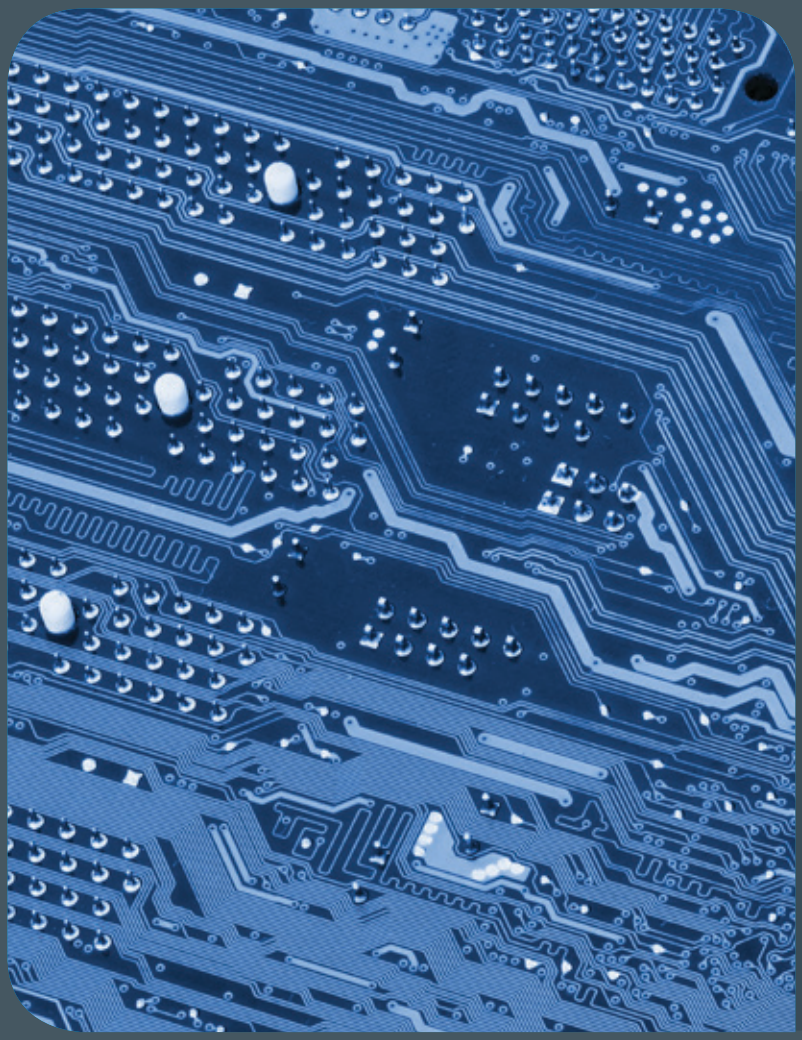
GWDG
NACHRICHTEN
Special 01|14

E-Mail-Verschlüsselung mit X.509-Zertifikaten

Zusammenfassung der Artikelserie aus den GWDG-Nachrichten 9 – 12/2013

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



GWDG
NACHRICHTEN

Special 01|14

Inhalt

E-Mail-Verschlüsselung mit X.509-Zertifikaten

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
37. Jahrgang
Special 1/2014

www.gwdg.de/gwdg-nr

Fotos:
© Maksym Yemelyanov - Fotolia.com (1)
© Spectral-Design - Fotolia.com (6)
© xiaoliangge - Fotolia.com (7)
GWDG (2)

Herausgeber:

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg 11
37077 Göttingen
Tel.: 0551 201-1510
Fax: 0551 201-2150

Redaktion:
Dr. Thomas Otto
E-Mail: thomas.otto@gwdg.de

Herstellung:
Maria Geraci
E-Mail: maria.geraci@gwdg.de

Druck:
GWDG / AG H
E-Mail: printservice@gwdg.de

E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 1: Beantragung und Sicherung von Zertifikaten

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

Aus aktuellem Anlass der National Security Agency (NSA) Prism-Affäre, bei der E-Mails massenhaft gespeichert und ihre Inhalte möglicherweise durchsucht wurden, soll in einer mehrteiligen Artikelserie, die in den kommenden Ausgaben der GWDG-Nachrichten fortgesetzt wird, gezeigt werden, wie sensible Informationen in E-Mails vor dem Zugriff Dritter geschützt werden können. Es kann natürlich mit dem Verfahren der E-Mail-Verschlüsselung nicht verhindert werden, dass diese aus den Datenströmen im Internet abgezweigt und gespeichert werden können. Aber es wird potenziellen Stellen im In- und Ausland wesentlich erschwert oder unmöglich gemacht, die Inhalte der E-Mails zu manipulieren oder diese gar zu lesen und nach bestimmten Begriffen durchzumustern.

BEGRIFFSERKLÄRUNGEN

Die zwei Hauptbegiffe, die im Zusammenhang mit dem Umgang von E-Mail-Verschlüsselung fallen, sind **X.509-Zertifikate** und **Public Key Infrastructure**, im Weiteren kurz **PKI** genannt.

Die PKI ist ein hierarchisch organisierter Aufbau von Zertifikatsautoritäten, engl. **Certification Authority** (im Weiteren kurz **CA** genannt), beginnend mit einer Wurzel, über Zwischenstationen hin zur ausstellenden Autorität für Zertifikate. Diese Kette der Autoritäten bildet die Grundlage einer PKI.

Die Zertifikate wiederum sind eine digitale Repräsentation von Benutzern, Diensten, Netzwerkgeräten oder Computern, die durch eine CA ausgestellt wurden. Diese Zertifikate sind zusammen mit jeweils einem privaten (private key) und einem öffentlichen (public key) Schlüssel miteinander verbunden.

Technisch betrachtet ist das Zertifikat eine digital signierte Ansammlung von Informationen, u. a. Informationen über den Benutzer, Dienst, Netzwerkgerät oder Computer, die ausstellende CA, die verwendeten Signier-/Verschlüsselungsverfahren, Informationen über die Abruf-URLs von Sperrlisten für gesperrte Zertifikate usw.

X.509 wiederum ist ein ITU-T-Standard (Internationale Fernmeldunion) für eine PKI zum Er-/Ausstellen digitaler Zertifikate.

ZERTIFIKAT BEANTRAGEN

Um nun ein Zertifikat zu beantragen, ist es als erstes wichtig zu wissen, welche ausstellende Registrierungsautorität, engl. **Registration Authority** (im Weiteren kurz **RA** genannt), für Antragsteller zuständig ist. Für die Kunden der Max-Planck-Gesellschaft und der Universität Göttingen gibt es jeweils einen Link, den es sich lohnt in der Lesezeichenliste aufzunehmen.

Für die MPG-CA ist das *https://ca.mpg.de/request* oder *https://ca.mpg.de/ras*.

Und für die Universität Göttingen-CA ist das *https://ca.uni-goettingen.de/request* oder *https://ca.uni-goettingen.de/ras*.

In jahrelanger Praxis hat es sich bewährt, das/die Zertifikat(e) mit dem Mozilla Firefox zu beantragen und zu verwalten. Ein weiterer Vorteil des Firefox-Webbrowser ist, dass dieser auf allen drei gängigen Plattformen Windows, Linux und Mac OS X zur Verfügung steht.

E-mail encryption using X.509 certificates

Due to recent events at the National Security Agency (NSA) Prism affair, in which the NSA stored mass of e-mails and searched their content for important keywords, a multipart series of articles, that will be continued in future issues of GWDG News, will show how sensitive information in e-mails can be protected from third party access. Of course with the method of the e-mail encryption it can not be prevented that e-mails can be diverted and stored from the data streams in the Internet. But it is made potential sites at homeland and abroad very difficult or impossible to manipulate the contents of the e-mails or even read this and to screen for certain terms.

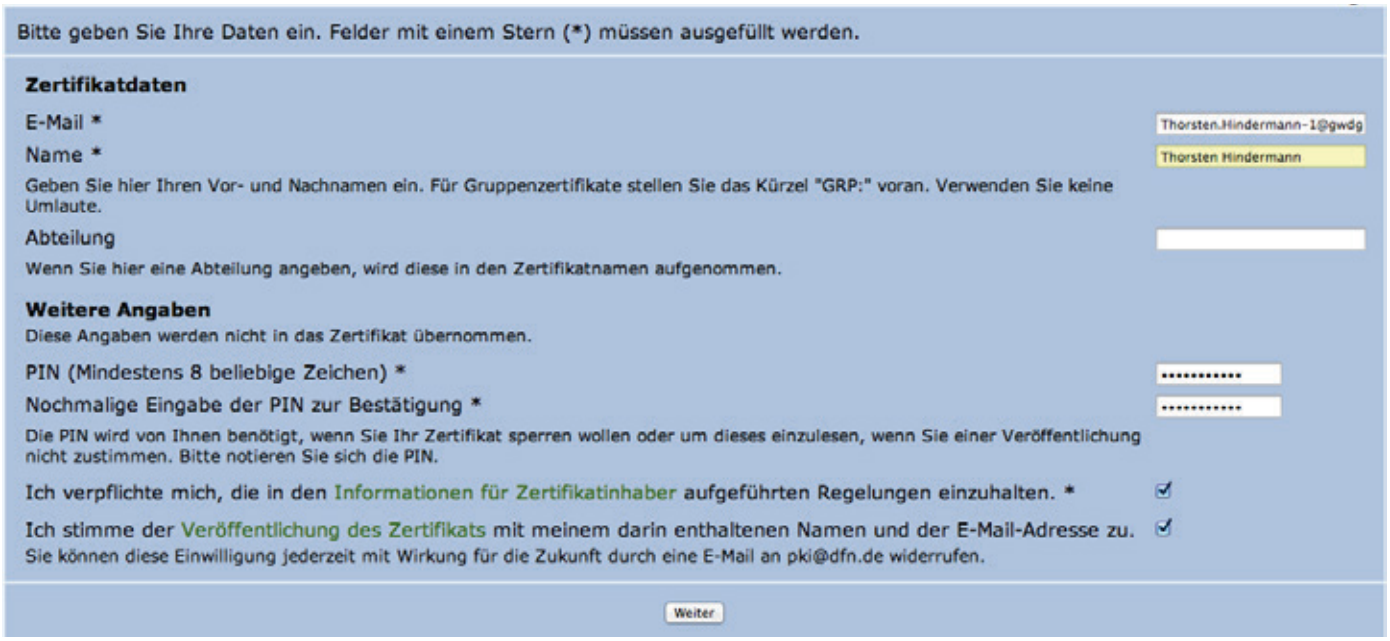


Abb. 1

Der eigentliche Antrag wird durch Klick auf die Schaltfläche „Nutzerzertifikat“ in der Menüleiste des Registerreiters „Zertifikate“ dann bei der ausgewählten RA mittels des Webbrowsers Firefox gestellt (siehe Abb. 1). Bei diesem Webformular ist es wichtig, dass die mit * gekennzeichneten Felder ausgefüllt werden. Eine Abteilung kann wahlweise angegeben werden. Nun muss noch eine PIN eingegeben werden. Diese wird oftmals beim Import des Zertifikats in den Firefox gebraucht und wenn der Anwender selbst sein Zertifkat sperren möchte. Auch hier wird dann die PIN abgefragt, bevor das Zertifikat dann gesperrt wird. Bitte diese Angabe gut merken! Da in einer PKI der öffentliche Schlüssel (engl. public key) ohne Bedenken weitergegeben werden kann, kann der Haken bei „Veröffentlichung des Zertifikats“ ohne Bedenken gesetzt werden. Diese Möglichkeit kann sich sogar als vorteilhaft erweisen, wie später noch beschrieben wird. Die „Informationen für den Zertifikatinhaber“ müssen auf alle Fälle durch Setzen des Hakens anerkannt werden. Jetzt auf „Weiter“ klicken.

In der Übersichtsseite über die eingegebenen Angaben können diese noch einmal auf ihre Richtigkeit geprüft werden und mit einem Klick auf „Ändern“ korrigiert werden. Andernfalls nun auf „Bestätigen“ klicken.

Wurde auf „Bestätigen“ geklickt, wird im Firefox der private Schlüssel generiert und im Firefox-Zertifikatspeicher abgelegt. Dieser Zertifikatspeicher ist unabhängig vom verwendeten Betriebssystem. Weiterhin wird der Zertifikatantrag, engl. **certificate signing request** (im Weiteren kurz **CSR**), in der ausgewählten RA hochgeladen.

Es wird eine Bestätigungsseite angezeigt. Mit einem Klick auf „Zertifikatantrag anzeigen“ wird der generierte Antrag im PDF-Format entweder gleich angezeigt oder heruntergeladen und kann dann mit einem PDF-Anzeigeprogramm angezeigt und ausgedruckt werden. Diese Handhabung hängt vom verwendeten Betriebssystem und/oder installierten PDF-Anzeigeprogramm ab. Den ausgedruckten Antrag muss der Zertifikatnehmer eigenhändig unterschreiben.

