unten.

2

-Ergebnis

Zertifikat erfolgreich erzeugt. Fingerabdruck: CF31D7DC32E2EBB4999FE5AE412EE0FE25C051D4

Nächste Schritte

Sicherheitskopie Ihres Schlüsselpaares erstellen ...

Zertifikat per E-Mail versenden ...

Zertifikat an einen Zertifikatsserver übermitteln ...

<u>F</u>ertigstellen

2

X

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 62

Die Zwischenablage ist unser Freund

Senden E-Mail mi	Senden und able t PGPNotes	gen Als Entwurf speichern Zustelloptionen 下 🕈 🖉 Signatur 🛪 Anzeig	
	An: Kopie: Blindkopie: Betreff:	verschlüsselte Mail	
Hallo Ur hier eine vlg	sula, verschlüsselte	Mail, die ich über die <u>Zwischenablage</u> verschlüsselt und signiert habe.	

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 63

Zertifikate import	ieren 🔛 Zertifik	ate exportieren	C Aktualisieren	🐼 Vorgang abb	rechen	🍪 Zertifikate auf S	erver suchen	Zwischenablage
Search <alt+q> Alle Zertifikate Name Oliver Schn Sebastian Je Dirk Nowit Thomas Fü Ursula Müll Juergen K</alt+q>	Vertrauenswürd E-Mail Dirk.Nowitzki	lige Zertifikate Gültig ab 2013-10-24 2014-01-13 2015-02-26 2014-03-07 2014-12-30 2014-06-29	Andere Zertifikate Gültig bis 2017-10-24 2019-03-06 2019-06-28	Importierte Zert Details OpenPGP OpenPGP OpenPGP OpenPGP OpenPGP OpenPGP	fikate 010 010 125 250 817 999 999	Schlüssel-Kennung 29CCA0 5624C9 C051D4 7F20A3 92A266 9E3E4B	Alle Zertifika	Zertifikatimport Verschlüs eln S/MIME-Signieren OpenPGP-Signieren Entschlüsseln/Überprüfen

Empfänger					
Empfänger	Urs	chlüssel) <ursula_i< th=""><th>e.de> (999</th><th>92A266) 💌</th><th></th></ursula_i<>	e.de> (999	92A266) 💌	
	ß				
Empfänger hinzufüger	Ausgewählte e	ntfernen			
Warnung: Keines der verschlüsselten Daten	ausgewählten Zertifik anschließend wieder z	ate scheint Ihr eigenes Zertifikat z u entschlüsseln.	u sein. Sie werden nicht ir	n der Lage sein, die	

E-Mail-Nachricht verschlüsseln	
--------------------------------	--

Ergebnisse

Alle Operationen abgeschlossen.

Verschlüsseln abgeschlossen.

Fenster geöffnet lassen wenn Operation abgeschlossen

Zurück

2

V Abbrechen

2

X

100%

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Seite 66

Senden	Senden und able	gen Als Entwurf speichern Zustelloptionen ド 🕈 🖉 Signatur 🖲
E-Mail n	nit PGPNotes	
	An:	Ursula <u>_11.11aullar@t-online.d</u> e,
-	Kopie:	
	Blindkopie:	
	Betreff:	verschlüsselte Mail

-----BEGIN PGP MESSAGE-----Version: GnuPG v2

hQIMAwRUVD+ZkgJmARAAt1EIXRVevKmmW+QAsEBGTYavris0pr3xnR6zE5nTSiQz eRvzZsia66XPg7FTv9a2GgEW2FKBEgXoTXJ0sJ3/8cz4qxoAs4DBl8cD9P05SZU2 vYpEr6JARFYncVJk2otxzuvu0KcY28KdsrgesdAV2vDnPPG0TwuHqVXF3a6n7eDd dRgHIG61al+AK0F39tZuv+BMzUik1t5HJX3KQ6dEr0jUkgAaZ8i5d8UGsvcTol/X x7EmpKyHkN7fHDRyzp1s2BuPgciFQuInCBV4uko3gYK6NComLIGXHDAe1+YKJHGI xqq2Tdo6UiXTxEMeUXKA3/VULoWAI+0/iaxNEoV07PId1WmEv2qBxn1038CtRwP+ 0JHHCp/wBQIOZYVIHUFeEE5XVAS3GTPub2dYLI7cy3lmaRzhQD/L1l2c9LPpzluX i5aO1Wi8xQ6m7C8v007lvym840tvyq2AnPpM9AYp611Dv9YmNTovvw+5XxuvXo5R 9iGfl9rrH5sJ5D/PGCeLPsDqxDnW1FshqqVqeKulP87v9QaRaiXYhWPDYvlwAZrU vKLhqp0KIsVVVBqRwM0phXZ/hzWOo7I7VtQWBvo3vRSIrzLtHdwRJ8/JEd8BLtFh p0c9K0jbllpbcZ13PAKpX6WJchBHWxW7xtbJMeQjTwzMm7sVxaBdF8q05VEumIXS pgE4mc4aVduL9Zu3TcHNRiHa8x326Mu0kEziQDBbwfXV8TCDrmi4Vu4rRCveoK0b Z5Em5DpoU+6zQCWDiyHntqv1q4hRxCxfm6EvJTH11+3zwGtf3jlKMN8+5VHIdXUO yJx6PYp94XSF89wzJ89PUtMVVgr42SPpm0TKuEWM0Qgo21ElxO/nWCkiHZdaMBD1 u+yCVTFIfYqa6kz5Gr8zYuQRMbP432I= =2XvW

-----END PGP MESSAGE-----

PGPNotes

Kostenpflichtiges Plug-In f ür Notes (Teilmaske)

