

Verschlüsselung von Dateien

mittels

SecCommerce SecSigner und Gpg4win

Stand 03.02.2014

Landesbetrieb Daten und Information Valenciaplatz 6 55118 Mainz



LDI Team A1-eGovernment



Inhaltsverzeichnis

1. Ein	nleitung	
2. Ve	rschlüsselung mittels SecSigner	
2.1.	Installation und Konfiguration	
2.2.	Herunterladen des Verschlüsselungszertifikats der virtuellen Poststelle	
2.3.	Verschlüsselung einer Datei	9
3. Ve	rschlüsselung mittels Gpg4win	
3.1.	Installation und Konfiguration	
3.2.	Import der Verschlüsselungszertifikate	
3.3.	Verschlüsseln einer Datei	
Abbild	ungsverzeichnis	
	-	



1. Einleitung

Die virtuelle Poststelle des Landes Rheinland-Pfalz ist in der Lage, S/MIME-verschlüsselte E-Mail-Nachrichten zu entschlüsseln. Dazu muss der Absender in der Regel ein eigenes X.509 E-Mail-Zertifikat, sowie ein spezifisches X.509 E-Mail-Zertifikat für das zu adressierende virtuelle Postfach in seiner E-Mail-Software hinterlegen. Zurzeit existieren nur für wenige virtuelle Postfächer spezifische E-Mail-Zertifikate, in diesen Fällen bieten die entsprechenden Behörden das Zertifikat direkt auf ihren Internetseiten zum Download an. Mittels der S/MIME-Verschlüsselung wird die komplette Nachricht verschlüsselt, mit Ausnahme von Absender, Empfänger und Betreff.

Für alle virtuellen Postfächer besteht darüber hinaus die Möglichkeit, zumindest Dateianhänge sicher zu verschlüsseln. Bitte beachten Sie hierzu, dass im E-Mail-Text dann keine datenschutzrelevanten Informationen übermittelt werden sollten.

Zur Verschlüsselung von Nachrichtenanhängen, können beliebige Softwareprodukte zum Einsatz kommen, die eine Verschlüsselung mittels 3-DES durchführen.

Unter Windows getestet und exemplarisch im Folgenden dargestellt wird die Nutzung der kostenlosen Software SecCommerce SecSigner ab Version 3.5.0 und Gpg4win ab der Version 2.2.1.

SecSigner kann sowohl zur qualifizierten elektronischen Signatur von Dateien als auch zur Verschlüsselung von Dateien verwendet werden. Gpg4win unterstützt PGP/GPG-Verschlüsselung und Signatur sowie die in diesem Fall benötigte Verschlüsselung mittels S/MIME.

In diesem Dokument wird ausschließlich die Verschlüsselung von Nachrichtenanhängen mit dem Algorithmus Triple-DES (3DES) behandelt.

Das Zertifikat zur Dateiverschlüsselung ist bis zum 04.02.2017 gültig. Anfang 2017 werden wir unter <u>http://www.rlp-service.de/RLPGateway/FVP/FV/middleware/DownloadFiles/RLP-Intermediaer.zip</u> ein neues Zertifikat zur Verfügung stellen.

2. Verschlüsselung mittels SecSigner

2.1. Installation und Konfiguration

Die Software SecSigner ist über die Seite des Hersteller zu beziehen: <u>https://www.seccommerce.de/de/products/secsigner/download.html</u> Bzw. Direktlink: <u>https://www.seccommerce.de/de/public-downloads/file/1-windows-setup.html</u>

Die Installationsdatei muss heruntergeladen (ca. 4,7 MB) und installiert werden:



löchten	Sie diese D	atei speicherr	n oder ausführe	en?
-	Name:	Setup-3-5-0.exe		
	Тур: -	Anwendung, 4,7	2 MB	
	Von:	www.seccomm	nerce.de	
		A <mark>u</mark> sführen	<u>S</u> peichern	Abbrechen
A P	ateien aus de	m Internet könne	n nuitzlich sein, a	ber dieser Dateityp

Abbildung 1: Speichern des Setup-Programms

Speichern Sie die Installationsdatei bitte zunächst auf Ihrem Rechner.

)atei öffi	nen - Sicherheitswarnung	×
Möcht	en Sie diese Datei ausführen?	
	Name: <u>Setup-3-5-0.exe</u>	
	Herausgeber: SecCommerce Informationssysteme GmbH	
	Typ: Anwendung	
	Von: C:\Dokumente und Einstellungen\Administrator\De	
▼ Vor	dem Öffnen dieser Datei immer bestätigen	
	Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Führen Sie	
~	Risiko besteht?	

Abbildung 2: Ausführen des Setup-Programms

Starten Sie nun das soeben heruntergeladene Setup-Programm durch Doppelklick auf die Datei "Setup-3-5-0.exe". Eine etwaige Sicherheitswarnung bestätigen Sie bitte mit "Ausführen".



SecCommerce SecSigner 3	.5.0		×
	SecCommerc	e SecSigner 3.5.0	
	Ersteller: Website: Email-Adresse:	SecCommerce Informationssysteme GmbH http://www.seccommerce.de info@seccommerce.de	
	Tarma Installer w Computer installi	vird SecCommerce SecSigner auf Ihrem eren oder aktualisieren.	
	Klicken Sie auf W	eiter, um fortzufahren.	
	Copyright (c) 2	2005 - 2010 SecCommerce	
	Diese Anwendun internationale Ve Reproduktion ode oder einer ihrer k	g ist durch das Urheberrechtsgesetz und rträge geschützt. Eine unberechtigte er Weitergabe an Dritte dieser Anwendung Komponenten verstößt gegen geltendes Rech	t.
Info		< Zurück Weiter > Abbrechen	

Abbildung 3: Startbildschirm des Setup-Programms

Nun erscheint der Startbildschirm des Setup-Programms. Mit "Weiter" gelangen Sie zur nächsten Seite.