Mit diesem Formular muss er dann zum RA-Operator der ausgewählten RA gehen. Dort wird die persönliche Identifizierung vorgenommen, d. h. mittels des Personalausweises des Zertifikatnehmers vergleicht und überprüft der RA-Operator die Angaben auf dem Zertifikatantrag mit dem Ausweis. Wenn alles in Ordnung ist, wird der RA-Operator das Zertifikat dann zeitnah ausstellen. Per Bestätigungsmail an den Zertifikatnehmer wird dieser über die Ausstellung des Zertifikats unterrichtet. Korrekterweise muss hier von der Signierung des öffentlichen Schlüssels, des hochgeladenen CSR, durch die entsprechende CA gesprochen werden.

In der Bestätigungsmail kopiert der Zertifikatnehmer den zweiten URL – das ist wichtig(!) – aus der E-Mail und kopiert diesen in die Adresszeile des Firefox. Ist auf dem System des Zertifikatnehmers der Firefox der Standardbrowser, genügt ein Klick auf diesen Link.

Nun werden im Firefox der private und signierte öffentliche Schlüssel zusammengeführt und beide ergeben zusammen das Zertifikat (siehe Abb. 2). Ist dieser Vorgang erfolgreich abgeschlossen, wird folgender Hinweis präsentiert. (siehe Abb. 3). Im

Abb. 2

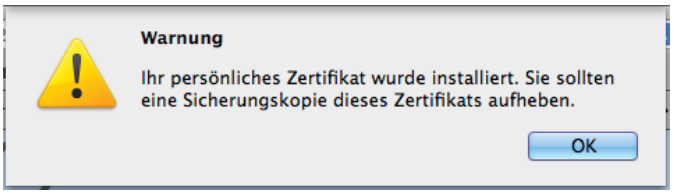


Abb. 3

folgenden Kapitel wird dieser wichtige Teil beschrieben.

Ein detaillierte Anleitung zur Beantragung eines Zertifikats ist unter dem URL *http://www.gwdg.de/index.php?id=zertifikat_beantragen* zu finden.

Anmerkung: Neben dem Firefox kann auch mit dem Internet Explorer (im Weiteren kurz IE genannt) auf grafische Weise ein Zertifikatantrag erzeugt werden. Manchmal kann es aber mit dem IE vorkommen, dass oftmals, abhängig von der eingesetzten Windows-Version, ein wichtiger betriebssystemseitiger Bestandteil noch nicht installiert ist, so dass es zu Fehlermeldungen kommen kann und die Beantragung scheitert. Hier müssen dann oftmals die VortOrt-Administratoren erst noch das fehlende Programmteil installieren, bevor die Beantragung gelingt. Es ist auch die Erzeugung eines CSR mittels des Kommandozeilenprogramms Open-SSL möglich, allerdings werden hier dann schon erweiterte Kenntnisse mit Zertifikaten und der Umgang mit der Kommandozeile vorausgesetzt. Aus diesem Grund hat sich die Verwendung des Firefox im Laufe der Jahre als am praktikabelsten herausgestellt.

SICHERUNG VON ZERTIFIKATEN

Eine der wichtigsten Handlungen ist es, eine Sicherheitskopie des gerade erstellten Zertifikats anzufertigen. Auch hier ist der Firefox Webbrowser dem Zertifikatnehmer behilflich.

Dazu muss unter „Extras" der Einstellungen-Dialog im Firefox geöffnet werden. Hier das Zahnrad-Symbol mit der Unterschrift „Erweitert" anklicken und auf der mehrfach geteilten Schaltfläche darunter auf „Zertifikate" klicken. Nun die Schaltfläche „Zertifikate anzeigen" anklicken (siehe Abb. 4).

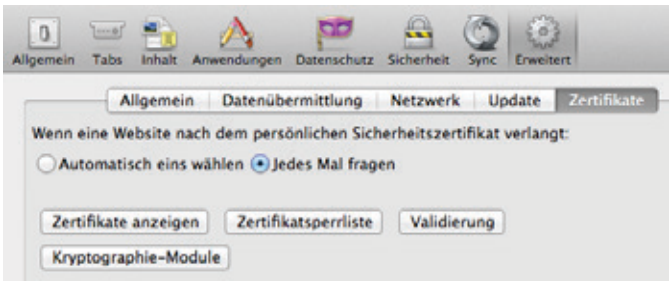


Abb. 4

In dem nun erscheinenden Dialog auf der mehrfach geteilten Schaltfläche/Registerreiter auf „Ihre Zertifikate" klicken und das gerade zusammengeführte Zertifikat anklicken. Auf die Schaltfläche „Sichern..." klicken (siehe Abb. 5). Es wird nach einem Kennwort gefragt, mit der die Container-Datei im PKCS#12-Format verschlüsselt wird. Der Grund dafür ist, dass diese Datei sowohl den privaten als auch den öffentlichen Schlüssel enthält, also das gesamte Zertifkat. Gerade wegen des privaten Schlüssels ist es wichtig, dass diese Datei entsprechend gesichert ist.

Im entsprechenden Speicherdialog muss ein Datenträger/Verzeichnis angegeben werden, wo die Datei mit der Dateiendung *.P12* gespeichert werden soll. Es empfiehlt sich ein externer Datenträger. Praktischer Hintergrund: Wenn der Rechner, auf dem das Zertifikat mal beantragt wurde, ausgetauscht wird, die Festplatte formatiert wird oder defekt ist, ist das Zertifikat unwiderruflich verloren. Dann ist ein Entschlüsseln von E-Mails, die mit diesem Zertifikat verschlüsselt worden sind, für immer unmöglich!

Anmerkung: Die Sicherung hat auch noch einen anderen, praktischen Aspekt, der nicht unterschätzt werden sollte. Im Laufe der Tätigkeit sammeln sich mit der Zeit einige Zertifikate an. Wenn nun mit einem oder mehreren Zertifikaten E-Mails verschlüsselt worden sind, können diese alten E-Mails nur mit dem dann aufbewahrten Zertifikat wieder entschlüsselt werden, selbst wenn zu diesem Zeitpunkt das Zertifikat sein Ablaufdatum überschritten hat. Deshalb ist die Sicherung und Aufbewahrung ein wichtiger Schritt. D. h. bei einem Rechnerwechsel müssen dann am besten

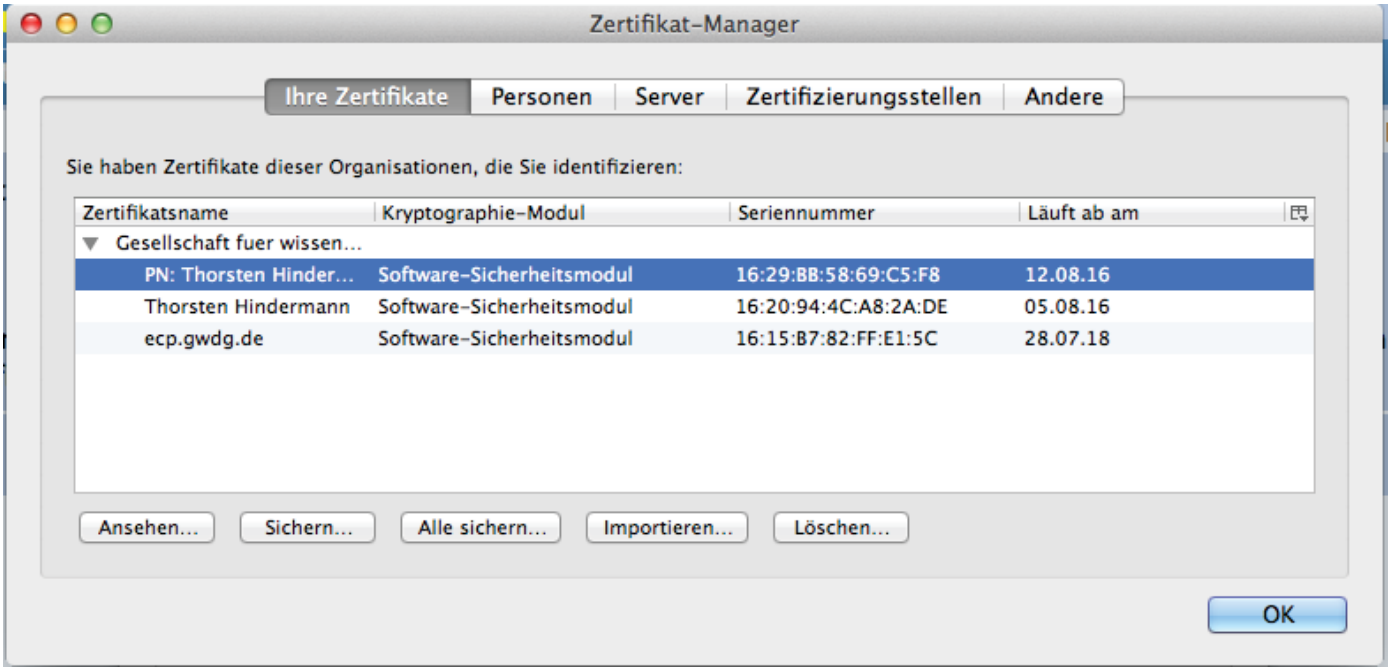


Abb. 5

alle alten und das aktuelle Zertifikat in die entsprechenden Zertifikatspeicher importiert werden. Dieser Vorgang wird im Teil 2 in den nächsten GWDG-Nachrichten näher beschrieben.

Hinweis: Ein persönliches Zertifikat, um E-Mail-Nachrichten zu signieren/verschlüsseln, hat eine Laufzeit von drei Jahren.

AUSBLICK

Nachdem in diesem Artikel die Beantragung und Sicherung von Zertifikaten zur E-Mail-Verschlüsselung erläutert wurden, sollen in den nächsten Teilen folgende Themen detailliert behandelt werden:

- Installation und Verteilung von Zertifikaten (GWDG-Nachrichten 10/2013)
- Verschlüsselung bei Outlook-Mailanwendungen (GWDG-Nachrichten 11/2013)
- Verschlüsselung bei Thunderbird, Notes 9 und Apple-Mailanwendungen (GWDG-Nachrichten 12/2013)

Infobox

Wichtige URLs

Zertifikate beantragen

MPG: *https://ca.mpg.de/request oder https://ca.mpg.de/ras*
Universität Göttingen: *https://ca.uni-gottingen.de/request* oder *https://ca.uni-goettingen.de/ras*

Informationen

Allgemein: *http://www.gwdg.de/pki*
Public-Key-Infrastruktur: *http://www.gwdg.de/index.php?id=pki*
Detailinfomationen: *http://wiki.gwdg.de/index.php/Kategorie:PKI*
PKI-FAQ: *http://www.gwdg.de/index.php?id=faq#c2374*

Artikel in den GWDG-Nachrichten zum Thema „Zertifikate“

Ein zweiteiliger Artikel zur Einführung in die Welt der X.509-Zertifikate in den Ausgaben 9/2011 und 10/2011

Ein Artikel, wie Zertifikate für die VMware-Infrastruktur-Dienste erstellt werden, in der Ausgabe 5/2013

Kontakt

Bei weiteren Fragen zu diesem Thema schreiben Sie bitte eine entsprechende E-Mail an *support@gwdg.de*.

E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 2: Installation und Verteilung von Zertifikaten

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

Im ersten Teil dieses mehrteiligen Artikels ging es um die Beantragung von X.509-Zertifkaten für die E-Mail-Verschlüsselung. Weiterhin wurde erläutert, wie das erhaltene und im Webbrowser enthaltene Zertifikat gesichert wird. Im zweiten Teil geht es nun darum, wie das Zertifikat in die Zertifikatspeicher von Betriebssystemen und Anwendungen importiert wird. Weiterhin wird aufgezeigt, wie der öffentliche Schlüssel eines X.509-Zertifikats in zentralen Verzeichnissen verteilt und abgerufen werden kann.

INSTALLIEREN VON ZERTIFIKATEN IN ZERTIFIKATSPEICHERN

Windows

Unter Windows wird ein Zertifikat im persönlichen Zertifikatspeicher des angemeldeten Benutzers gespeichert. Dazu die .P12-Datei, die im vorherigen Abschnitt (s. Teil 1 in den GWDG-Nachrichten 9/2013) wie beschrieben abgespeichert wurde, doppelt anklicken. Der Zertifikatimport-Assistent öffnet sich. Das hier beschriebene Verfahren bezieht sich auf Windows 8. Für vorherige Versionen von Windows sind die Dialoge ähnlich und das Ergebnis am Ende des Importvorgangs identisch. Beim Speicherort darauf achten, dass „Aktueller Benutzer“ ausgewählt ist und dann auf „Weiter“ klicken (s. Abb. 1).