Senden Senden un	d ablegen Als Entwurf speichern Zustelloptionen Þ 🔻 🖉 Signatur 🛪 Anzeig	en 🔻 Mehr 🕈 📋 PGP Versc	hlüsseln/Senden
E-Mail mit PGPNote	s		ν <u>ς</u>
<u>An</u> :			
Коріє			
Blind	kopie:		
Betre	ff:		
🖾 I Empfänger	Betreff	Datum 🔻	Größe 🖉 🕨
a U	Test mit Anhang in der Mail mit PGPNotes verschlüsselt und signiert	26.02.2015 09:55	4,711 🖼

PGPNotes 2

pinent	y D3	Re: Test mit Anhang in der Mail mit PGPNotes verschlüsse
	Sie benötigen entsperren. Benutzer: "Jue 2048-bit RSA 9 999E3E4B) Passphrase	eine Passphrase, um den geheimen OpenPGP Schlüssel zu ergen Kunert <jku@ite2.de>" Schlüssel, ID 3A19B46D, erzeugt 2014-06-29 (Hauptschlüssel-ID</jku@ite2.de>
		OK Abbrechen
Trenta Mi		

Unterschiede S/MIME und PGP

- Vertrauen: Zertifikatshierarchie vs. Web Of Trust
- Schlüsselverwaltung: Kleopatra vs. Kontakte
- bei S/MIME wird beim Senden einer signierten Mail der Schlüssel mit versandt, bei PGP nicht
- Open Source
- S/MIME: kann die NSA mitlesen?

Perfect Forward Secrecy

- Folgenlosigkeit (englisch perfect forward secrecy, PFS; auf deutsch etwa perfekte vorwärts gerichtete Geheimhaltung) bedeutet in der Kryptographie die Eigenschaft von Schlüsselaustauschprotokollen, dass aus einem aufgedeckten geheimen Langzeitschlüssel nicht auf damit ausgehandelte Sitzungsschlüssel eines Kommunikationskanals geschlossen werden kann.^[1] Quelle: Wikpedia
- In Notes und Domino aktuell nicht implementiert,
- nur mit Proxy möglich

Alternativen (zu Bordmitteln)

- PGP
- Inhalt in verschlüsseltes PDF oder ZIP einpacken
- Eigenes Gateway zur Mail-Verschlüsselung (mit Schlüsselmanagement) (z.B. IQ-Suite)
- Verschlüsselung über externen Dienstleister/Cloud - Webmail
Was tun? Aspekte für eine Auswahl

- Abhängig von der Anzahl der Kommunikationspartner
- Abhängig von Gesetzen und Rechtsprechung
- Abhängig von Vertretungsregelungen
- Kosten
- Usability für die Endbenutzer
- Supportbarkeit f
 ür die internen Mail-Admins (verschl
 üsselte Mails lassen sich schlecht einsehen) -> Mail-Gateway
- Virenscanner kann nur unverschlüsselte Mails prüfen

Das war's zum Thema eMail-Verschlüsselung

Nun wird der Domino-Webserver abgesichert

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

TSL/SSL-Jumpstart

- Wie funktioniert SSL?
- Warum SSL?
- Wie bekomme ich einen Keyring?
- Konfiguration in Domino

SSL/TLS

- steht f
 ür Secure Socket Layer
- von Netscape entwickeltes Protokoll f
 ür Standard-Browser zum sicheren Übertragen von vertraulichen Informationen
 über das Internet
- unter dem neuen Namen TLS (Transport Layer Security) weiterentwickelt

Versionen

- <mark>SSL</mark> 2.0 1995
- S<mark>SL</mark> 3.0 1996
- TL<mark>S 1</mark>.0 1999
- TLS 1.1 2006 (aktuell nicht von Domino unterstützt)
- TLS 1.2 2008 (aktuell nicht von Domino unterstützt)
- TLS 1.3 to be announced

Wie funktioniert SSL?



Nach Erzeugung eines Session-Schlüssels wird zwischenClient und Server eine sichere Verbindung aufgebaut.

Warum TLS/SSL?

- Verschlüsselung:
 - Die Kommunikation zwischen Server und Client wird verschlüsselt
- Authentisierung
 - Der Client kann sich sicher sein, dass er mit dem gewünschten Server kommuniziert (unter Benutzung einer PKI)

Sicherheitslücken

- Poodle
- TLS 1.0
- Heartbleed (Domino nicht betroffen, aber ggf. vorgelagerte Systeme)
- und sicherlich einige, von denen wir noch nichts wissen…

Gekauftes oder selbsterstelltes Zertifikat?

- Nachteil:
 - Ein Gekauftes kostet Geld
 - läuft auch ab
- Vorteile:
 - höhere Sicherheit für die Clients
 - Wird von Browsern und anderen Clients akzeptiert (es gibt Ausnahmen)
 - Keine Arbeiten im Client-Browser

Zertifikate bearbeiten

- "Server Certificate Administration" wird nicht mehr weiterentwickelt,
- unterstützt keine aktuell sicheren Zertifikate
- Ersatz: openssl und kyrtool



Ε

Click on the steps below to create an SSL key ring and populate it with certificates.



with a self-certified certificate for testing purposes.