SecCommerce SecSigner 3.5.0		
izenzvertrag	E SecCommerce	
Bitte lesen Sie den Lizenzvertrag sorafältig	bevor Sie fortfahren	
Dire lesen die den Lizenzverrag sorgrang.	, bevol bie lokaliten.	
engegenzunenmen.		
5. Geistiges Eigentum / Urheberrechte von	n SecCommerce	
Die Software ist sowohl durch Deutsche II.	Irbeherrechtsgesetze und	
Verträge, als auch internationale Verträge u	und Gesetze als geistiges	
Eigentum der SecCommerce Informationss	ysteme GmbH geschützt. SecSigner	
ist ein eingetragenes Warenzeichen der Se	ecCommerce Informationssysteme GmbH.	
Alle Rechte liegen bei:		
SecCommerce Informationssysteme GmbH	I	
Obenhauptstr. 5		
22335 Hamburg		
info@seccommerce.de		
Tel. 040-53052-0		
Eav. 040-53052-100		
Tel. 040-53052-0 Fay: 040-53052-100		
1 dn. 040 00002 100		Ŧ
		•
ma® Installer		Ξ

Abbildung 4: Bestätigung der Lizenzbedingungen



Prüfen und bestätigen Sie nun bitte den Lizenzvertrag durch Setzen des Häkchens bei "Ich stimme den Bedingungen zu.". Klicken Sie anschließend bitte auf "Weiter".

 SecCommerce SecSigner Plug-in für Adobe Acrobat Reader 1 Plug-in für Adobe Acrobat 10 Plug-in für Adobe Acrobat Reader 5 Plug-in für Adobe Acrobat 9 CSP für Windows-Anwendungen 	Dies installiert SecCommerce SecSigner.
· ☑ Makro für Microsoft Office	Komponentengröße: 5.647KE Installationsgröße: 6.395KE Deinstallationsgröße: 0KE
d	Freier Speicherplatz: 102.848KE

Abbildung 5: Einstellung der Installationsoptionen

Die Installationsoptionen können Sie unverändert lassen. Benötigt werden in jedem Fall: SecCommerce SecSigner und CSP für Windows-Anwendungen. Der Installationsordner kann bei Bedarf geändert werden. Durch Klick auf "Installieren" wird die Software installiert.



SecCommerce SecSigner 3	.5.0
<u>-e</u> seccommerce secsigner 3	Installation abgeschlossen SecCommerce SecSigner wurde erfolgreich auf Ihrem Computer installiert.
	Klicken Sie auf Beenden, um Tarma Installer zu schließen.

Abbildung 6: Abschluss des Setup-Programms

Das Abschlussfenster des Setup-Programms schließen Sie bitte durch Klick auf "Beenden".

🚞 C:\Programme\SecCommerce\	SecCom	merce SecSigner			
Datei Bearbeiten Ansicht Favo	riten E:	xtras ?			
🔇 Zurück 👻 🕥 🖌 🏂 🔎	Suchen	😥 Ordner 🛛 🔢 🗸			
Adresse 🛅 C:\Programme\SecComme	erce\SecC	ommerce SecSigner			
1		Name	Größe	Тур	Geändert am 💌
Datei- und Ordneraufgaben	¥	secsigner.properties	5 KB	PROPERTIES-Datei	05.04.2011 16:54
3		Esecsigner_res.pkcs7	4 KB	PKCS7-Datei	05.04.2011 16:21
Andere Orte	×	SecSignerRes99886F18A5E1A2A55624A986A7820A704C96CE7A0719FA23FDF	776 KB	Executable Jar File	05.04.2011 16:21
		SecSigner.jar	1.634 KB	Executable Jar File	05.04.2011 16:21
Detaile	×	🔊 SecSignerExt.jar	412 KB	Executable Jar File	05.04.2011 16:18
Decails	×	E SecSigner.exe	63 KB	Anwendung	05.04.2011 16:06
		S CallSecSignerDLL.dll	95 KB	Programmbibliothek	05.04.2011 16:06
		🔊 secwintools.dll	68 KB	Programmbibliothek	05.04.2011 15:31
		🔊 scdriver.jar	201 KB	Executable Jar File	05.04.2011 15:31
		SecSignerShellExt.dll	156 KB	Programmbibliothek	05.04.2011 15:05
		SecCryptoSP.dll	96 KB	Programmbibliothek	05.04.2011 15:04
		SecSignerShellExt.dllrb	156 KB	_RB-Datei	24.11.2009 19:31
		SecComCSP.dll	64 KB	Programmbibliothek	05.01.2009 18:36
		S msvcr71.dl	340 KB	Programmbibliothek	07.03.2007 18:35
		🛅 doc		Dateiordner	13.04.2011 11:45

Abbildung 7: Öffnen der Konfigurationsdatei "secsigner.properties"

Im Nachgang ist noch eine Konfigurationsänderung erforderlich, um die Software mit der virtuellen Poststelle des Landes Rheinland-Pfalz verwenden zu können. Wechseln Sie dazu bitte in das Installationsverzeichnis der Anwendung (Standardmäßig: "C:\Programme\SecCommerce\SecCommerce\SecSigner").