Im nächsten Dialog ist durch den Doppelklick das Eingabefeld „Dateiname:“ mit der doppelt angeklickten .P12-Datei schon ausgefüllt. Hier einfach auf „Weiter“ klicken. Im nun erscheinenden Dialog muss das Kennwort eingegeben werden, dass beim Export des Zertifikats angegeben wurde. Die Auswahlmöglichkeiten wie angezeigt anhaken, da diese sich in der Praxis bewährt haben. Dann auf „Weiter“ klicken. (s. Abb. 2).

Zusätzlich kann noch die Wahlmöglichkeit „Hohe Sicherheit für den privaten Schlüssel aktivieren“ ausgewählt und dann auf „Weiter“ geklickt werden. Wie im Erklärungstext der Wahlmöglichkeit steht, wird bei jeder Verwendung des privaten Schlüssels eine Kennworteingabe angezeigt.

Hier darauf achten, dass „Zertifikatspeicher automatisch wählen“ ausgewählt ist und auf „Weiter“ klicken (s. Abb. 3).

Zum Abschluss kommt noch ein Dialogseite, die alle Eingaben zusammenfasst. Wenn alle Angaben richtig sind auf „Fertig stellen“ klicken (s. Abb. 4).

Hinweis: Wenn neben einem Arbeitsplatzrechner auch noch Zugriff auf eine Microsoft Terminalserver-Umgebung besteht, müssen diese Schritte auch dort wiederholt werden, wenn in

E-mail encryption using X.509 certificates – Part 2: Installation and distribution of certificates

In the first part of this multi-part article, we went over the application of X.509 certifcates for e-mail encryption. Furthermore it was explained how the received certificate, that is contained in the web browser, can be backed. The second part is about how the certificate is imported into the certificate store of operating systems and applications. Furthermore, it is shown how the public key of an X.509 certificate can be distributed and accessed in directory services.

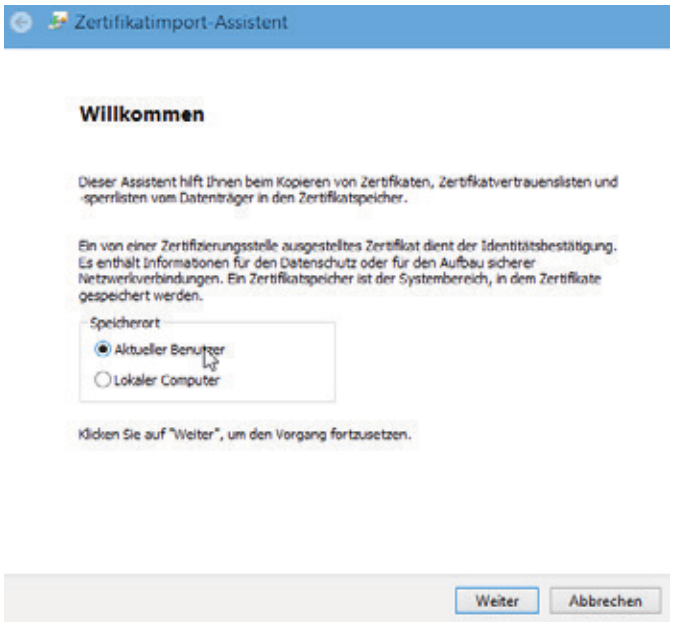


Abb. 1

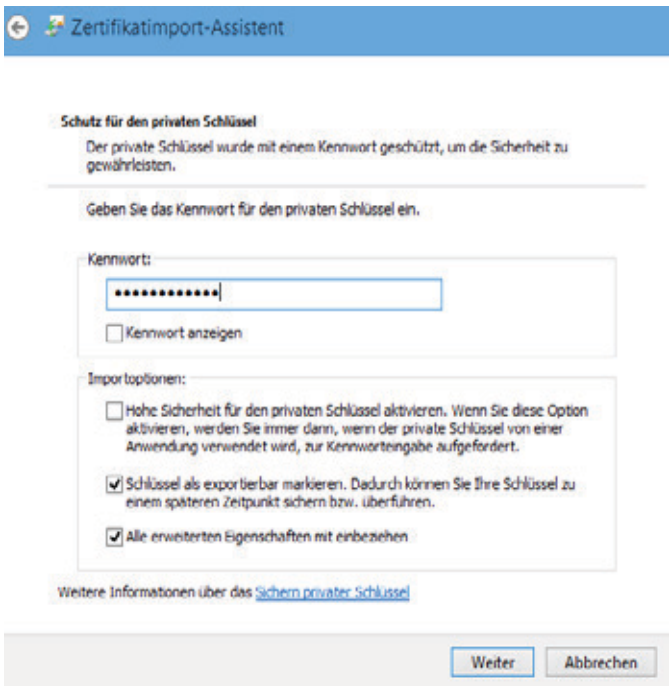


Abb. 2

der Terminalserver-Umgebung andere dort zentral zur Verfügung gestellte Anwendungen auf den persönlichen Windows-Zertifikatspeicher zugreifen möchten.

OS X

Um das Zertifikat in die Schlüsselbundverwaltung zu importieren müssen folgende Schritte ausgeführt werden.

Auf „Ablage|Objekt importieren…" klicken und in dem angezeigten Dialog den Datenträger und das entsprechende Verzeichnis auswählen, in das die .P12-Datei aus dem vorherigen Abschnitt gespeichert wurde. Die Datei und den Ziel-Schlüsselbund auswählen und auf „Öffnen" klicken (s. Abb. 5).

Im nun erscheinenden Dialog muss das Kennwort eingegeben werden, dass beim Export des Zertifikats angegeben wurde. Danach auf „OK" klicken.

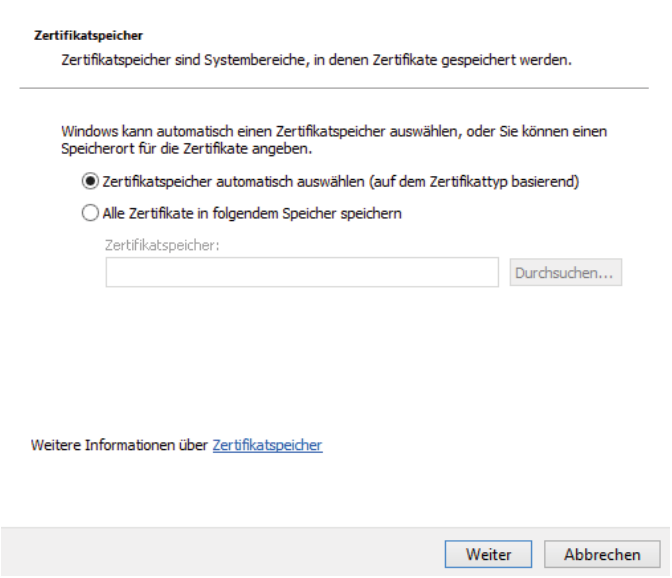


Abb. 3

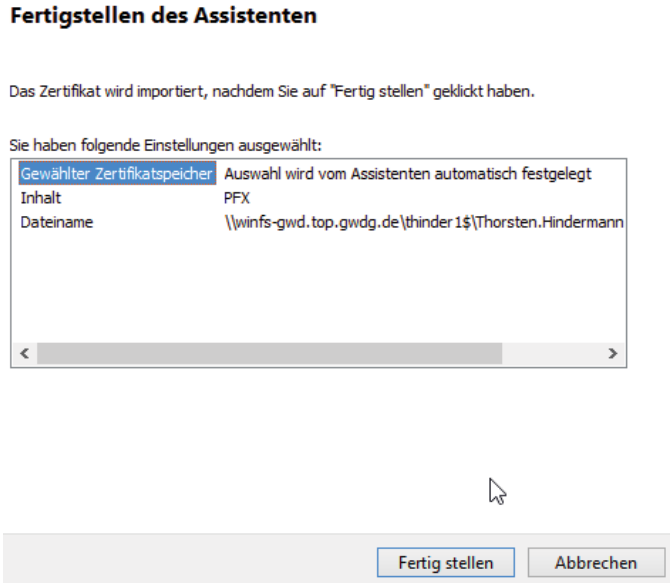


Abb. 4

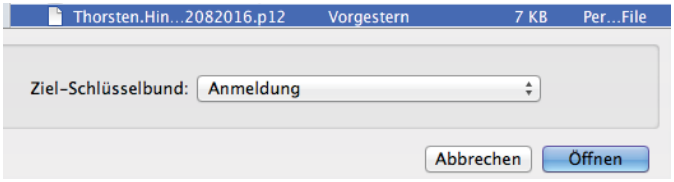


Abb. 5

Thunderbird

Den Einstellungsdialog aufrufen. Dort dann das Symbol „Erweitert" anklicken, in der mehrfach geteilten Schaltfläche/Registerreiter „Zertifikate" auswählen und die Schaltfläche „Zertifikate" anklicken.

Auf der mehrfach geteilten Schaltfläche/Registerreiter „Ihre Zertifikate" auswählen und auf „Importieren…" klicken.

In dem angezeigten Dialog den Datenträger und das entsprechende Verzeichnis auswählen, in das die .P12-Datei aus dem vorherigen Abschnitt gespeichert wurde. Darauf achten, dass bei „Format:" *PKCS12-Dateien* eingestellt ist. Dann auf „Öffnen" klicken.

Im nun erscheinenden Dialog muss das Kennwort eingegeben werden, dass beim Export des Zertifikats angegeben wurde. Danach auf „OK“ klicken.

Anmerkung: Um ein Zertifikat im Firefox zu installieren, bitte die gleichen Schritte durchführen. Aber hier heißt die Schaltfläche nicht einfach „Zertifikate“ sondern „Zertifikate anzeigen“.

IBM Notes 9

Den Dialog unter „Datei > Sicherheit > Benutzersicherheit“ öffnen. Auf das Plus-Zeichen bei „Ihre Identität“ klicken und das Untermenü „Ihre Zertifikate“ auswählen.

In diesem Dialogfeld dann die Drop-Down-Liste anklicken und das Listenelement „Ihre Internetzertifikate“ auswählen.

Nun die Drop-Down-Liste mit der Aufschrift „Zertifikate abrufen“ anklicken und „Internetzertifikate importieren...“ auswählen (s. Abb. 6).

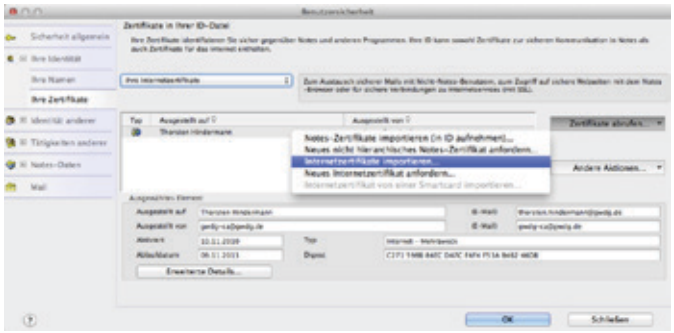


Abb. 6

In dem nun geöffnetem Dialog zu dem Verzeichnis/Datenträger wechseln, in dem sich ein Zertifikat-Container im PKCS#12-Format befindet. Diese Container sind an einer Dateiendung *.P12* oder *.PFX* zu erkennen. Den entsprechenden Container auswählen und „Öffnen“ anklicken.

In der nun geöffneten Dialogbox die Einstellung auf PKCS 12 stehen lassen und auf „Weiter“ klicken (s. Abb. 7).

Abb. 7

In dem nächsten Dialogfeld das Kennwort eingeben, mit der die PKCS#12 geschützt ist. Dann auf „OK“ klicken (s. Abb. 8).

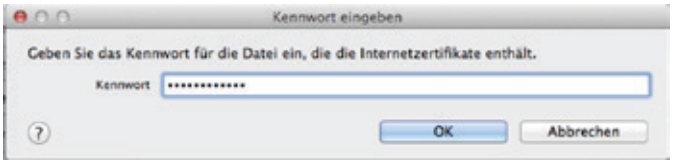


Abb. 8

In der Dialogbox „Internetzertifikate importieren“ auf „Alle annehmen“ klicken. Nachdem das Importieren beendet ist, sieht die Anzeige aller Internetzertifikate wie folgt aus (s. Abb. 9).