Create Key Ring with Self-Certified Certificate

OpenSSL

- Freie Software
- Das Tool, um Zertifikate zu managen
- <u>http://slproweb.com/products/Win32Open</u>
 <u>SSL.html</u>

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

OpenSSL Funktionalität

- CSRs generieren
- Zertifikate erstellen
- Zertifikate ansehen
- Zertifikate verifizieren
- Speicherformate konvertieren

OpenSSL Installation

- http://slproweb.com/products/Win32Open SSL.html
- Wir haben auf einem Win7/64-Windows-Rechner die folgenden Setup-Files genommen:
- Win64 OpenSSL v1.0.1j Light1MB Installer Installs the most commonly used essentials of Win64 OpenSSL v1.0.1j (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
- Visual C++ 2008 Redistributables (x64) 1.7MB Installer Having problems with error messages when trying to run 64-bit OpenSSL? This will likely fix the problem. Only works with Windows 2003 Server and later. Although there is a "newer version" of this installer, this is the correct version to install.

OpenSSL Konfiguration

- OpenSSL-Win64 ist das Installationsverzeichnis von OpenSSL
- C:\OpenSSL-Win64\bin>set OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg
- C:\OpenSSL-Win64\bin>set RANDFILE=.rnd

OpenSSL Aufruf

- Im Zweifel CMD als Administrator ausführen! oder
- Starten der openssl.exe

C:\OpenSSL-Win64\bin\openssl.exe	- 🗆 ×
OpenSSL> _	_
۲	
	-

 Dann muss bei den folgenden Sequenzen auf das anfängliche openssl verzichtet werden

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Schlüsselpaar generieren (Datei server.key):

C:\OpenSSL-Win64\bin>openssl genrsa -out server.key 4096

Loading 'screen' into random state - done Generating RSA private key, 4096 bit long modulus++

e is 65537 (0x10001)

C:\OpenSSL-Win64\bin>

.....++

Schlüssel ansehen: (Datei server.key) C:\OpenSSL-Win64\bin>type server.key -----BEGIN RSA PRIVATE KEY-----MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5 wZzl8U1b2XfwBwxr8g6

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8Zr Bsh+TXQVKX2k= -----END RSA PRIVATE KEY-----

C:\OpenSSL-Win64\bin>

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

CSR (server.csr) erzeugen, Zertifikatsinformationen eingeben:

C:\OpenSSL-Win64\bin>openssl req -new -sha256 -key server.key -out server.csr Loading 'screen' into random state - done You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:DE State or Province Name (full name) [Some-State]:Hamburg Locality Name (eg, city) []:Hamburg Organization Name (eg, company) [Internet Widgits Pty Ltd]:ITEE Organizational Unit Name (eg, section) []:Headquarter Common Name (e.g. server FQDN or YOUR name) []:WIN2008STD01.itee.zz Email Address []:juergen.kunert@itee.de

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:geheim An optional company name []:

C:\OpenSSL-Win64\bin> EntwicklerCamp 2015 - Jürgen Kunert - ITEE

CSR (server.csr) ansehen: C:\OpenSSL-Win64\bin>type server.csr -----BEGIN CERTIFICATE REQUEST-----MIIE+TCCAuECAQAwgZwxCzAJBgNVBAYTAkRFMRAwD gYDVQQIDAdIYW1idXJnMRAw

SNLIFpVXaHEk/JnMh2vOAE+I0+RiX0UiWhiJCBE=

C:\OpenSSL-Win64\bin>

. . .

Zertifikat selbst signieren (server.pem)

C:\OpenSSL-Win64\bin>openssl x509 -req -days 3650 sha256 -in server.csr -signkey server.key -out server.pem Loading 'screen' into random state - done Signature ok subject=/C=DE/ST=Hamburg/L=Hamburg/O=ITEE/OU=He adquarter/CN=WIN2008STD01.itee.zz/emailAddress=juerg en.kunert@itee.de Getting Private key

Zertifikat (server.pem)ansehen C:\OpenSSL-Win64\bin>type server.pem -----BEGIN CERTIFICATE-----MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFA DCBnDELMAkGA1UEBhMC

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k= ----END CERTIFICATE-----

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

- Und jetzt muss das Ganze in einen Schlüsselring:
- Dazu verwenden wir kyrtool
- Download:

http://www.ibm.com/support/fixcentral/swg/quickorder?pa rent=ibm%7ELotus&product=ibm/Lotus/Lotus+Domino&r elease=9.0.1.2&platform=All&function=fixId&fixids=KYR Tool_9x_ClientServer&includeSupersedes=0&source=fc

 Installation: (Kopieren) von kyrtool.exe ins Notes/Domino Programmverzeichnis

kyrtool Help: [C:\] kyrtool =c:\lotus\notes\notes.ini -h

KyrTool v1.0

kyrtool [=/path/to/notes.ini] command [subcommand] [flags]

Commands: create Create a new keyring file delete Delete a root in a keyring file import Import into a keyring file show Show information about a keyring file verify Verify the content of a PEM import file

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Schlüsselring erzeugen

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" create -k c:\lotus\notes\data\keyring.kyr -p geheim

Keyfile c:\lotus\notes\data\keyring.kyr created successfully

KYR-Datei

STH-Datei

29 KB

1 KB

Seite 96

C:\Program Files (x86)\IBM\Notes>

08.01.2015 19:12

08.01.2015 19:12

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

keyring.kyr

keyring.sth

Zertifikate (server.key und server.pem) zusammenfügen (server.txt)

C:\OpenSSL-Win64\bin>COPY C:\OpenSSL-Win64\bin\server.key+C:\OpenSSL-Win64\bin\server.pem server.txt

C:\OpenSSL-Win64\bin\server.key

C:\OpenSSL-Win64\bin\server.pem

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Zwischenergebnis ansehen: C:\OpenSSL-Win64\bin>type server.txt -----BEGIN RSA PRIVATE KEY-----MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6 ... 1p6/tll FeldCK l2pl \//8Xd3xqA3yOT/COSs2kB6XEP2yi8ZrBsb+TXO\/KX2k=