Öffnen Sie dort bitte die Datei secsigner.properties (z.B. mit Wordpad) und fügen Sie am Ende der Datei bitte folgende Zeile (ohne Anführungszeichen) ein: "seccommerce.secsigner.encryption.cipherid=0"



Abbildung 8: Ergänzung der Datei secsigner.properties

Nachdem Sie die Zeile ergänzt haben speichern Sie bitte Änderungen.

2.2. Herunterladen des Verschlüsselungszertifikats der virtuellen Poststelle

Um eine Datei mit dem Verschlüsselungszertifikat der virtuellen Poststelle des Landes Rheinland-Pfalz zu verschlüsseln, benötigen Sie den öffentlichen Schlüssel der virtuellen Poststelle.

Der öffentliche Schlüssel der VPS ist auf der Website <u>www.rlp-Service.de</u> zu finden (<u>http://www.rlp-service.de/RLPGateway/FVP/FV/middleware/DownloadFiles/RLP-</u><u>Intermediaer.zip</u>) bitte speichern Sie die ZIP-Datei in einem beliebigen Ordner auf Ihrem PC und entpacken Sie sie anschließend.

Ihnen liegt nun eine Datei mit der Bezeichnung "RLP-VPS-base64.cer" vor.



2.3. Verschlüsselung einer Datei



Abbildung 9: Zu verschlüsselnde Datei auswählen

Nach der Installation von SecSigner finden Sie bei Verwendung der rechten Maustaste auf die zu verschlüsselnde Datei einen Menupunkt "SecSigner", der wiederum als untersten Menupunkt "Daten nur verschlüsseln" anbietet.



rschlüsselungszertifikat laden	×
Verschlüsselungszertifikat laden	
Laden Sie das Verschlüsselungszertifikat des Empfängers aus dem Dateisystem.	-

Abbildung 10: Bestätigungsfenster zur Auswahl des Verschlüsselungszertifikats

Das nun folgende Bestätigungsfenster können Sie durch einfachen Klick auf "OK" bestätigen.

🛓 Datei ausw	rählen
Suchen in:	RLP-Intermediaer
RLP-Inte	ermediaer.cer
Dateiname:	instellungen\Administrator\Desktop\RLP-Intermediaer\RLP-Intermediae
- Da <u>t</u> eityp:	Alle Dateien
Dařenàh:	
	Offnen Abbrechen

Abbildung 11: Auswahl des Verschlüsselungszertifikats

Nach der Auswahl "Daten nur verschlüsseln" haben Sie noch den Speicherort des öffentlichen Schlüssels der virtuellen Poststelle auf Ihrem PC anzugeben. Achten Sie darauf bei Dateityp LDI Team A1-eGovernment Seite 10



"Alle Dateien" auszuwählen. Navigieren Sie zu der im Vorfeld heruntergeladenen Datei "RLP-VPS-base64.cer", wählen Sie diese aus und klicken Sie anschließend auf "Öffnen".

goperenem				
Spe <u>i</u> chern ir	n: 📑 Desktop			
rg Writer.Inl	ĸ	🗋 Softerra LDA	P Browser 2.6.Ink	
e <mark>r</mark> 3.0.lnk		🗋 Test.doc		
r3Readme.htm		🗋 test.txt		
diaer.zip		🗋 Test1.doc		
t				
k				
•			Ш	
∢ [Datei <u>n</u> ame:	Test.doc.pkcs7		W)
∢ Datei <u>n</u> ame: Dateityp:	Test.doc.pkcs7		II	
↓ Datei <u>n</u> ame: Da <u>t</u> eityp:	Test.doc.pkcs7			

Abbildung 12: Speichern der verschlüsselten Datei

Sie erhalten nun die Möglichkeit auszuwählen, wo die neue verschlüsselte Datei gespeichert werden soll. Standardmäßig wird der ursprüngliche Dateiname um die Endung ".pkcs7" ergänzt, dies sollten Sie beibehalten. Ihre Ursprungsdatei wird dann nicht verändert.

Die verschlüsselte Datei mit der Endung ".pkcs7" können Sie nun an eine E-Mail anhängen, die Sie an eine virtuelle Postfachadresse des Landes Rheinland-Pfalz senden möchten.



3. Verschlüsselung mittels Gpg4win

3.1. Installation und Konfiguration

Gpg4win (*GNU Privacy Guard for Windows*) ist ein Installationspaket für <u>Windows</u> und kann kostenfrei aus dem Internet (<u>http://www.gpg4win.de/</u>) heruntergeladen werden.

Bitte beachten Sie, dass die aktuelle Version der virtuellen Poststelle Nachrichten mit angehängten PGP/GPG-Zertifikaten nicht verarbeiten kann. D.h. Nachrichtenanhänge für die virtuelle Poststelle können wie unten beschrieben verschlüsselt werden, die Nutzung der übrigen durch Gpg4win bereitgestellten Funktionen wird in diesem Kontext noch nicht unterstützt.