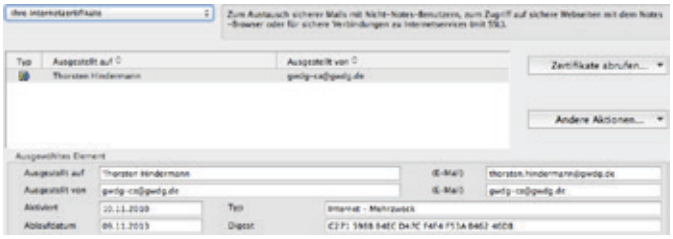


Abb. 9

Weitere Einstellungen für das X.509-Zertifikat: Weiterhin im Dialog „Benutzersicherheit“ bleiben und in der Navigation links ganz unten den letzten Eintrag „Mail“ anklicken. Als erstes den Haken „Mail zum Senden signieren“ setzen (s. Abb. 10).

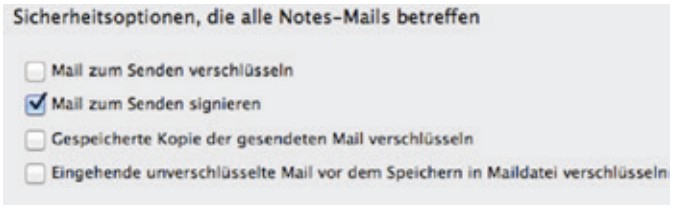


Abb. 10

Dann auf „Optionen für Mail im Internetstil...“ klicken. Den Haken unter dem Punkt „MIME-Format zum Senden von Mail“ setzen (s. Abb. 11).

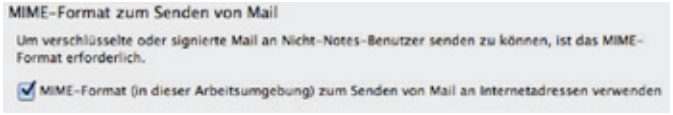


Abb. 11

Dann auf „Zertifikatskonfiguration...“ klicken. Überprüfen, ob hier das importierte Zertifikat zu sehen ist (s. Abb. 12).

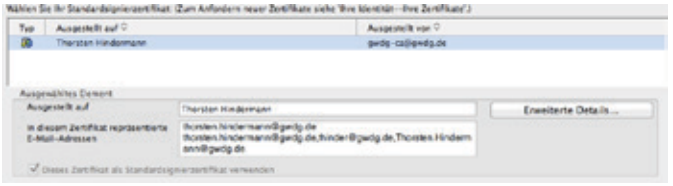


Abb. 12

Damit sind der Import und die Konfiguration eines X.509-Zertifikats für die Signierung von Mails im Internet-Stil abgeschlossen.

ABLAGE UND VERTEILUNG DES ÖFFENTLICHEN SCHLÜSSELS

X.509-Zertifikate bestehen, wie schon erwähnt, aus zwei Teilen: dem privaten und dem öffentlichen Schlüssel. Während der private Schlüssel gut geschützt beim Zertifkatnehmer verbleibt, kann und darf der öffentliche Schlüssel verbreitet werden. Für dieses Vorhaben gibt zwei Möglichkeiten, entweder eine zentrale Ablage verwenden oder ihn per E-Mail versenden.

DFN

Eine zentrale Möglichkeit ist der Public Key Server des DFN. Wenn bei der Beantragung des Zertifikats der Haken bei

„Veröffentlichung des Zertifikats“ gesetzt wird, dann wird der öffentliche Schlüssel nach der Ausstellung des Zertifikats automatisch vom DFN dort abgelegt. Damit unten beschriebene E-Mail-Anwendungen bei der Mailverschlüsselung dort nach dem öffentlichen Schlüssel suchen, müssen diese Anwendungen dafür eingerichtet werden. Hier die Werte, die eingestellt werden müssen: Port: *389*, Servername: *ldap.pca.dfn.de*, Basispunkt: *O=DFN-Verein,C=DE*.

Wenn es nicht gewollt oder gewünscht ist, das komplette DFN-weite Verzeichnis abzusuchen, kann auch eine Einschränkung auf die eigene Gesellschaft eingestellt werden. Dazu einfach den Basispunkt (im Weiteren kurz Base-DN genannt) genauer einstellen: **MPG:** *O=Max-Planck-Gesellschaft,OU=DFN-PKI,O=DFN-Verein,C=DE*, **Universität Göttingen:** *O=Georg-August-Universitaet Goettingen,OU=DFN-PKI,O=DFN-Verein,C=DE*, **GWDG:** *O=Gesellschaft fuer wissenschaftliche Datenverarbeitung,OU=DFN-PKI,O=DFN-Verein,C=DE*.

Outlook 2013 für Windows

Unter Windows die Systemsteuerung aufrufen und das Programm-Symbol „E-Mail“ anklicken. Damit das Programm-Symbol leicht gefunden werden kann, in der Systemsteuerung unter „Anzeige:“ die Auswahlliste von „Kategorie“ auf „Große Symbole“ oder „Kleine Symbole“ umstellen. In dem nun erscheinenden Dialog auf „E-Mail-Konten...“ klicken (s. Abb. 13).

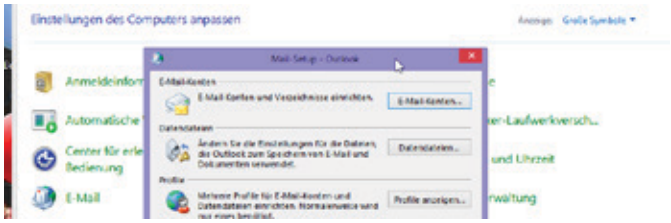


Abb. 13

Im nächsten Dialog auf den Registereiter „Adressbücher“ klicken und dann auf „Neu...“ (s. Abb. 14).

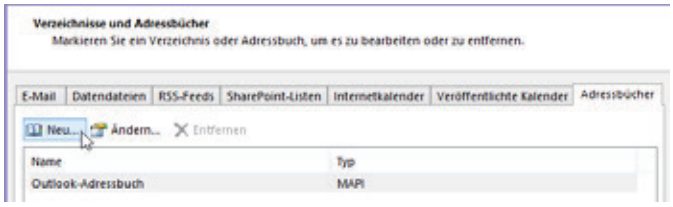


Abb. 14

Im nächsten Dialog ist „Internetverzeichnisdienst (LDAP)“ vorausgewählt. Um fortzufahren auf „Weiter >“ klicken (s. Abb. 15).

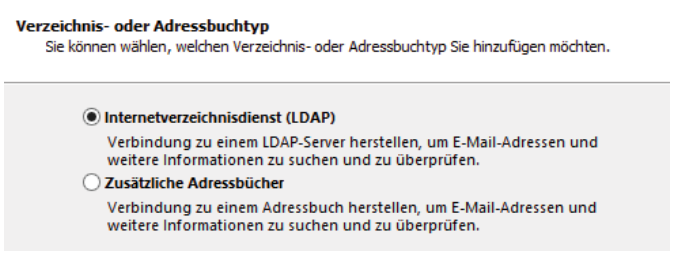


Abb. 15

Im nun erscheinenden Dialog den Serveramen des Server im Eingabefeld für „Servername:“ eingeben und danach auf „Weitere Einstellungen...“ klicken (s. Abb. 16).

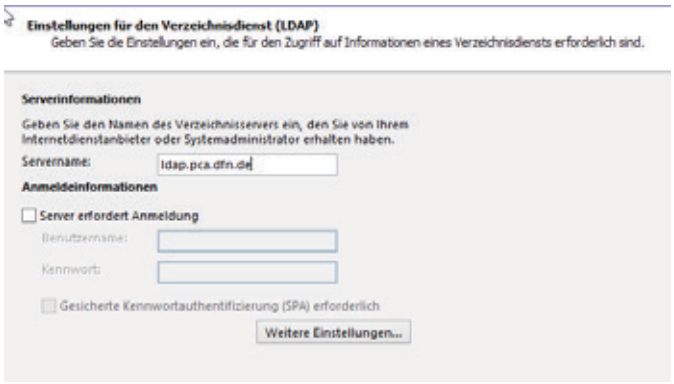


Abb. 16

Im nun folgenden Dialog auf den Registerreiter „Suche“ klicken. Hier in der Gruppe „Suchbasis“ „Benutzerdefiniert:“ anklicken und in das Eingabefeld den Base-DN eingeben und auf „OK“ klicken (s. Abb. 17).

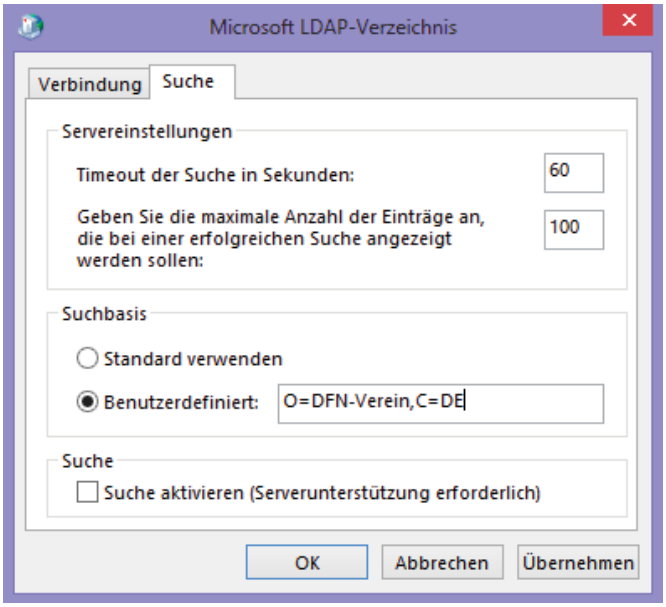


Abb. 17

Nun auf „Weiter >“ und im Folgenden auf „Fertig stellen“ klicken.

Hinweis: Wenn neben einem Arbeitsplatzrechner auch noch Zugriff auf eine Microsoft Terminalserver-Umgebung besteht, müssen diese Schritte auch dort wiederholt werden, wenn in der Terminalserver-Umgebung Outlook genutzt wird. Technische Begründung ist, dass das Active Directory- und das Terminalserver-Profil zwei getrennte Profile sind.

Outlook 2011 für OS X

Ist Outlook geöffnet, über das Menü „Einstellungen...“ das Symbol „Konten“ oder über „Extras|Konten...“ anklicken.

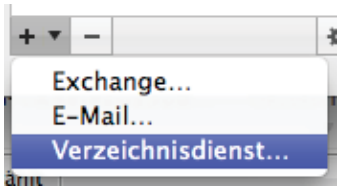


Abb. 18

In dem angezeigten Dialog auf das Pluszeichen unten links in der Ecke klicken und „Verzeichnisdienst...“ auswählen (s. Abb. 18).

In dem Dialog in das Eingabefeld für „LDAP-Server“ oben angegebenen Servernamen eingeben und auf „Konto hinzufügen klicken“ (s. Abb. 19).

Abb. 19

Wenn gewünscht, kann der Name von *Dfn* noch auf *DFN-PKI* geändert werden. Unten rechts auf „Erweitert...“ klicken (s. Abb. 20).

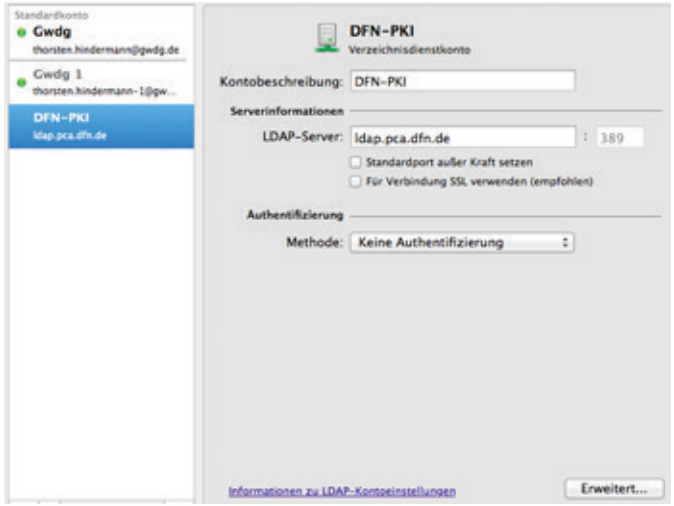


Abb. 20

In dem jetzt erscheinenden Dialog den Base-DN im Eingabefeld für die „Suchbasis:“ eingeben und mit „OK“ bestätigen (s. Abb. 21).