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k= -----END RSA PRIVATE KEY----------BEGIN CERTIFICATE-----MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC

ZzzPMQuMHhpQuHfvlu3chwcKWrw+aUBng+oQLf6kvDoPP/ZqcNyLX7hq+CFW9xmn 0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k= -----END CERTIFICATE-----

C:\OpenSSL-Win64\bin>dir server.* Volume in Laufwerk C: hat keine Bezeichnung. Volumeseriennummer: A0FB-9BD7

Verzeichnis von C:\OpenSSL-Win64\bin 08.01.2015 18:59 1.801 server.csr 08.01.2015 18:51 3.243 server.key 08.01.2015 19:01 2.041 server.pem 08.01.2015 20:31 5.285 server.txt 4 Datei(en), 12.370 Bytes 0 Verzeichnis(se), 4.394.057.728 Bytes frei EntwicklerCamp 2015 - Jürgen Kunert - ITEE

server.txt verifizieren:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" verify "C:\OpenSSL-Win64\bin\server.txt"

KyrTool v1.0

Successfully read 4096 bit RSA private key INFO: Successfully read 1 certificates INFO: Private key matches leaf certificate INFO: Final certificate in chain is self-signed

Zertifikat in den Schlüsselring importieren: C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" import all -k c:\lotus\notes\data\keyring.kyr -i "C:\OpenSSL-Wi n64\bin\server.txt"

Using keyring path 'c:\lotus\notes\data\keyring.kyr' Successfully read 4096 bit RSA private key SECIssUpdateKeyringPrivateKey succeeded SECIssUpdateKeyringLeafCert succeeded

Schlüssel anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" **show keys -k** c:\lotus\notes\data\keyring.kyr

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Key length: 4096 bits

-----BEGIN PUBLIC KEY-----MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwxx5LDjqs4s4jBGNncEr

u9GAIJwEWeEfdSXN8/JcuUkCAwEAAQ== -----END PUBLIC KEY-----

Key length: 4096 bits

-----BEGIN RSA PRIVATE KEY-----MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k= -----END RSA PRIVATE KEY-----

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Zertifikate anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" show certs -k c:\lotus\notes\data\keyring.kyr Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Certificate #0

Subject:

EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=D E

Issuer:

EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=D E

Not Before: 08.01.2015 19:01:41 Not After: 05.01.2025 19:01:41 Key length: 4096 bits Signature Alg: sha256WithRSAEncryption

-----BEGIN CERTIFICATE-----

MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k= -----END CERTIFICATE-----

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Zertifikate auf den Server kopieren: Domino/Data:

keyring.sth 08.01.2015 19:12 STH-Datei 1 KB	keyring.kyr	08.01.2015 19:12	KYR-Datei	29 KB
	keyring.sth	08.01.2015 19:12	STH-Datei	1 KB

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Schlüsselpaar generieren (Datei server.key):

C:\OpenSSL-Win64\bin>openssl genrsa -out server.key 4096

Loading 'screen' into random state - done Generating RSA private key, 4096 bit long modulus++

e is 65537 (0x10001)

C:\OpenSSL-Win64\bin>

.....++

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Erzeugten Schlüssel ansehen: (Datei server.key) C:\OpenSSL-Win64\bin>type server.key -----BEGIN RSA PRIVATE KEY-----MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5 wZzl8U1b2XfwBwxr8g6

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8Zr Bsh+TXQVKX2k= -----END RSA PRIVATE KEY-----

C:\OpenSSL-Win64\bin>

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

CSR (Certificate Signing Request, Datei server.csr) erzeugen, Zertifikatsinformationen eingeben:

C:\OpenSSL-Win64\bin>openssl req -new -sha256 -key server.key -out server.csr

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:. State or Province Name (full name) []: Locality Name (eg, city) [Default City]:. Organization Name (eg, company) [Default Company Ltd]:. Organizational Unit Name (eg, section) []:. Common Name (eg, your name or your server's hostname) []:www.example.com Email Address []:

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []: C:\OpenSSL-Win64\bin>

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

CSR (server.csr) ansehen: C:\OpenSSL-Win64\bin>type server.csr -----BEGIN CERTIFICATE REQUEST-----MIIE+TCCAuECAQAwgZwxCzAJBgNVBAYTAkRFMRAwD gYDVQQIDAdIYW1idXJnMRAw ...

SNLIFpVXaHEk/JnMh2vOAE+I0+RiX0UiWhiJCBE=

C:\OpenSSL-Win64\bin>

EntwicklerCamp 2015 - Jürgen Kunert - ITEE
- Auf die Webseite des Trustcenters gehen, auswählen, beraten lassen
- Fragen, welche Zertifikat das passende ist
 - Wir wollen Webmail/Traveler absichern
 - Wir wollen folgende Endgeräte einsetzen
 - Das Zertifikat soll so lange gelten