Nach dem Download von Gpg4win wird die Installation durch Doppelklick auf die Datei gpg4winX.X.exe (X.X= die jeweils aktuelle Versionsnummer) und Klick auf den Button "Ausführen" gestartet:

Datei öffn	en - Sicherhe	itswarnung			X
Möchte	en Sie diese l)atei ausführen?			
	Name: Herausgeber:	gpg4win-2.2.1.exe Intevation GmbH			
	Тур: Von:	Anwendung 10.68.120.33			
			<u>A</u> usführen	Abbrechen	
١	Dateien aus d kann eventue nur Software v <u>Risiko besteht</u>	em Internet können n I auf dem Computer S ron Herausgebern au <u>?</u>	ützlich sein, a ichaden anric s, denen Sie v	ber dieser Dateity hten. Führen Sie vertrauen. <u>Welch</u>	/p <u>es</u>

Abbildung 13: Installation 1

Während der Installation kann man die gewünschte Sprache auswählen:



Abbildung 14: Installation 2

LDI Team A1-eGovernment



Es erscheint der Begüßungsbildschirm:

Gpg4win Installation GPGWin Willkommen bei der Installation von Gpg4win Gpg4win ist ein Installationspaket für Windows zur Nutzung von E-Mail- und Datei-Verschlüsselung unter Verwendung der Kernkomponente GnuPG für Windows. Die beiden relevanten kryptographischen Standards OpenPGP und S/MIME werden unterstützt. Gpg4win und die in Gpg4win enthaltene Software sind Freie Software. Klicken Sie auf Weiter, um fortzufahren. Dies ist Gpg4win Version 2.2.1 Dateiversion 2.2.1.16059 Belaesedebum 2000 100.27	
	Willkommen bei der Installation von Gpg4win
\cap	Gpg4win ist ein Installationspaket für Windows zur Nutzung von E-Mail- und Datei-Verschlüsselung unter Verwendung der Kernkomponente GnuPG für Windows. Die beiden relevanten kryptographischen Standards OpenPGP und S/MIME werden unterstützt. Gpg4win und die in Gpg4win enthaltene Software sind Freie Software.
	Klicken Sie auf Weiter, um fortzufahren.
GPG	Dies ist Gpg4win Version 2.2.1 Dateiversion 2.2.1.16059 Releasedatum 2013-10-07
	Weiter > Abbrechen

Abbildung 15: Installation 3

Im Folgenden werden die Lizenzinformationen angezeigt:

Gpg4win Installation		_ 🗆 🗙
	Lizenzabkommen Diese Software ist unter der GNU General Publ lizensiert.	ic License (GPL)
Drücken Sie die Bild-nach-u	unten Taste, um den Rest des Abkommens zu sehe	en.
Spg4win consist of several different license condition under the GNU General Pu are free to use without re may be distributed. If the distributed along with the pointed out, distribution is What follows are the term copyright and license noti	al independent developed packages, available und s. Most of these packages however are available ublic License (GNU GPL). Common to all is that the strictions, may be modified and that modifications a source files (i.e. gpg4win-src-x.y.z.exe) are binaries and the use of the GNU GPL has been s in in all cases possible. Ins of the GNU GPL; for a list of individual ces please see the installed README file.	er 🔺
) In aller Kürze: Sie haben d die Software weitergeben, Sie erhalten haben.	as Recht, die Software zu jedem Zweck einzusetze , sofern Sie dem Empfänger dieselben Rechte einra	en. Sie können äumen, die auch
llsoft Install System v2.46-	7	

Abbildung 16: Installation 4



Die	Retätigung	der	Weiter_	Ruttons	führt zur	Kom	nonentenauswahl	1.
$\mathbf{D}\mathbf{R}$	Detailgung	uci	W CITCI-	Duttons	Iumi Lui	rom	ponontenauswan	ι.

	Komponenten auswählen Wählen Sie die Komponenten aus	, die Sie installieren möchten.
Wählen Sie die Komponente die Sie nicht installieren woll Wählen Sie die Komponente aus, die Sie installieren möchten:	n aus, die Sie installieren möchten u en. Klicken Sie auf Weiter, um fortz n IgnuPG Kleopatra	und wählen Sie diejenigen ab, ufahren. Beschreibung Bewegen Sie den Mauszeiger über eine Komponente, um ihre
Benötigter Speicher: 100.9N	G GpgOL ✓ GpgEX Claws-Mail ✓ Gpg4win-Kompendium	Beschreibung zu sehen.
llsoft Install System v2.46-7	ا	Weiter > Abbrecher

Abbildung 17: Installation 5

Hier kann die Standardvorbelegung übernommen werden. In jedem Fall aber muss Kleopatra (Ein Zertifikatsmanager für OpenPGP und X.509 (S/MIME)) mit ausgewählt sein. Ein Klick auf den Weiter-Button schließt die Komponentenauswahl ab.



Gpg4win Installation	×
	Zielverzeichnis auswählen Wählen Sie das Verzeichnis aus, in das Gpg4win installiert werden soll.
Gpg4win wird in das unter Verzeichnis installieren mö Verzeichnis aus. Klicken Si	n angegebene Verzeichnis installiert. Falls Sie in ein anderes ichten, klicken Sie auf Durchsuchen und wählen Sie ein anderes ie auf Weiter, um fortzufahren.
Zielverzeichnis C:\Programme\GNU\o	GnuPG
Benötigter Speicher: 100. Verfügbarer Speicher: 8.6	9MB GB
Nullsoft Install System v2,46	-7

Nun ist das Zielverzeichnis für die zu installierenden Komponenten festzulegen:

Abbildung 18: Installation 6

Im Bildschirm "Installationsoptionen" wird die gewünschte Verknüpfung hinterlegt:

😌 Gpg4win Installation		_ 🗆 🗙
Gre O	Installationsoptionen Startlinks	
Bitte wählen Sie, welche V	erknüpfungen angelegt werden sollen:	
Startmenü		
🔲 Arbeitsfläche		
C Schnellstartleiste		
(In der Schnellstartleiste v	verden nur Verknüpfungen für Programme angelegt.)	
Nullsoft Install System v2.46-	7	
	< <u>Z</u> urück <u>W</u> eiter > At	brechen

Abbildung 19: Installation 7

LDI Team A1-eGovernment



Schließlich wird der Startmenü-Ordner bestimmt:

Gpg4win Installation				
	Startmenü-Orc Bestimmen Sie Programmverkr	Iner bestimmen einen Startmenü-Oro nüpfungen.	Iner für die	
Wählen Sie den Startmer Ordner erstellen möchte	nü-Ordner für die Pro n, geben Sie dessen	ogrammverknüpfung Namen ein,	en aus. Falls Sie (einen neuen
Gpg4win				
7-210 Autostart E-Mail Converter Governikus Signer Microsoft Office				
Microsoft Silverlight Mozilla Firefox Mozilla Thunderbird Notepad++				
OpenSSL PC-WARE OSCI Add-In SecCommerce SecSigne	für Notare r			-
ullsoft Install System v2,4	5-7			
		< Zurück	Installieren	Abbrechen

Abbildung 20: Installation 8

Damit ist die Installation vollständig:

Gre D	Die Installation ist vollständig Die Installation wurde erfolgreich abgeschlossen.	
Fertig		
Details anzeigen		
Nullsoft Install System v2.46-j	7	
	< <u>Z</u> urück <u>Weiter ></u> Abb	rechen

Abbildung 21: Installation 9

LDI Team A1-eGovernment



Und abgeschlossen:	
Conduin Installation	

C Gpg4win Installation	
	Die Installation von Gpg4win wird abgeschlossen
GPG	Windows muss neu gestartet werden, um die Installation von Gpg4win zu vervollständigen. Möchten Sie Windows jetzt neu starten? © Jetzt neu starten © Windows später selbst neu starten
	< Zurück Eertig stellen Abbrechen

Abbildung 22: Installation 10

Im Folgenden ist die Einstellung von Kleopatra vorzunehmen bzw. zu kontrollieren. Dazu muss Kleopatra gestartet und in der Menüleiste die Auswahl "Einstellungen" und anschließend "Kleopatra einrichten" gewählt werden.

atei <u>A</u> nsicht <u>Z</u> ertifikate E <u>x</u> tras	Einstellungen Eenster Hilfe					
Zertifikate importieren 🛛 🕍 Ze	Selbsttest <u>d</u> urchführen	en	🔕 Vorgang a	abbrechen	Kate auf Ser	ver suchei
ichen:	Angezeigte Werkzeugleisten			Vertrauer	nswürdige Zertifikate	1
Yertrauenswürdige Zertifikate						
Name 🗸 E-Mail	🦄 Kurzbefehle festlegen		Details	9	ichlüssel-Kennung	
PCA-1-¥er	🖗 Werkzeugleisten einrichten		X.509	3FA4	9157	
	🔑 Kleopatra ein <u>r</u> ichten					
		22				

Abbildung 23: Kleopatra Einrichtung 1

Hier ist es wichtig, darauf zu achten, dass für Seite GnuPG-System auf der Registerkarte GPG for S/MIME in jedem Fall als Verschlüsselungsverfahren 3DES eingetragen ist.



Falls der Rechner, auf dem die Verschlüsselung durchgeführt wird, keinen Zugriff auf das Internet hat, ist es notfalls hier auch möglich, die Option "Niemals eine CRL konsultieren" auszuwählen. Das hat zur Folge, dass keine Prüfung auf zurückgezogene Zertifikate erfolgen kann.

1 R		
Zertifikatsserver	GPG for OpenPGP GPG Agent Smartcard Daemon GPG for S/MIME Directory Manager	
mar 2	Ontionen zur Einstellung der Diannoseausgaben	
Erscheinungsbild	Detaillierte Informationen	
0		
Kryptografie-	Optionen zur Einstellung der Konfiguration	
Aktionen	NAME als voreingestellten Schlüssel benutzen	-
	Auch an NAME verschlüsseln	- 3
S/MIME-Prüfung		
0	Benutze die Kodierung NAME für PKCS#12 Passphrasen	
Caulton Caulton	Schlüssel bei diesem Server nachschlagen Kein Server eingerichtet Bearbeiter	1
GnuPG-System	Nützliche Optionen zur Fehlersuche	
	Debug-Stufe festlegen auf 0 – Keine (Keinerlei Debug-Meldungen)	-
	Schreibe im Servermodus Logs auf DATEI	
	Optionen zur Einstellung der Sicherheit	_
	☐ Niemals <u>e</u> ine CRL konsultieren	
	☐ Die Gültigkeit <u>m</u> ittels OCSP prüfen	
	🖵 Zertifikatsrichtlinien nicht überprüfen	
	Fehlende Zertifikate automatisch holen	
	Verschlüsselungsverfahren NAME benutzen 3DES	

Abbildung 24: Kleopatra Einrichtung 2

3.2. Import der Verschlüsselungszertifikate

Um das Verschlüsselungszertifikat der virtuellen Poststelle inklusive Herausgeberzertifikat und Zwischenzertifikat zu importieren, wird zunächst Kleopatra gestartet:

Alle	e <u>P</u> rogramme 🔸	m Notepad++			Dokumentation	Þ
			💋 Ab <u>m</u> elden	600	Kleopatra Uninstall	
🤁 Start		9 9 1 0				

Abbildung 25: Kleopatra starten



Batei Ansicht Zertif	ikate Extras Ei	nstellungen Fenster	Hilfe				_ 🗆 ×
Zertifikate import	ieren 🔐 Zerti	fikate exportieren	C Aktualisieren	🛞 Vorgang a	bbrechen	🍂 Zertifikate auf Serve	er suchen
Suchen:					Vertrauer	nswürdige Zertifikate	•
Yertrauenswürdi	ge Zertifikate	Ande <u>r</u> e Zertifikate 丨					
Name 🗸	E-Mail	Gültig ab	Gültig bis	Details	9	ichlüssel-Kennung	
<u> </u>							
							-

Abbildung 26: Kleopatra Startbildschirm

Zur Auswahl der zu importierenden Zertifikate klickt man auf den Button "Zertifikate importieren":

Datei Ansicht	Zertifikate Extr	as Einstellungen Fer	nster Hilfe			_ 🗆 ×
Zertifikat	e importieren] Zertifikate exportierer	n 🛛 💽 Aktualisieren	🙆 Vorgang abbrechen	🍪 Zertifikate au	uf Server suchen
Suchen:	2ertifikatsdatei a	auswählen			? ×	
<u>Vertrau</u> Name	<u>S</u> uchen in:	C RLP-Intermediaer		💽 ጐ 🗈 💣 📰]•	
Name	Zuletzt verwendete D Desktop Eigene Dateien Arbeitsplatz	Binärformat DOI-CA-2-base64. PCA-1-Verwaltung RLP-VPS-base64.ce	cer 09-base64.cer er	Star:	Öffnen	
	Netzwerkumgeb ung	Datei <u>n</u> ame: JPU Datei <u>t</u> yp: Ze	.A-1-verwaltung-U9-base ertifikate (*.asc *.cer *.ce	b4.cer ▼ t *.crt *.der *.pem *.g ▼	Abbrechen	

Abbildung 27: Zertifikatsauswahl



Datei Ar	atra nsicht <u>Z</u> ert	ifikate E <u>x</u> tras	<u>E</u> instellungen <u>F</u> enste	er <u>H</u> ilfe				_ 🗆 ×
Zert	tifikate impoi	rtieren 👔 Ze	rtifikate exportieren	C Aktualisieren	😡 Vorgang abbr	echen 🛛 🚳	👌 Zertifikate auf Se	rver suchen
Suchen:					A	lle Zertifikate		*
<u>V</u> ert	trauenswürd	lige Zertifikate 🏾 🗎	Ande <u>r</u> e Zertifikate	Importierte Zertifika	ate Importierte	Zertifikate		
Nam	e $ abla bla bla bla bla bla bla bla$	E-Mail	Gültig ab	Gültig bis	Details	Schlüs	sel-Kennung	
			Ergebnis des Detailli C:/Dok Einstell Interm base64	Zertifikatimports – erte Ergebnisse des Im umgen/Administrator/C ediaer/PCA-1-Verwaltu I.cer: Insgesamt bearbe Import	Kleopatra ? X ports von Desktop/RLP- ing-09- itet: 1 iert: 1 iert: 1			

Zunächst wird das Rootzertifikat PCA-1-Verwaltung-09-base64.cer ausgewählt:

Abbildung 28: Import des Rootzertifikats

Ein Rechtsklick auf das Rootzertifikat ermöglicht es, diesem Zertifikat das erforderliche Vertrauen zu erteilen:

Zertifikate importi	ieren 🛄 Ze	rtifikate exportieren	Aktualisieren 🤅	🗿 Vorgang abbrechen	🛛 🊜 Zertifikate auf Serve	er s
nen:				- Alle Zer	tifikate	
Vertrauenswürdig	je Zertifikate	Ande <u>r</u> e Zertifikate	Importierte Zertifikate	e Importierte Zertif	ikate	
Name 🗸	E-Mail	Gültig ab	Gültig bis	Details	Schlüssel-Kennung	
			Inhaber-Vertraue <u>W</u> urzelzertifikat Wurzelzertifikat r	nswürdigkeit ändern /ertrauen gicht vertrauen	n	
			Zertifikat beglaut <u>A</u> blaufdatum änd <u>K</u> ennsatz ändern <u>B</u> enutzerkennung	oigen ern j hinzufügen		
			💢 Löschen		Entf	
			Zertifikate <u>e</u>xpor Mag Geheime Schlüss Zertifikate zu ein	tieren el exportieren em Server e <u>x</u> portieren.	Strg+E Strg+Umschalt+E	
			Certifikatsdetails			

Abbildung 29: Wurzelzertifikat vertrauen



Anschließend ist das Wurzelzertifikat blau hinterlegt:

o Kleopatra Datei Ansicht Zertifikate	e E <u>x</u> tras <u>E</u>	jinstellungen <u>F</u> enste	er <u>H</u> ilfe					_ 🗆 ×
Zertifikate importierer	n 👘 Zert	ifikate exportieren	C Aktualisieren	0	Vorgang abbrech	en 🛛 🚜 Z	Zertifikate auf Se	rver suchen
Suchen:					Alle Z	ertifikate		<u>_</u>
Vertrauenswürdige Ze	ertifikate 📔	Andere Zertifikate	Importierte Zertifi	kate	Importierte Zer	tifikate		
Name 🗸	E-Mail	Gültig ab	Gültig bis		Details	Schlüssel	-Kennung	
End PCA-1-Ver		2010-01-19	2016-01-18	X.50)9 3	FR49157		