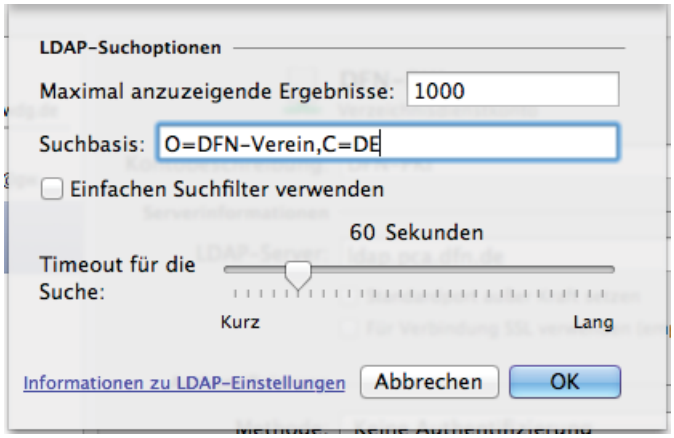


Abb. 21

Mail.app OS X 6.5

Die Einstellungen mittels *CMD+,* der OS X Mail.app aufrufen und das Symbol mit dem Untertitel „Verfassen“ anklicken. In dem angezeigten Einstellungsdialog nun in der Gruppe „Adressen:“ auf die Schaltfläche „LDAP...“ klicken (s. Abb. 22).

Abb. 22

In dem nun erscheinenden Dialog auf das kleine „+“-Symbol klicken.

Im nun folgenden Dialog „Serverinfo“ die entsprechenden Eingaben wie oben beschrieben tätigen und auf „Sichern“ klicken (s. Abb. 23).

Abb. 23

Der vorherige Dialog sieht nun wie folgt aus (s. Abb. 24).

Abb. 24

Diesen Dialog nun mit einem Klick auf „Fertig“ verlassen.

Thunderbird Version 17

Den Einstellungsdialog aufrufen. Dort dann das Symbol „Verfassen“ anklicken, in der mehrfach geteilten Schaltfläche/Registerreiter „Adressieren“ anklicken.

In dem aktuellen Dialog den Haken bei

„LDAP-Verzeichnisserver“ setzen (s. Abb. 25).

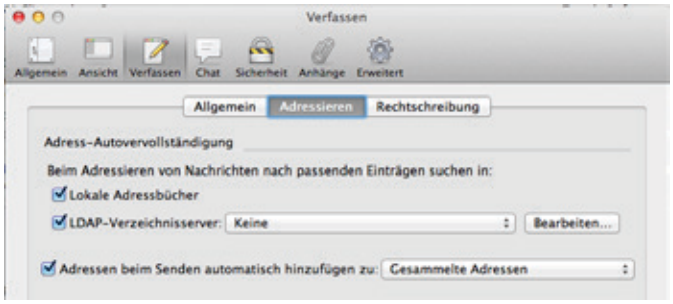


Abb. 25

Auf „Bearbeiten“ klicken. In dem Dialogfenster auf „Hinzufügen“ klicken. Werte wie oben angegeben eingeben (s. Abb. 26).

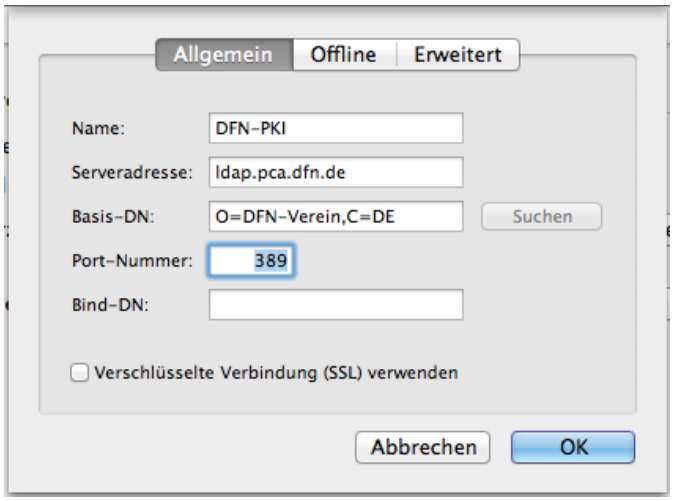


Abb. 26

Mit „OK“ bestätigen und nochmals mit „OK“ bestätigen. Nun in der Auswahlliste für „LDAP-Verzeichnisserver“ den Eintrag „DFN-PKI“ auswählen (s. Abb. 27).

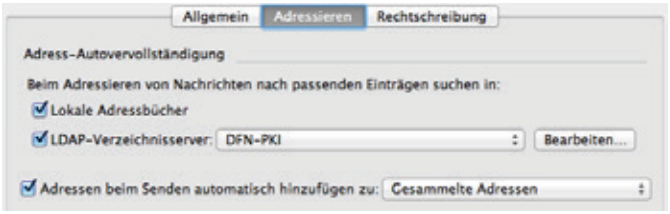


Abb. 27

IBM Notes 9

Dazu den Benutzervorgaben-Dialog für IBM Notes 9 aufrufen. Unter gleich dem ersten Eintrag „Accounts“ sind in der rechten Inhaltsseite die vorangestellten Verbindungen zu sehen (s. Abb. 28).

Abb. 28

Jetzt in der Gruppe „Allgemein“ auf „Neuer Account“ klicken. Die ersten allgemeinen Informationen eingeben, wie der „Accountname:“ *DFN-PKI*, wahlweise eine Beschreibung. Den „Typ:“ auf *LDAP* aus der Auswahlliste wählen und bei „Servername:“ *ldap.pca.dfn.de* eingeben (s. Abb. 29).

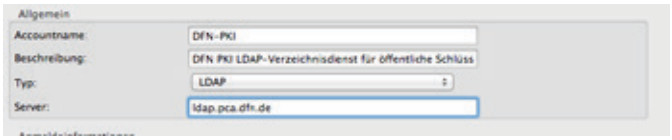


Abb. 29

Mit einem Klick auf die Gruppenüberschrift „+ Erweiterte Eigenschaften“ die weiteren Einstellungsmöglichkeiten aufklappen. Im Eingabefeld der „Suchbasis:“ folgende Eintragung vornehmen: *O=DFN-Verein,C=DE*. Die restlichen, voreingestellten Eintragungen so beibehalten. Nun den Dialog mit „OK“ abschließen (s. Abb. 30).

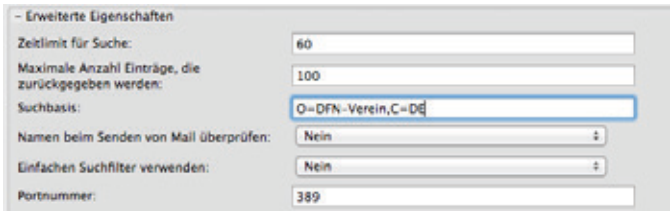


Abb. 30

Den Benutzervorgaben-Dialog ebenfalls mit „OK“ schließen.

Abruf des Zertifikats mittels Kommandozeilenprogramm

Mittels des Kommandozeilen-Programm *ldapsearch* ist möglich, den öffentlichen Schlüssel abzurufen.

Zu diesem Zweck ldapsearch mit den folgenden Übergabeparametern aufrufen: *ldapsearch -h ldap.pca.dfn.de -t -x -b O=DFN-Verein,C=DE ‚(mail=thorsten.hindermann-1@gwdg.de)‘ userCertificate*

Hier die Erklärung der Parameter:

-h – Servername des DFN LDAP-Verzeichnisservers

-t – speichert binäre Werte von Attributen in temporären Dateien

-x – baut eine Verbindung ohne Anmeldung auf

-b – Basispunkt (Base-DN)

Nun folgt der Suchfilter, in diesem Beispielfall *‚(mail=thorsten.hindermann-1@gwdg.de)‘*.

Darauf folgen die Attribute, die ausgelesen werden sollen. In diesem Fall nur das Attribut *userCertificate*.

Mit dem Befehl *man 1 ldapsearch* wird eine ausführliche Hilfeseite in jedem UNIX-basierten System oder Subsystem, z. B. cygwin für Windows, angezeigt.

Active-Directory-Verzeichnisdienst

Mit Hilfe des E-Mail-Clients Outlook 2013 ist der Zertifikatnehmer selbst in der Lage, seinen öffentlichen Schlüssel in einem lokalen Active-Directory-Verzeichnisdienst zu speichern.

Über „Datei|Optionen“ den „Outlook-Optionen“-Dialog öffnen. In der linken Navigationsspalte ganz unten auf „Trust Center“ klicken.

Hinweis: Bei Outlook 2010 heißt „Outlook-Optionen“ nur „Optionen“ und „Trust Center“ heißt „Sicherheitscenter“.

Im Inhaltsfenster rechts nun ganz unten auf die Schaltfläche „Einstellungen für das Trust Center...“ klicken.

Der „Trust Center“-Dialog öffnet sich. In der linken

Navigationsspalte auf „E-Mail-Sicherheit“ klicken.

Im Inhaltsfenster rechts in der Gruppe „Verschlüsselte E-Mail-nachrichten“ die Schaltfläche „Einstellungen...“ klicken und den angezeigten Dialog mit „OK“ bestätigen (s. Abb. 31).

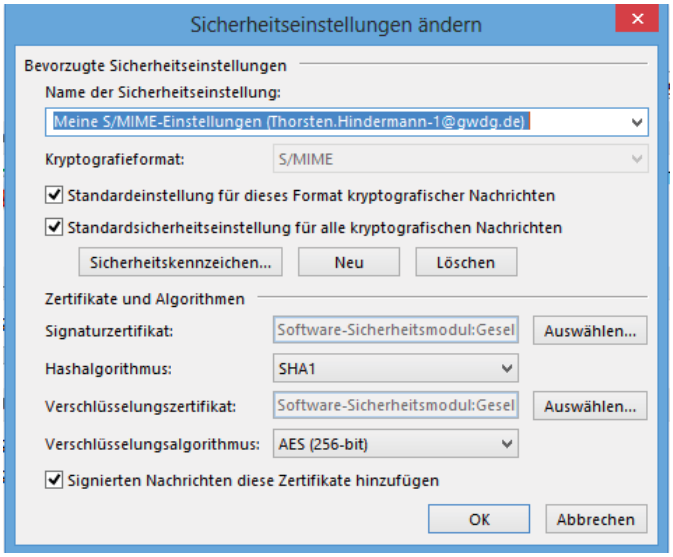


Abb. 31

Nun in der Gruppe „Digitale IDs (Zertifikate)“ die Schaltfläche „In GAL veröffentlichen...“ anklicken. Damit wird der öffentliche Schlüssel, wie im vorherigen Abschnitt beschrieben, aus dem persönlichen Windows-Zertifikatspeicher in das Active Directory exportiert bzw. gespeichert (s. Abb. 32).

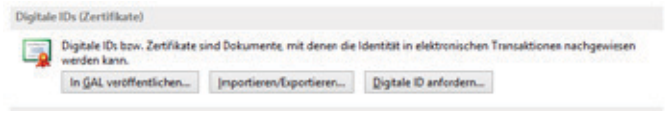


Abb. 32

Falls der folgende Warnhinweis erscheint, einfach auf „Ja“ klicken (s. Abb. 33).

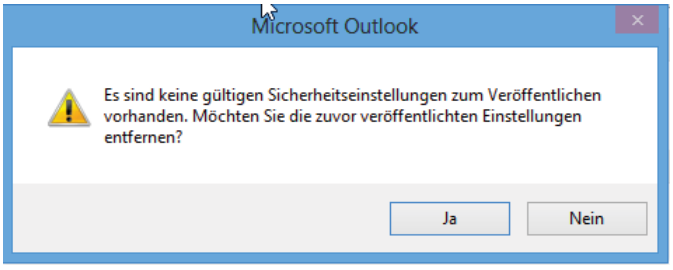


Abb. 33

Wenn der Vorgang erfolgreich abgeschlossen werden konnte, wird folgender Hinweis-Dialog angezeigt. Diesen mit einem Klick auf „OK“ bestätigen (s. Abb. 34).

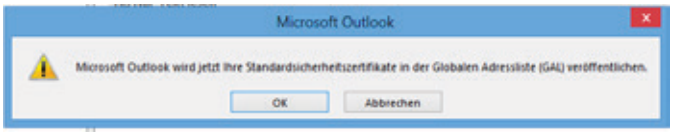


Abb. 34

Im Bestätigungsdialog auf „OK“ klicken (s. Abb. 35).

Abb. 35

Als Mailanhang

Der Zertifikatnehmer kann aber auch in eigener Verantwortung seinen öffentlichen Schlüssel verteilen, indem dieser entweder bei allen oder ausgewählten E-Mails mit versendet wird.

Outlook 2013 für Windows: Über „Datei|Optionen“ den „Outlook-Optionen“-Dialog öffnen. In der linken Navigationsspalte ganz unten auf „Trust Center“ anklicken.

Hinweis: Bei Outlook 2010 heißt „Outlook-Optionen“ nur „Optionen“ und „Trust Center“ heißt „Sicherheitscenter“.