								4.11
	<u>Zertifiziert</u>	Domain <u>Beispiel</u> <u>Domain</u>	Domain <u>Beispiel</u> <u>Domain</u>	Domain <u>Beispiel</u> <u>Domain</u>	ldentität <u>Beispiel</u> Identität	ldentität <u>Beispiel</u> Identität	ldentität <u>Beispiel</u> Identität	
		🜔 ab 5.01	🜔 ab 5.01	🜔 ab 3.0	🜔 ab 5.01	🜔 ab 5.01	🜔 ab 3.0	
2		🔕 ab 6.0	🔕 ab 4.51	🔊 ab 2.0	🔊 ab 6.0	🔊 ab 4.51	🔕 ab 2.0	
		🛕 ab 5.0	🛕 ab 5.0	🛕 ab 3.0	🛕 ab 5.0	🛕 ab 5.0	🛕 ab 3.0	
		🚯 ab 8.0	🚯 ab 7.0	🚯 ab 3.0	🚯 ab 8.0	🚯 ab 7.0	🚯 ab 3.0	
		🧒 ab 1.0	🎯 ab 1.0	🎯 ab 1.0	🎯 ab 1.0	🎯 ab 1.0	🎯 ab 1.0	
		🥹 ab 1.0	🥹 ab 1.0	🥘 ab 1.0	🥹 ab 1.0	🥹 ab 1.0	🥘 ab 1.0	
Entwic	Unterstützte	🙀 ab 1.0	🙀 ab 1.0	횑 ab 1.0	🔍 ab 1.0	🙀 ab 1.0	👰 ab 1.0	
	Browser	🦻 ab 1.0	🦻 ab 1.0	🦻 ab 1.0	🦻 ab 1.0	🦻 ab 1.0	🦻 ab 1.0	
	<u>onne</u> Fehlermeldung	🎂 ab 1.5	cinalx ap 3.0	cineux ab 1.0	🎂 ab 1.5	cinaix ab 3.0	cimux ab 1.0	

Seite 109

FIKATSEIGENSCHAFTEN:

Auf die Webseite des Trustcenters gehen, auswählen, beraten lassen

	Darstellung (Muster)	POSITIVE SSL TRONED IN COMON	SECURED BY RapidSSL 128 bit SSL Security SiteSeal	Secured by that yyyy-mm-dd SiteSeal	Composition <u>TrustLogo</u> (außer bei 30 Tage, MDC und UCC)	VERIFIED BY GeoTrust* LYNCH, INC CLICK hh: mm ddimmlyy TrustLogo	Secured by thave yyyy-mm-dd <u>TrustLogo</u>	
	<u>Zwischen-</u> <u>zertifikat</u> <u>serverseitig</u> <u>erforderlich</u>	Ja <u>Beispiel</u> <u>Zwischen-</u> zertifikat	Ja <u>Beispiel</u> <u>Zwischen-</u> zertifikat	Ja <u>Beispiel</u> <u>Zwischen-</u> <u>zertifikat</u>	Ja <u>Beispiel</u> <u>Zwischen-</u> zertifikat	Ja <u>Beispiel</u> <u>Zwischen-</u> zertifikat	Ja <u>Beispiel</u> <u>Zwischen-</u> <u>zertifikat</u>	
	Ausstellende CA	Cornodo	RapidSSL/GeoTrust	Thawte/VeriSign	Cornodo	GeoTrust	Thawte/VeriSign	
	Produkt	PositiveSSL	FreeSSL/ RapidSSL	<u>SSL123</u>	InstantSSL/ PremiumSSL	True BusinessID	SSL Web Server	
	Root-Zertifikat	AddTrust External CA Root	Equifax Secure CA	Thawte Premium Server CA	AddTrust External CA Root	Equifax Secure CA	Thawte Premium Server CA	
	Validierung	E-Mail-Robot	E-Mail-Robot	E-Mail-Robot	Dokumente, E-Mail-Robot und Rückruf	Dokumente und Rückruf	Dokumente und Rückruf	
	Ausstellung in (Richtwert)	10 Minuten_	10 Minuten ¹	30 Minuten <mark>1</mark>	10 Minuten_	2-3 Werktagen_	2-3 Werktagen ¹	
	Kostenloser Austausch ²	ja	bei uns inklusive	ja	ja	ja	ja	
Entwickler	Zusätzliche physikalische Maschinen	bei uns ohne Aufpreis	ohne Aufpreis	gleich dem Zertifikatspreis	bei uns ohne Aufpreis	ohne Aufpreis	gleich dem Zertifikatspreis	Seite 110
	Empfohlen für	Adminnanels	Intranetsites	Mobilsites	kleine Shons	mittlere Shons	große Shons	

SSL-ZERTIFIKATE & TRUSTLOGOS

TRUST IT

> 2. Schritt: Bereitstellung Ihrer Zertifizierungsanforderung (CSR)

Zunächst erstellen Sie eine Zertifizierungsanforderung (CSR) mit Ihrer Serversoftware. Entsprechende Anleitungen für die gängigsten Server finden Sie auf unserer englischsprachigen Partnersite. Sobald Sie Ihr CSR erstellt haben, können Sie mit der Bestellung fortfahren.

Bei der Wahl Ihres Allgemeinen Namens (CN) haben Sie die folgenden Möglichkeiten:

Ihr voller Domainname (FQDN), z.B. www.domain.de, schützt https://www.domain.de/...

Bitte achten Sie darauf, dass Ihr privater Schlüssel mindestens 2048 bit und maximal 4096 bit lang sein darf.

Nachdem Sie das CSR mit Ihrer Serversoftware erstellt haben, kopieren Sie dessen Inhalt mit Hilfe eines Texteditors in das folgende Textfeld. Ihr CSR sollte dabei ungefähr so aussehen:

----BEGIN CERTIFICATE REQUEST----MIIDUDCCArkCAQAwdTEWMBQGAlUEAxMNdGVzdC50ZXNOLmNvbTESMBAGAlUECxMJ TWFya2VOaW5nMREwDwYDVQQKEwhUZXNOIE9yZzESMBAGAlUEBxMJVGVzdCBDaXR5

Rq+blLr5X5iQdzyFlpLqPlMck5VeleCzOR9/OekGSRno7ow4TVyxAF6J6ozDaw7e GisfZw40VLT0/6IGvK2jX0i+t58RFQ8WYT0cTRlPnkG8B/uV -----END CERTIFICATE REQUEST-----

Bei Verlängerung eines domainvalidierten Zertifikates unter IIS beachten Sie unbedingt unsere Hinweise.