Abbildung 30: Darstellung vertrauenswürdiges Wurzelzertifikat

Nun	wird auf	dem	gleichen	Weg da	s Zwiscl	nenzertifika	at DOI-0	CA-2 im	portiert
Carlos and a second second									

Kie opatra							- 🗆 ×
<u>D</u> atei <u>A</u> nsicht <u>Z</u> ert	tihikate E <u>x</u> tras <u>E</u> i	nstellungen <u>F</u> enst	er Hilfe	-	in a lange		
Zertifikate impo	rtieren 🔛 Zertif	ikate exportieren	C Aktualisieren	😡 Vorgang a	bbrechen 🛛 🍪 🕻	Zertifikate auf Serv	er suchen
Suchen:					Alle Zertifikate		-
Vertrauenswürd	dige Zertifikate 📔 /	Ande <u>r</u> e Zertifikate	Importierte Zertifik	kate I <u>m</u> portie	erte Zertifikate		1
Name 🗸	E-Mail	Gültig ab	Gültig bis	Details	Schlüssel	-Kennung	
PCA-1-Ver		2010-01-19	2016-01-18	X.509	3FA49157		
	Zertifikatsdatei	auswählen				? ×	
	<u>S</u> uchen in	C RLP-Interme	diaer	•	+ 🗈 💣 🎟]+	
	Eigene Dateien	Binärformat DOI-CA-2-bas PCA-1-Verwal RLP-VPS-base	DOI-CA-2-base64.ce	cer		<u>Ū</u> įfnen Abbrechen	

Abbildung 31: Import des Zwischenzertifikats



Der erfolgreiche Import des Zwischenzertifikats wird wie folgt bestätigt:

🗖 Kleop	atra							_ 🗆 ×
Datei A	nsicht <u>Z</u> ert tifikate impor	ifikate Extras (Einstellungen Eenste tifikate exportieren	er Hilfe C Aktualisieren	🙆 Vorgang	abbrechen	🍂 Zertifikate auf S	erver suchen
Suchen:						Alle Zertifika	ate	Ŧ
Veri	trauenswürd	ige Zertifikate \mid	Ande <u>r</u> e Zertifikate	Importierte Zertifi	kate I <u>m</u> por	tierte Zertifikate	e Importierte Zer	tifikate 🛛 🗾
Nam	ie 🗸	E-Mail	Gültig ab	Gültig bis	Details	Sch	lüssel-Kennung	
E PCA	1-Ver		2010-01-19	2016-01-18	X.509	3FR49:	157	
			2 Ergebnis des Ze Detailliert C:/Dokum Einstellun Intermed	ertifikatimports — e Ergebnisse des Imp nente und igen/Administrator/Di iaer/DOI-CA-2-base6 Insgesamt bearbei Importi	Kleopatra ? borts von esktop/RLP- i4.cer: tet: 1 ert: 1 ert: 1			

Abbildung 32: Ergebnis des Zwischenzertifikat-Imports

Datei <u>A</u> n	tra sicht <u>Z</u> ertifi	ikate E <u>x</u> tras	<u>E</u> instellungen <u>F</u> enste	er <u>H</u> ilfe					_ [
Zerti	fikate importi	ieren 🔔 Ze	rtifikate exportieren	C Aktualisieren	0	Vorgang abbre	echen 🛛 🝂	Jertifikate auf S	erver su	chen
Suchen:						A	le Zertifikate			-
<u>V</u> ertr	auenswürdig	ge Zertifikate	Ande <u>r</u> e Zertifikate	Importierte Zertil	ikate	Importierte	Zertifikate	Importierte Zert	ifikate	
Name	∇	E-Mail	Gültig ab	Gültig bis	1	Details	Schlüs	sel-Kennung		
	I-Ver DI CA 2		2010-01-19 2010-08-31	2016-01-18 2014-10-01	X.50 X.50	19 9	3FA49157 8C77F9C0			

Abbildung 33: Ausgeklapptes Zwischenzertifikat



👩 Kleopatra							- 🗆 ×
Datei Ansicht Zerl	tifikate E <u>x</u> tras	<u>E</u> instellungen <u>F</u> enste	er <u>H</u> ilfe				
Zertifikate impo	rtieren 🔛 Zer	tifikate exportieren	C Aktualisieren	🙆 Vorgani	g abbrechen 🛛 🧔	🍓 Zertifikate auf Serve	er suchen
Suchen:					Alle Zertifikate		*
Vertrauenswürd	dige Zertifikate	Ande <u>r</u> e Zertifikate	Importierte Zertifi	kate I <u>m</u> po	rtierte Zertifikate	Importierte Zertifika	ate 📃
Name $ abla$	E-Mail	Gültig ab	Gültig bis	Detail	s Schlüs	ssel-Kennung	
DOI CA 2		2010-01-19 2010-08-31	2016-01-18 2014-10-01	X.509 X.509	3FA4915 8C77F9C	7 0	-27
	Zertifikatsdat	ei auswählen				? ×	
	<u>S</u> uchen	in: 🔀 RLP-Interme	diaer] + 🖻 💣	.	
	Zuletzt verwendete D Desktop Eigene Dateie Arbeitsplatz Netzwerkumge ung	eb Dateiname: Dateityp:	se64.cer tung-09-base64.cer 64.cer RLP-VPS-base64. Zertifikate (*.asc *	cer .cer *.cert *.crt	×.der *.pem *,g v	<u>Ü</u> ʃfnen Abbrechen	