Im Inhaltsfenster rechts nun ganz unten auf die Schaltfläche „Einstellungen für das Trust Center...“ klicken.

Der „Trust Center“-Dialog öffnet sich. In der linken Navigationsspalte auf „E-Mail-Sicherheit“ klicken.

Im Inhaltsfenster rechts hat es sich in der Praxis bewährt, zusätzlich zur angehakten dritten Möglichkeit auch die zweite auszuwählen (s. Abb. 36).

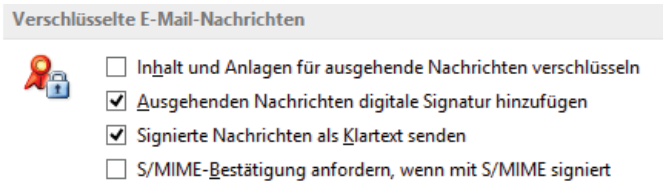


Abb. 36

Outlook 2011 für OS X: Über das Menü „Einstellungen...“ das Symbol „Konten“ oder über „Extras|Konten...“ anklicken.

Das entsprechende E-Mail-Konto auswählen, unten rechts auf „Erweitert...“ klicken und auf der mehrfach geteilten Schaltfläche auf „Sicherheit“ klicken (s. Abb. 37).

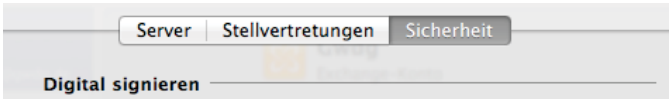


Abb. 37

Hier hat es sich in der Praxis bewährt, alle drei Möglichkeiten anzuhaken. Aber in diesem Absatz geht es ja um das Mitsenden des öffentlichen Schlüssels mit der E-Mail. Zu diesem Zweck den letzten Punkt auf alle Fälle anhaken (s. Abb. 38).

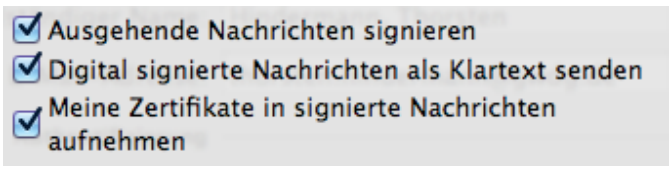


Abb. 38

E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 3: Outlook E-Mail-Anwendungen

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

In den ersten beiden Teilen dieses mehrteiligen Artikels wurden zunächst die Beantragung eines Zertifikats mit dem Webbrowser Firefox beschrieben, anschließend dann die Sicherung und der Import des Zertifikats in den Windows-Benutzer-Zertifikatspeicher, in die Mac-OS-X-Schlüsselbundverwaltung und in den E-Mail-Client Thunderbird. In diesem dritten Teil wird kurz der allgemeine Ablauf einer E-Mail-Signierung und -Verschlüsselung beschrieben, um dann darzustellen, wie Zertifikate für die Signierung/Verschlüsselung von E-Mails in Outlook 2013 für Windows, Outlook 2011 für Mac OS X und der Outlook Web App 2010 verwendet werden.

ALLGEMEINER ABLAUF EINER E-MAIL-SIGNIERUNG UND/ODER -VERSCHLÜSSELUNG

Bevor in diesem Teil und im späteren Teil 4 erklärt wird, wie mit heute aktuellen, gängigen E-Mail-Anwendungen E-Mails digital unterschrieben (signiert) und/oder verschlüsselt werden, sollen nachfolgend beide Verfahren kurz beschrieben werden.

Digitale Unterschrift (Signatur)

1. Der Anwender schreibt seine E-Mail.
2. Die E-Mail-Anwendung erzeugt, in einfachen Worten gesprochen, eine Prüfsumme (engl. message digest) über den Text der E-Mail.
3. Die Prüfsumme wird mit dem privaten Schlüssel des in der E-Mail-Anwendung eingestellten Signaturzertifikats verschlüsselt.
4. Die E-Mail mitsamt der verschlüsselten Prüfsumme werden an den Empfänger gesendet. **Anmerkung:** Bei der Signatur wird im Normalfall die eigentliche E-Mail in keiner Weise verschlüsselt. D. h. die E-Mail kann auf dem Weg von Alice zu Bob verändert werden. Aber jede Veränderung macht die ermittelte Prüfsumme ungültig!
5. Der Empfänger entschlüsselt die verschlüsselte Prüfsumme unter Verwendung des mitgesendeten öffentlichen Schlüssels des Signaturzertifikats vom Absender. **Hinweis:** Wenn der Sender der E-Mail ein Signatur-/Verschlüsselungszertifikat besitzt, werden je nach Einstellung in der E-Mail-Anwendung die jeweiligen öffentlichen Schlüssel in der E-Mail mit zum Empfänger gesendet.
6. Die E-Mail-Anwendung des Empfängers stellt dieselbe Berechnung zur Ermittlung der Prüfsumme über die empfangene E-Mail an.
7. Beide Prüfsummen werden verglichen. Sind beide Prüfsummen gleich, ist alles in Ordnung. Sollten sich die beiden Prüfsummen unterscheiden, gibt die E-Mail-Anwendung an den Empfänger eine entsprechende Warnung aus.

Verschlüsseln

1. Um die vom Sender geschriebene E-Mail zu verschlüsseln,

E-mail encryption using X.509 certificates - Part 3: Outlook e-mail applications

In the first two parts of this multi-part article first the application for a certificate using the web browser Firefox has been described, then the backup and import of the certificate into the Windows user certificate store, in the Mac OS X keychain and in the email client Thunderbird. In this third part the general flow of an e-mail signature and encryption is briefly described, and then we show how certificates for signing/encrypting of e-mail messages in Outlook 2013 for Windows, Outlook 2011 for Mac OS X and Outlook Web app 2010 can be used.

2. ermittelt/extrahiert die E-Mail-Anwendung des Senders den öffentlichen Schlüssel des Verschlüsselungszertifikats des Empfängers aus einem in der E-Mail-Anwendung angeschlossenem (z. B. Active Directory bei Outlook) oder angegebenen Verzeichnisdienst (z. B. den weiter oben beschriebenen DFN LDAP-Server) oder der Kontaktliste der E-Mail-Anwendung.
3. Nun erzeugt die E-Mail-Anwendung des Senders einen symmetrischen Schlüssel und benutzt diesen zum Verschlüsseln der E-Mail-Nachricht.
4. Der im vorherigen 3. Schritt erzeugte Schlüssel wird mit dem von der E-Mail-Anwendung im 2. Schritt ermittelten öffentlichen Schlüssels des Empfängers verschlüsselt.
5. Der nun verschlüsselte symmetrische Schlüssel aus dem 3. Schritt und die verschlüsselte E-Mail-Nachricht werden zum Empfänger gesendet.
6. Der Empfänger der E-Mail-Nachricht verwendet nun den eigenen privaten Schlüssel, um den im 3. Schritt erzeugten symmetrischen Schlüssel aus der empfangenen E-Mail zu entschlüsseln.
7. Die verschlüsselte E-Mail-Nachricht wird nun mit dem im 6. Schritt entschlüsselten symmetrischen Schlüssel entschlüsselt und kann nun vom Empfänger gelesen werden.

OUTLOOK

2013 für Windows

Wie das Zertifikat in den persönlichen Zertifikatspeicher von Windows importiert werden kann, wurde in einem Abschnitt weiter oben beschrieben.

Über „Datei > Optionen“ den „Outlook-Optionen“-Dialog öffnen. In der linken Navigationsspalte ganz unten auf „Trust Center“ klicken.

Hinweis: Bei Outlook 2010 heißt „Outlook-Optionen“ nur „Optionen“ und „Trust Center“ heißt „Sicherheitscenter“.

Im Inhaltsfenster rechts nun ganz unten auf die Schaltfläche „Einstellungen für das Trust Center...“ klicken.

Der „Trust Center“-Dialog öffnet sich. In der linken Navigationsspalte auf „E-Mail-Sicherheit“ klicken.

Im Inhaltsfenster rechts in der Gruppe „Verschlüsselte E-Mail-Nachrichten“ die Schaltfläche „Einstellungen...“ klicken und den angezeigten Dialog mit „OK“ bestätigen (s. Abb. 1).

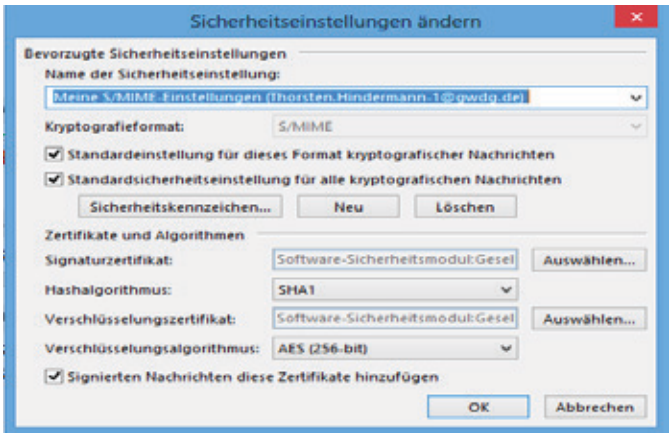


Abb. 1

Hinweis: Existiert zu diesem Zeitpunkt mehr als ein Zertifikat, dann jeweils unter Gruppe „Zertifikate und Algorithmen“ bei „Signaturzertifikat:“ und „Verschlüsselungszertifikat:“ jeweils neben dem Beschreibungsfeld auf die Schaltfläche „Auswählen...“ klicken und in dem jetzt präsentierten Dialog das für diesen Zweck entsprechende Zertifikat auswählen (s. Abb. 2).

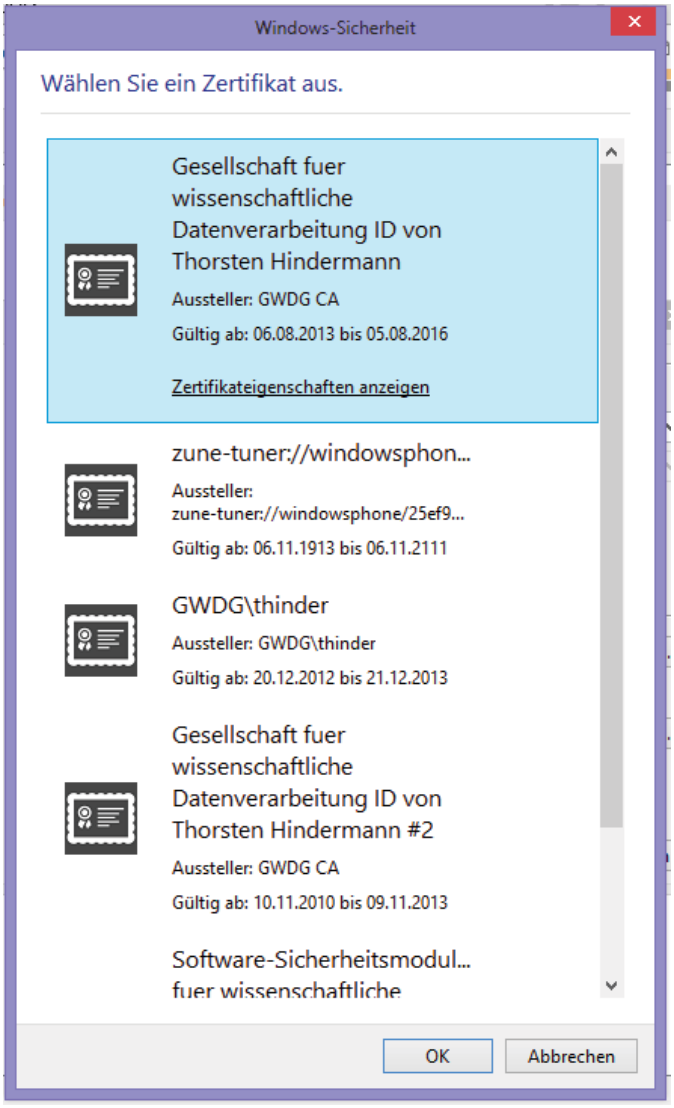


Abb. 2

Alle weiteren Auswahlmöglichkeiten so unverändert ausgewählt lassen und abschließend auf „OK“ klicken.

„OK“ klicken um den „Trust Center“-Dialog zu schließen und nochmals „OK“ klicken um den Dialog „Outlook-Optionen“ zu klicken.

Wenn nun auf eine E-Mail geantwortet oder eine neue E-Mail verfasst wird, kann wie folgt ermittelt werden, ob die E-Mail signiert und/oder verschlüsselt wird:

Im Menüband des E-Mail-Bearbeitungsfensters auf „Optionen“ klicken. In der Gruppe mit der Beschriftung „Berechtigung“ ist die Auswahlmöglichkeit „Signieren“ auf Grund der getroffenen Einstellungen standardmäßig eingeschaltet (s. Abb. 3).