Probleme mit Ihrer Zertifizierungsanforderung? Prüfen Sie Ihr CSR hier.

Zertifizierungsanforderung:

. . .

EntwicklerCamp 2

Verwendete Serversoftware:



× *

Lotus Domino

*

SSL-ZERTIFIKATE & TRUSTLOGOS

TRUST IT

Seite 112

2. Schritt: Bereitstellung Ihrer Zertifizierungsanforderung (CSR)

Zunächst erstellen Sie eine Zertifizierungsanforderung (CSR) mit Ihrer Serversoftware. Entsprechende Anleitungen für die gängigsten Server finden Sie auf unserer englischsprachigen Partnersite. Sobald Sie Ihr CSR erstellt haben, können Sie mit der Bestellung fortfahren.

Bei der Wahl Ihres Allgemeinen Namens (CN) haben Sie die folgenden Möglichkeiten:

Ihr voller Domainname (FQDN), z.B. www.domain.de, schützt https://www.domain.de/...

Bitte achten Sie darauf, dass Ihr privater Schlüssel mindestens 2048 bit und maximal 4096 bit lang sein darf.

Nachdem Sie das CSR mit Ihrer Serversoftware erstellt haben, kopieren Sie dessen Inhalt mit Hilfe eines Texteditors in das folgende Textfeld. Ihr CSR sollte dabei ungefähr so aussehen:

----BEGIN CERTIFICATE REQUEST----

MIIDUDCCArkCAQAwdTEWMBQGA1UEAxMNdGVzdC50ZXN0LmNvbTESMBAGA1UECxMJ TWFya2V0aW5nMREwDwYDVQQKEwhUZXN0IE9yZzESMBAGA1UEBxMJVGVzdCBDaXR5

Rq+blLr5X5iQdzyF1pLqP1Mck5Ve1eCz0R9/OekGSRno7ow4TVyxAF6J6ozDaw7e GisfZw40VLT0/6IGvK2jX0i+t58RFQ8WYTOcTR1PnkG8B/uV -----END CERTIFICATE REQUEST----

Bei Verlängerung eines domainvalidierten Zertifikates unter IIS beachten Sie unbedingt unsere Hinweise.

Probleme mit Ihrer Zertifizierungsanforderung? Prüfen Sie Ihr CSR hier.

Zertifizierungs- anforderung:	Hier einfügen	
Verwendete Serversoftware:	Lotus Domino	:
EntwicklerCam	p 2015 - Jürgen Kunert - ITEE Seite 113	

- Je nach Sicherheitsstufe des Zertifikats muss der Käufer seine Validität nachweisen (vom Firmenstempel bis zum Handelsregisterauszug)
- Ggf. Zeit einplanen und vorher den Support fragen

Wir haben entweder

- eine Datei mit einem Zertifikat (server.pem)
- oder
- das Zertifikat in der Zwischenablage

Wir machen daraus in jedem Fall eine Datei (server.pem)

Zertifikat (server.pem) ansehen C:\OpenSSL-Win64\bin>type server.pem -----BEGIN CERTIFICATE-----MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFA DCBnDELMAkGA1UEBhMC

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k= ----END CERTIFICATE-----

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Zertifikate (server.key und server.pem) zusammenfügen (server.txt)

C:\OpenSSL-Win64\bin>COPY C:\OpenSSL-Win64\bin\server.key+C:\OpenSSL-Win64\bin\server.pem server.txt

C:\OpenSSL-Win64\bin\server.key

C:\OpenSSL-Win64\bin\server.pem

Ggf. auch noch Zwischenzertifikate (Intermediate) einfügen

Zwischenergebnis ansehen: C:\OpenSSL-Win64\bin>type server.txt -----BEGIN RSA PRIVATE KEY-----MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6 ... 1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k=

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQ1/COSs2kB6XFP2vj8ZrBsh+1XQVKX2k= -----END RSA PRIVATE KEY---------BEGIN CERTIFICATE-----MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC

ZzzPMQuMHhpQuHfvlu3chwcKWrw+aUBng+oQLf6kvDoPP/ZqcNyLX7hq+CFW9xmn 0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k= -----END CERTIFICATE-----

C:\OpenSSL-Win64\bin>dir server.* Volume in Laufwerk C: hat keine Bezeichnung. Volumeseriennummer: A0FB-9BD7

Verzeichnis von C:\OpenSSL-Win64\bin 08.01.2015 18:59 1.801 server.csr 08.01.2015 18:51 3.243 server.key 08.01.2015 19:01 2.041 server.pem 08.01.2015 20:31 5.285 server.txt 4 Datei(en), 12.370 Bytes 0 Verzeichnis(se), 4.394.057.728 Bytes frei EntwicklerCamp 2015 - Jürgen Kunert - ITEE

server.txt verifizieren:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" verify "C:\OpenSSL-Win64\bin\server.txt"

KyrTool v1.0

Successfully read 4096 bit RSA private key INFO: Successfully read 1 certificates INFO: Private key matches leaf certificate INFO: Final certificate in chain is self-signed

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Zertifikat in den Schlüsselring importieren: C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" import all -k c:\lotus\notes\data\keyring.kyr -i "C:\OpenSSL-Wi n64\bin\server.txt"