Jetzt wird das eigentliche Zertifikat, RLP-VPS, importiert:

Abbildung 34: Import des Zertifikats RLP-VPS





Abbildung 35: Importergebnis für das Zertifikats RLP-VPS

LDI Team A1-eGovernment



3.3. Verschlüsseln einer Datei

Es liegt eine zu verschlüsselnde Datei vor:

Test.txt					
🚺 Te:	st.txt - Edito	Dľ			- 🗆 🗙
Datei	<u>B</u> earbeiten	F <u>o</u> rmat	<u>A</u> nsicht	2	201-022
zu v	erschlüs	selnde	Datei	I	
					► //.

Abbildung 36: Zu verschlüsselnde (Text) Datei

Ein Rechtsklick auf die Datei ermöglicht die Auswahl "Mehr GpgEX Optionen": Dort wird der Unterpunkt "Verschlüsseln" gewählt.

Entschlüsseln
Prüfen Entschlüsseln und prüfen
Verschlüsseln
 Signieren
Signieren und verschlüsseln Zertifikate importieren
Prüfsummen erstellen
Hilfe zu GpgEX





Im folgenden Bildschirm muss die Option "Verschlüsseln" gewählt sein und mit "Weiter" bestätigt werden:

Ausgewählte Datei:	
• C:/Dokumente und Ei	nstellungen/Administrator/Desktop/Test.txt
Dateien archivieren mit:	TAR (PGP®-kompatibel)
Archivname (OpenPGP):	nte und Einstellungen/Administrator/Desktop/Test.txt.tar
Archivname (S/ <u>M</u> IME):	e und Einstellungen/Administrator/Desktop/Test.txt.tar.gz
C Signieren und verschlüsse	In (nur OpenPGP)
🖲 Verschlüsseln	
C Signieren	
Ausgabe als <u>T</u> ext (ASCII-I	Mantel)
🗖 Unverschlüsseltes Origina	Lapschließend löschen

Abbildung 38: Auswahl "Verschlüsseln

Jetzt wird das Zertifikat hinzugefügt und "Verschlüsseln" angeklickt:

uchen:			Alle Zertifik	ate		-
Name	∇	E-Mail	Gültig ab	Gültig bis	Details	
•						
			1			0
Name	∇	▼ Hinzufüg E-Mail	en E ntf	ernen Gültia bis	Details	
Name	P-VPS v	E-Mail ps@poststelle.rlp.de	Gültig ab 2011-03-16	ernen Gültig bis 2014-03-17	Details X.509	

Abbildung 39: Zertifikat hinzufügen und Verschlüsseln



Dieser Hinweis kann mit "Fortsetzen" ignoriert werden:

👩 Hinv	weis: Yerschlüsselung für sich selbst – Kleopatra	? ×
A	Keines der Empfängerzertifikate ist Ihr eigenes.	
<u> </u>	Das bedeutet, Sie können die Daten zwar verschlüsseln, aber nicht selbst wieder entsch	hlüsseln.
	Möchten Sie fortfahren, oder möchten Sie Ihre Wahl der Empfängerzertifikate ändern?	
∏ Die	ese Nachfrage nicht mehr anzeigen	
	Eortsetzen	bbrechen

Abbildung 40: Hinweis

Bei Bedarf kann hier auch die Option "Diese Nachfrage nicht mehr anzeigen" aktiviert werden.

Das Ergebnis wird im folgenden Bildschirm dargestellt:

		1
rgebnisse Hier wird der Status und der Fortschritt dei	r Verschlüsselungs-Ope	erationen angezeigt,
X.509: Alle Operationen abgeschlossen.		
Test.txt → Test.txt.p7m: Verschlüsseln ab	ogeschlossen.	<u>Details anzeigen</u> Prüfprotokoll anzeigen

Abbildung 41: Ergebnisdarstellung LDI Team A1-eGovernment



Mit einem Klick auf "Fertigstellen" wird der Vorgang abgeschlossen.

Die verschlüsselte Datei mit der Endung ".p7m" können Sie nun an eine E-Mail anhängen, die Sie an eine virtuelle Postfachadresse des Landes Rheinland-Pfalz senden möchten.



Abbildungsverzeichnis

Abbildung 1: Speichern des Setup-Programms	4
Abbildung 2: Ausführen des Setup-Programms	4
Abbildung 3: Startbildschirm des Setup-Programms	5
Abbildung 4: Bestätigung der Lizenzbedingungen	5
Abbildung 5: Einstellung der Installationsoptionen	6
Abbildung 6: Abschluss des Setup-Programms	7
Abbildung 7: Öffnen der Konfigurationsdatei "secsigner.properties"	7
Abbildung 8: Ergänzung der Datei secsigner.properties	8
Abbildung 9: Zu verschlüsselnde Datei auswählen	9
Abbildung 10: Bestätigungsfenster zur Auswahl des Verschlüsselungszertifikats	10
Abbildung 11: Auswahl des Verschlüsselungszertifikats	10
Abbildung 12: Speichern der verschlüsselten Datei	11