Abb. 3

Eine farbige Hinterlegung der entsprechenden Möglichkeit zeigt an, ob die E-Mail signiert, verschlüsselt oder sogar beides wird (s. Abb. 4).

In der Grundeinstellung durchsucht Outlook

Abb. 4

naturgemäß das Active Directory nach einem passenden öffentlichen Schlüssel, wenn eine E-Mail-Nachricht verschlüsselt werden soll.

Soll nun aber der eingerichtete DFN LDAP-Verzeichnisserver nach einem passenden Schlüssel durchsucht werden, muss zu diesem Zweck links neben den entsprechenden Adressfeldern auf die „An...", „Cc..." oder, wenn diese Möglichkeit eingeschaltet wurde, „Bcc..." geklickt werden (s. Abb. 5).

Abb. 5

In dem Dialog die herunterklappbare Liste unter „Adressbuch" anklicken und unter Rubrik „Weitere Adressbücher" den Eintrag *ldap.pca.dfn.de* auswählen (s. Abb. 6).

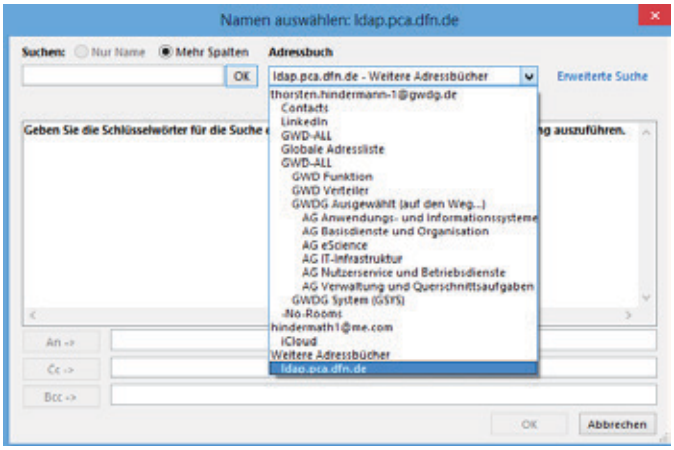


Abb. 6

Jetzt die Suche des E-Mail-Empfängers in diesem Verzeichnis durch Eingabe des Namens oder Bestandteil des Namens beginnen und mit einem Klick auf „OK" rechts neben dem Eingabefeld den Suchvorgang starten. Per Klick den/die Empfänger für die entsprechende Adresszeile „An...", „Cc..." oder „Bcc..." auswählen und den Dialog mit einem Klick auf „OK" abschließen (s. Abb. 7).

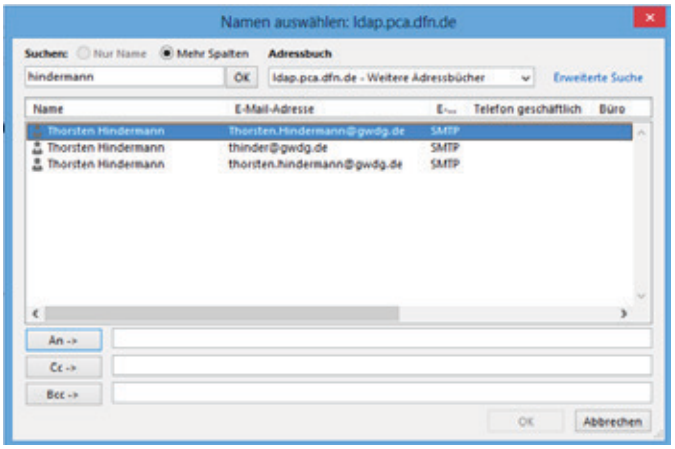


Abb. 7

2011 für Mac OS X

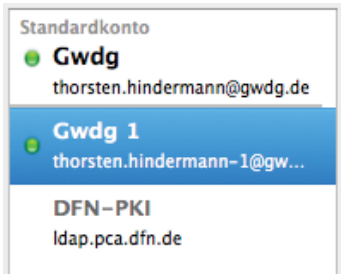


Abb. 8

Wie das Zertifikat in die Schlüsselbundverwaltung von Mac OS X importiert werden kann, wurde in einem Abschnitt weiter oben beschrieben. Die Einstellungen über „Outlook > Einstellungen..." aufrufen und auf das Symbol „Konten" klicken. Sind mehrere E-Mail-Konten konfiguriert, wählt der Anwender das Konto aus, mit dem eine E-Mail versendet werden soll (s. Abb. 8).

In dem rechts angezeigten Bereich für die allgemeinen Einstellungen zum verwendeten E-Mail-Konto nun auf „Erweitert..." klicken.

In dem jetzt erscheinenden Dialog auf der mehrfach geteilten Schaltfläche auf „Sicherheit" klicken.

Unter der Gruppe „Digital signieren" auf die Auswahlliste mit der links stehenden Beschriftung „Zertifikat:" klicken und das entsprechende Signaturzertifikat aus der Liste mit einem Klick auswählen (s. Abb. 9).

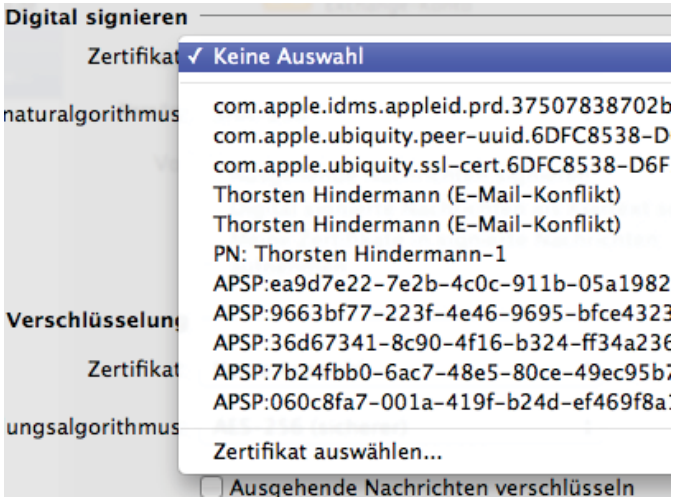


Abb. 9

Hinweis: Enthält die Liste viele gleichnamige Zertifikate, einfach am Ende der Liste auf „Zertifikat auswählen" klicken. In dem erscheinenden Dialog auf die Schaltfläche „Zertifikat einblenden" klicken und anhand der erweiterten Informationen das richtige Zertifikat auswählen und mit einem Klick auf „OK" bestätigen (s. Abb. 10 und 11).

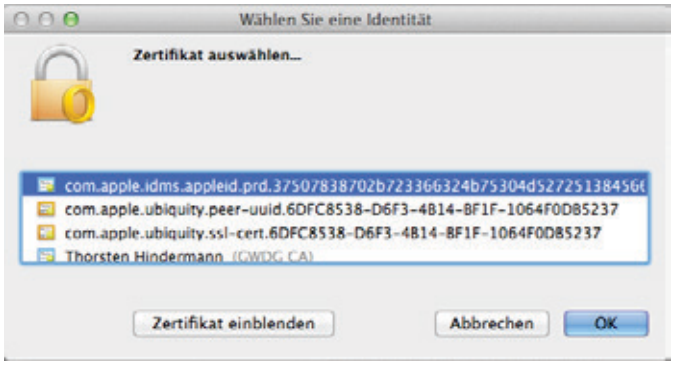


Abb. 10

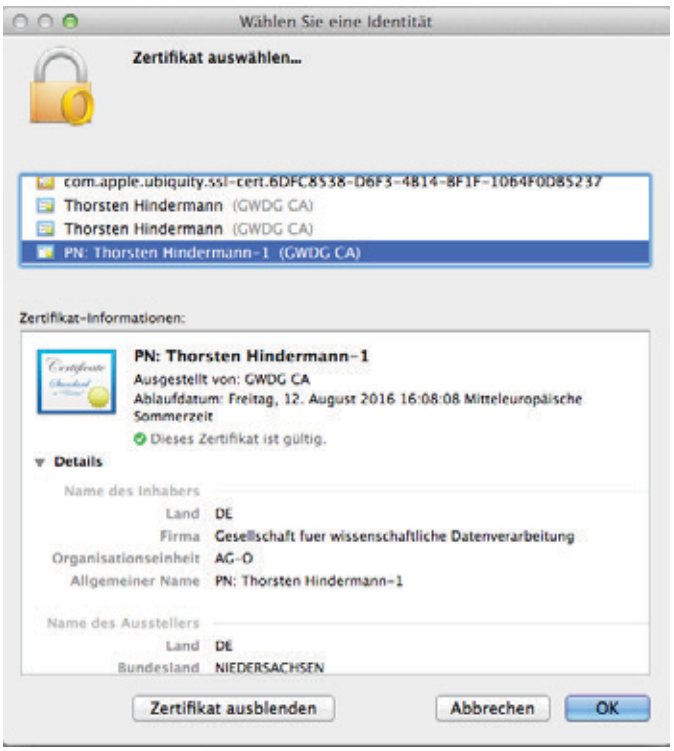


Abb. 11

Für die Gruppe „Verschlüsselung" das gleiche Verfahren zur Auswahl des Verschlüsselungszertifikats anwenden. Nachdem nun beide Zertifikate für digitale Signatur und Verschlüsselung ausgewählt worden sind, sieht der Dialog nun wie folgt aus und kann mit einem Klick auf „OK" bestätigt werden (s. Abb. 12).

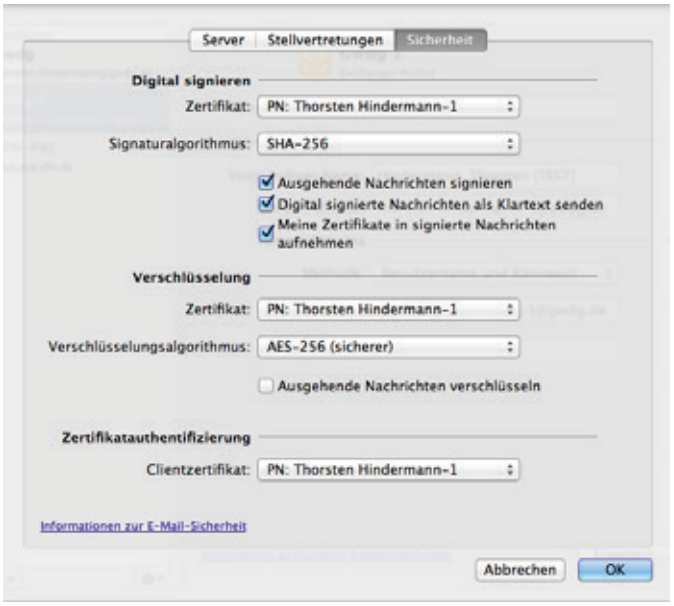


Abb. 12

Wenn nun auf eine E-Mail geantwortet oder eine neue E-Mail verfasst wird, kann wie folgt ermittelt werden, ob die Mail signiert und/oder verschlüsselt wird:

Im Menüband des E-Mail Bearbeitungsfensters auf „Optionen" klicken, hier dann auf das Symbol mit der Beschriftung „Sicherheit" klicken. Es erscheint eine Auswahlliste der beiden Auswahlmöglichkeiten. Ein Haken neben der entsprechenden Möglichkeit zeigt an, ob die E-Mail signiert, verschlüsselt oder sogar beides wird (s. Abb. 13).

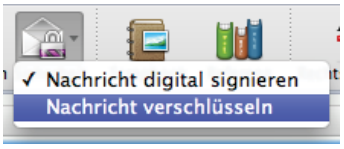


Abb. 13

In der Grundeinstellung durchsucht Outlook naturgemäß das Active Directory nach einem passenden öffentlichen Schlüssel, wenn eine E-Mail-Nachricht verschlüsselt werden soll.

Abb. 14

Soll nun aber der eingerichtete DFN LDAP-Verzeichnisserver nach einem passenden Schlüssel durchsucht werden, muss zu diesem Zweck rechts neben den entsprechenden Adressfeldern auf das „Kontakte"-Symbol geklickt werden (s. Abb. 14).

Unter dem Suchfeld für den passenden E-Mail-Empfänger muss zunächst der vorher eingerichtete DFN LDAP-Verzeichnisserver mit der Beschriftung „DFN-PKI Verzeichnis" ausgewählt werden.

Jetzt den E-MailEmpfänger in diesem Verzeichnis durch Eingabe des Namens oder Bestandteil des Namens suchen und per Klick den/die Empfänger für die entsprechende Adresszeile (An, Cc oder Bcc) auswählen (s. Abb. 15).