Using keyring path 'c:\lotus\notes\data\keyring.kyr' Successfully read 4096 bit RSA private key SECIssUpdateKeyringPrivateKey succeeded SECIssUpdateKeyringLeafCert succeeded

Schlüssel anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" **show keys -k** c:\lotus\notes\data\keyring.kyr

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Key length: 4096 bits

-----BEGIN PUBLIC KEY-----MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwxx5LDjqs4s4jBGNncEr

u9GAIJwEWeEfdSXN8/JcuUkCAwEAAQ==
-----END PUBLIC KEY-----

Key length: 4096 bits

-----BEGIN RSA PRIVATE KEY-----MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k= -----END RSA PRIVATE KEY-----

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Zertifikate anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" show certs -k c:\lotus\notes\data\keyring.kyr Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Certificate #0

Subject:

EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=D E

Issuer:

EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=D E

Not Before: 08.01.2015 19:01:41 Not After: 05.01.2025 19:01:41 Key length: 4096 bits Signature Alg: sha256WithRSAEncryption

-----BEGIN CERTIFICATE-----

MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k= -----END CERTIFICATE-----

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Jetzt haben wir einen Schlüsselring

🖬 traveler13.sth	1 KB	STH-Datei	08.03.2013 20:02
🖬 traveler13.kyr	31 KB	KYR-Datei	08.03.2013 20:02

 mit vom Browser bzw. vom Smartphone akzeptierten Zertifikaten.

Zertifikate auf den Server kopieren: Domino/Data:

	29 KB
keyring.sth 08.01.2015 19:12 STH-Datei	1 KB

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

- 1. Domino auf 9.0.1 updaten
- 2. Dazu entweder
 - 1. 9.0.1 Fix Pack 2 Interim Fix 3

oder

1. 9.0.1 Fix Pack 3

- Die beiden Dateien xxx.kyr und xxx.sth ins Data-Verzeichnis des Servers kopieren
- Serverdokument: Ports/Internet-Ports
 SSL-Schlüsseldatei eintragen

Server: ITEENS01/I	TEE/De kunertnts2.IT
Allgemein Sicherheit Ports	Server-Tasks Internetprotokol
Notes-Netzwerkports Internet-P	'orts Proxies
SSL-Einstellungen	
Name der SSL-Schlüsseldatei:	ITEE2011keyfile.kyr 🗧 🗲
SSL-Protokollversion (für alle Protokolle außer HTTP):	Vereinbart

4. Serverdokument: Ports/Internet-Ports

Web Verzeichnis Mail DIIOP Remote-Debug-Manager

Web (HTTP/HTTPS)	
TCP/IP-Portnummer:	⁶ 80 J
TCP/IP-Portstatus:	^ℤ Umleiten an SSL 』 💌
Einstellungen zum Serverzugriff erzwingen:	^r Ja▼
Optionen für Authentifizierung:	
Name und Kennwort:	[┎] Ja」▼
Anonym:	『Nein』
SSL-Portnummer:	^C 443 J
SSL-Portstatus:	^C Aktiviert ⊒ ▼
Optionen für Authentifizierung:	
Client-Zertifikat:	🕫 Nein 🗉 💌
Name und Kennwort:	^r Jaı▼
Anonym:	^C Nein J 💌

5. Alternative: über Internet-Site-Dokumente

6.SSL-Verschlüselungscodes = Cipher Suites

- im Serverdokument konfigurierbar:
 - Reiter Ports/Internet-Ports
 - aber dort nur f
 ür HTTPS
- für alle Ports in der notes.ini überschreibt die Einstellungen im Serverdok!
- SSLCipherSpec=2F35050A
 - 2F = SSL_RSA_WITH_AES_128_CBC_SHA
 - 35 = SSL_RSA_WITH_AES_256_CBC_SHA
 - 05 = SSL_RSA_WITH_RC4_128_SHA

- 0A = SSL_RSA_WITH_3DES_EDE_CBC_SHA EntwicklerCamp 2015 - Jürgen Kunert - ITEE

- 7. Wahlweise ACHTUNG:
 - Ggf. benötigen wir SSL 3 noch
 SSL 3 deaktivieren per notes.ini
 - DISABLE_SSLV3=1
- 8. HTTP Task neu starten
- 9. Testen, Zertifikat validieren

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

<u>D</u> atei	<u>B</u> earbeiten	Ansicht	<u>C</u> hronik	<u>L</u> esezeichen	E <u>x</u> tras	<u>H</u> ilfe	
9	LOG IN Hy	poVereins	bank 🗙	+			



0

Sie sind verbunden mit hypovereinsbank.de Diese Website wird betrieben von UniCredit Bank AG

UniCredit Bank AG (DE) https://my.hypovereinsbank.de/

München Bayern, DE

Verifiziert von: VeriSign, Inc.

Die Verbindung zu dieser Website ist sicher.

Weitere Informationen...

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Allgemein Medien Berechtigungen Sicherheit		
Aligemein Medien berechtigungen Sichemeit		
Vebsite-Identität		
Website: my.hypovereinsbank.de		
Besitzer: UniCredit Bank AG		
Validiert von: VeriSign, Inc.		
		Zertifikat anzeigen
)atenschutz & Chronik		
Habe ich diese Website früher schon einmal besucht?	Nein	
Speichert diese Website Daten (Cookies) auf meinem Computer?	Nein	Coo <u>k</u> ies anzeigen
Habe ich Passwörter für diese Website gespeichert?	Nein	Gespeicherte Passwörter anzeigen
fachaire ha Dataile		
	256_CBC_SHA, 256-Bi	t-Schlüssel, TLS 1.2)
Verbindung verschlüsselt (TLS_ECDHE_RSA_WITH_AES_2	an dae Internet Oberma	it alt unused a
Verbindung verschlüsselt (TLS_ECDHE_RSA_WITH_AES_2 Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie üb	er das Internet überm	ittelt wurde.

Zertifikat-Ansicht:"my.hypovereinsbank.de"

Allgemein Det ils

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

SSL-Server-Zertifikat

Ausgestellt für

Allgemeiner Name (CN)	my.hypovereinsbank.de
Organisation (O)	UniCredit Bank AG
Organisationseinheit (OU)	XL78458
Seriennummer	63:06:AA:0F:04:74:2F:8F:77:6C:0F:CB:20:C9:07:26

Ausgestellt von

Allgemeiner Name (CN) VeriSign Class 3 Extended Validation SSL SGC CA Organisation (O) VeriSign, Inc.

Organisationseinheit (OU) VeriSign Trust Network

Gültigkeitsdauer

Beginnt mit	11.04.2014
Läuft ab am	11.12.2015

Fingerabdrücke

6HA-256-Fingerabdruck	4E:82:C6:3D:EA:43:82:93:AA:43:7E:C3:B6:93:10:FB 71:55:FA:BB:5E:92:A2:D5:E5:8D:5B:62:39:74:1E:95
HA1-Fingerabdruck	76:DB:E6:78:04:79:BB:37:B9:12:DD:4C:B8:3D:56:28:61:BB:9F:66

EntwicklerCamp 2

Seite 133

x

:

SSLyze v0.10

C:\>G:\SSLyze\sslyze\sslyze.exe --regular www.beispiel.de

TLSV1 1 Cipher Suites: Server rejected all cipher suites. **TLSV1 Cipher Suites:** Preferred: DH-1024 bits 256 bits DHE-RSA-AES256-SHA HTTP 200 OK Accepted: DH-1024 bits 256 bits DHE-RSA-AES256-SHA HTTP 200 OK HTTP 200 OK AES256-SHA 256 bits DHE-RSA-AES128-SHA DH-1024 bits 128 bits HTTP 200 OK HTTP 200 OK RC4-SHA 128 bits RC4-MD5 HTTP 200 OK 128 bits AES128-SHA 128 bits HTTP 200 OK EDH-RSA-DES-CBC3-SHA DH-1024 bits 112 bits HTTP 200 OK **DES-CBC3-SHA** 112 bits HTTP 200 OK EDH-RSA-DES-CBC-SHA DH-1024 bits 56 bits HTTP 200 OK **DES-CBC-SHA** 56 bits HTTP 200 OK HTTP 200 OK EXP-EDH-RSA-DES-CBC-SHA DH-512 bits 40 bits EXP-RC4-MD5 HTTP 200 OK 40 bits HTTP 200 OK EXP-RC2-CBC-MD5 40 bits EXP-DES-CBC-SHA 40 bits HTTP 200 OK

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

 Webdienst: https://www.ssllabs.com/ssltest/

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Datenbankschablonen mit Bezug zur Verschlüsselung

- pubnames.ntf Domino Verzeichnis Speicher für öffentliche Schlüssel und Zertifikate
- pernames.ntf persönliches Adressbuch
 Speicher f
 ür öffentliche Schl
 üssel und Zertifikate
- csrv50.ntf Server Certificate Administration Editor für Schlüsselringe
- cca50.ntf Domino Certificate Authority Internes Trustcenter
- certlog.ntf Certification Log
 Logging der internen Domino-Registrierungen
- certpub.ntf Domino Certificate Publication Requests
 This database is used for requesting publication of client SSL certificates into the NAB.

Verschlüsselungstools

 Die besten kostenlosen
 Verschlüsselungstools (für den privaten Einsatz)

http://www.pcwelt.de/ratgeber/Datenschutz -Gratis-Tools-verschluesseln-alle-Ihre-Dateien-307316.html

Literatur/Quellen

- http://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung#S.2FMIME-basierte_E-Mail-Verschl.C3.BCsselung_und_-Signatur_im_Detail
- http://en.wikipedia.org/wiki/S/MIME
- und mehr Wikipedia
- zwei Artikel in der c't 18/2012
- http://www.computerwoche.de/security/2510521/#
- "Crispy Certificates with Spicy SSL Salsa" http://www.slideshare.net/WorkFlowStudios/lotusphere-2011-show104
- Alternativen zur eMail-Verschlüsselung mit Bordmitteln: Alexander Rubinstein (www.symplasson.de)

Literatur/Quellen 2

PFS: http://www.heise.de/security/artikel/Zukunftssicher-Verschluesseln-mit-Perfect-Forward-Secrecy-1923800.html

- <u>http://www.nashcom.de/nsh/web.nsf/ff5ce882e73ab026c</u> 1256942003bdf10/6084a81e9f2c2b00c1256cc30030c6c <u>1/\$FILE/BP102_final.pdf</u>
- <u>https://www.heise.de/artikel-archiv/ct/2015/06/160_Die-Schluessel-Falle</u>
- <u>http://blog.darrenduke.net/Darren/DDBZ.nsf/dx/domino-and-ssl-ciphers.-the-server-document-may-not-be-doing-what-we-expect-it-to-do.htm</u>
- http://www.golem.de/news/tls-verschluesselung-poodlekann-auch-tls-betreffen-1412-111037.html

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Vielen Dank für Ihre Aufmerksamkeit!

EntwicklerCamp 2015 - Jürgen Kunert - ITEE

Jürgen Kunert ITEE **InformationsTechnologie Effizient Einsetzen** Sandkrugweg 57a 22457 Hamburg Juergen.Kunert@itee.de