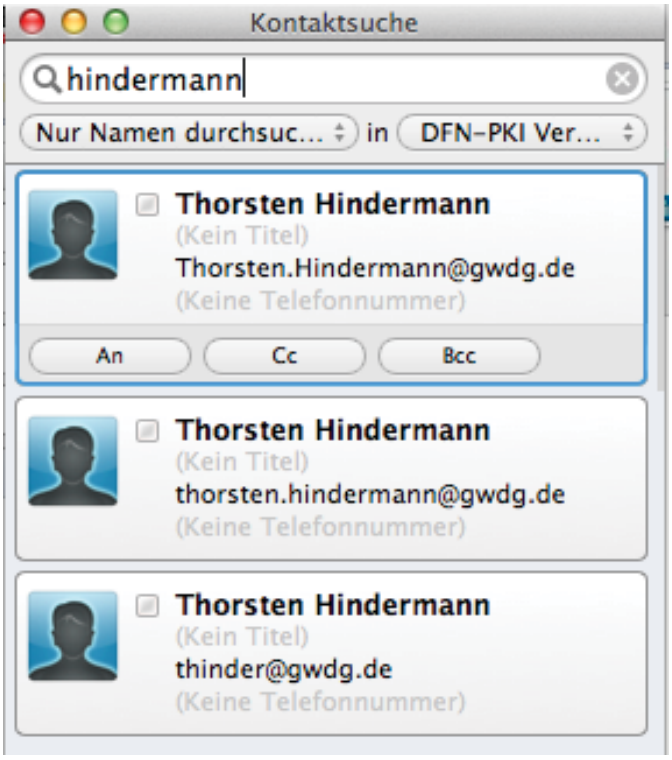


Abb. 15

Outlook Web App 2010

E-Mail-Nachrichten in der Outlook Web App des Microsoft Exchange 2010 Servers, im Folgenden kurz OWA genannt, zu signieren/verschlüsseln funktioniert derzeit nur mit dem Internet Explorer (im Folgenden kurz IE genannt). Derzeit ist nur der IE in der Lage, ActiveX-Steuerelemente auszuführen. Mit dieser Einschränkung geht einher, dass diese Möglichkeit derzeit nur unter Windows funktioniert. Als erstes muss der Anwender überprüfen, ob das ActiveX-Steuerelement installiert ist. Dazu im OWA auf „Optionen > Alle Optionen anzeigen..." klicken (s. Abb. 16).

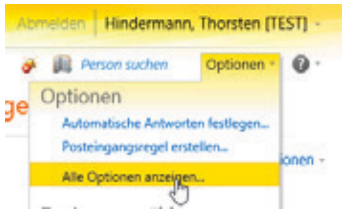


Abb. 16

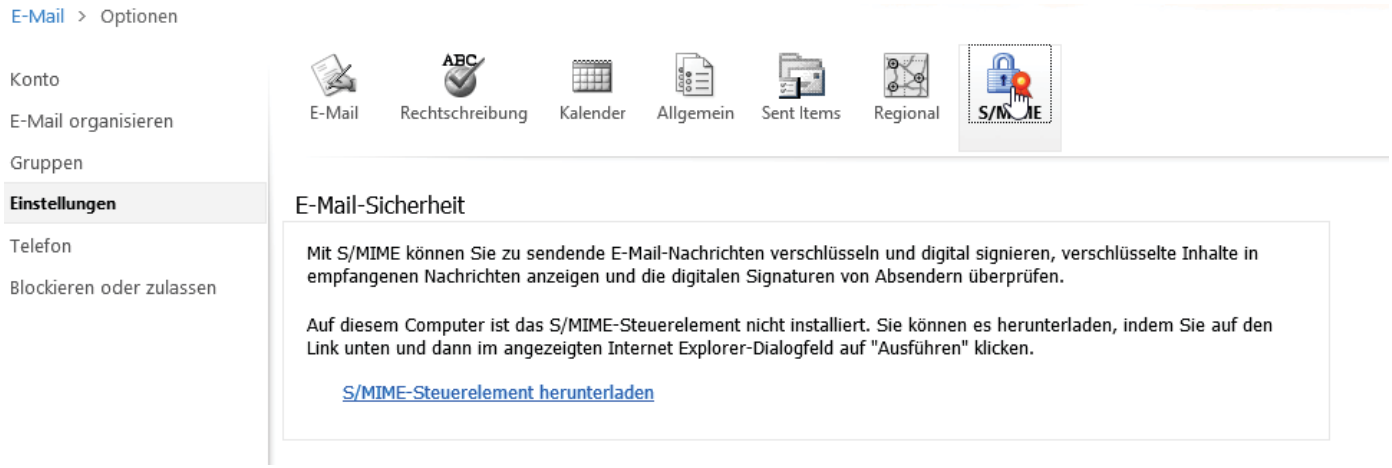


Abb. 17

In der Navigationsspalte links den Eintrag „Einstellungen“ anklicken. Im Inhaltsfenster rechts dann auf das Symbol mit dem Untertitel „S/MIME“ klicken. Wenn dann im Inhaltsfenster folgender Text (s. Abb. 17) zu lesen ist und der entsprechende Link zum Herunterladen der Steuerelemente-Installationsdatei angezeigt wird (wie in der Abb. zu sehen), muss die heruntergeladene *owasmime.msi*-Datei noch von einem Systemverwalter installiert werden.

Hinweis: Für Outlook Web Access 2003/2007 besteht ebenfalls diese Möglichkeit. In diesen Versionen sehen die Dialog/Webseiten zwar anders aus, aber auch mit diesen Web-Anwendungen können E-Mails signiert/verschlüsselt werden.

Da die Steuerelemente-Installationsdatei das .MSI-Paketformat hat, ist es in einem Active-Directory-Verzeichnis möglich, dieses Steuerelement per Softwareverteilungs-Gruppenrichtline auf entsprechende Windows-Systeme automatisiert zu verteilen.

Nachdem das Steuerelement erfolgreich installiert worden ist, sollte nun die S/MIME-Inhaltsseite wie folgt (s. Abb. 18) aussehen. In der Praxis hat es sich bewährt, wenn die Auswahlmöglichkeiten wie im Bild angezeigt voreingestellt wurden.

Abb. 18

Mit dem Verweis „Zertifikat für die Nachrichtensignierung auswählen“ wird nun das vorher installierte Zertifikat im persönlichen Windows-Zertifikatspeicher ausgewählt. Dazu auf den Verweis klicken und die Auswahl „Zertifikat manuell auswählen“ anklicken. Nun auf „Signaturzertifikat auswählen...“ klicken (s. Abb. 19).

Im angezeigten Dialog das vorher installierte Zertifikat auswählen und auf „OK“ klicken (s. Abb. 20).

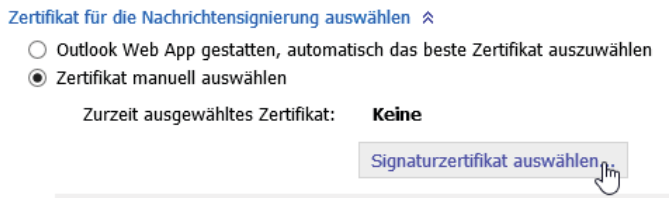


Abb. 19

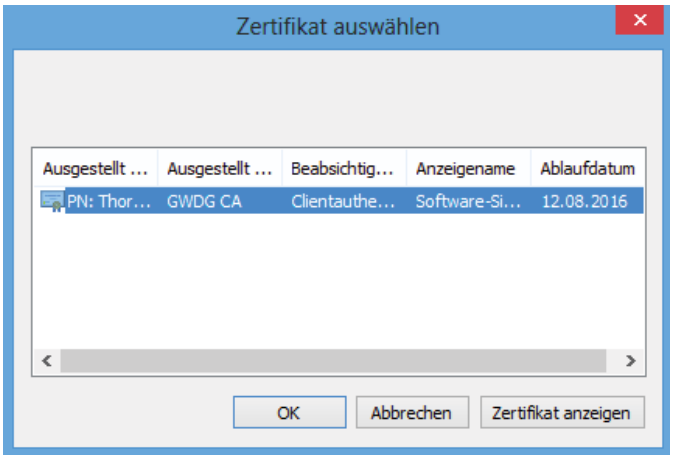


Abb. 20

Wenn alle Voreinstellungen getroffen sind, auf der Webseite unten rechts auf „Speichern“ klicken.

Abb. 21

Nachdem diese Vorarbeit geleistet ist, wird nun jede E-Mail signiert versendet; zu erkennen am Symbol im folgenden Bild (s. Abb. 21).

Soll die E-Mail nun zusätzlich noch verschlüsselt versendet werden, einfach auf das Symbol daneben klicken (s. Abb. 22).

Abb. 22

E-Mail-Verschlüsselung mit X.509-Zertifikaten – Teil 4: Apple E-Mail-Anwendungen, Thunderbird und Notes

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

In den ersten beiden Teilen wurde beschrieben, wie X.509-Zertifikate beantragt, gesichert und installiert werden. Im dritten Teil wurde mit den Microsoft Outlook E-Mail-Anwendungen gezeigt, wie E-Mails signiert und/oder verschlüsselt werden. Im vierten und letzten Teil wird nun auch für OS X Mail.app, iOS Mail.app, Thunderbird und IBM Notes beschrieben, wie mit diesen Anwendungen E-Mails signiert und/oder verschlüsselt werden.

MAIL.APP OS X 6.5

Wie das Zertifikat in die Schlüsselbundverwaltung von OS X importiert werden kann, wurde in einem Abschnitt weiter oben beschrieben (s. Teil 2 in den GWDG-Nachrichten (10/2013, S. 12). Sind mehrere E-Mail-Konten in der Mail.app konfiguriert, wählt der Anwender das Konto aus, mit dem eine E-Mail versendet werden soll. In der Konfiguration für das E-Mail-Konto ist ja auch eine E-Mail-Adresse enthalten. Findet die E-Mail.app kein passendes Zertifikat, dass die E-Mail-Adresse des aktuell ausgewählten E-Mail-Kontos enthält, werden die Möglichkeiten der E-Mail-Signierung/Verschlüsselung nicht freigeschaltet (s. Abb. 1).


Abb. 1

Stimmt hingegen die E-Mail-Adresse des aktuell ausgewählten E-Mail-Kontos mit der E-Mail-Adresse in einem importierten Zertifikat in der Schlüsselbundverwaltung überein, dann wird die Auswahlmöglichkeit für die E-Mail-Signatur freigeschaltet (s. Abb. 2).


Abb. 2

Sind die Voraussetzungen aus dem vorherigen Absatz erfüllt und hat die Mail.app für den in der E-Mail angegebenen E-Mail-Empfänger zusätzlich auch noch die Informationen über dessen öffentlichen Schlüssel, so werden beide Möglichkeiten, E-Mail-Signierung/Verschlüsselung, freigeschaltet (s. Abb. 3).


Abb. 3

Sind beide Möglichkeiten für die aktuelle E-Mail eingeschaltet, sehen die beiden Symbole wie in diesem Bild gezeigt aus (s. Abb. 4).


Abb. 4

Wird nun der öffentliche Schlüssel eines E-Mail-Empfängers für die Verschlüsselung einer E-Mail gebraucht, der diesen im DFN LDAP-Verzeichnisdienst veröffentlicht hat, sucht die Mail.app automatisch in dem vorher eingerichteten DFN LDAP-Verzeichnisdienst nach einer passenden Names- oder E-Mail-Adressen-Übereinstimmung und zeigt diese automatisch an (s. Abb. 5).

Abb. 5

MAIL.APP IOS 6.1.X

Hinweis: Die hier gezeigten Bildschirmfotos und Anweisungen sind mit einem iPad erstellt worden. Auf einem iPhone/iPod sind diese Schritte nahezu identisch und unterliegen, bedingt durch die Bauart, nur geringen Abweichungen.

E-mail encryption using x.509 certificates – Part 4: Apple e-mail applications, Thunderbird and Notes

The first two parts have described, how X.509 certificates will be requested, secured and installed. The third part has shown with the Microsoft Outlook e-mail applications, how e-mails will be signed and/or encrypted. In the fourth and final part it will be described how you can sign and/or encrypt e-mails with the applications OS X Mail.app, iOS Mail.app, Thunderbird and IBM Notes.

Im einfachsten Fall schickt sich der Anwender an sein eigenes Postfach (z. B. Exchange) eine E-Mail mit dem Zertifikat im Anhang, das ja, wie weiter oben beschrieben (s. Teil 1 in den GWDG-Nachrigen 9/2013, S. 6) als .P12-Datei vorliegt. Nach der Installation des Zertifikats auf dem iOS-Gerät sollte die E-Mail wieder gelöscht werden (s. Abb. 6).

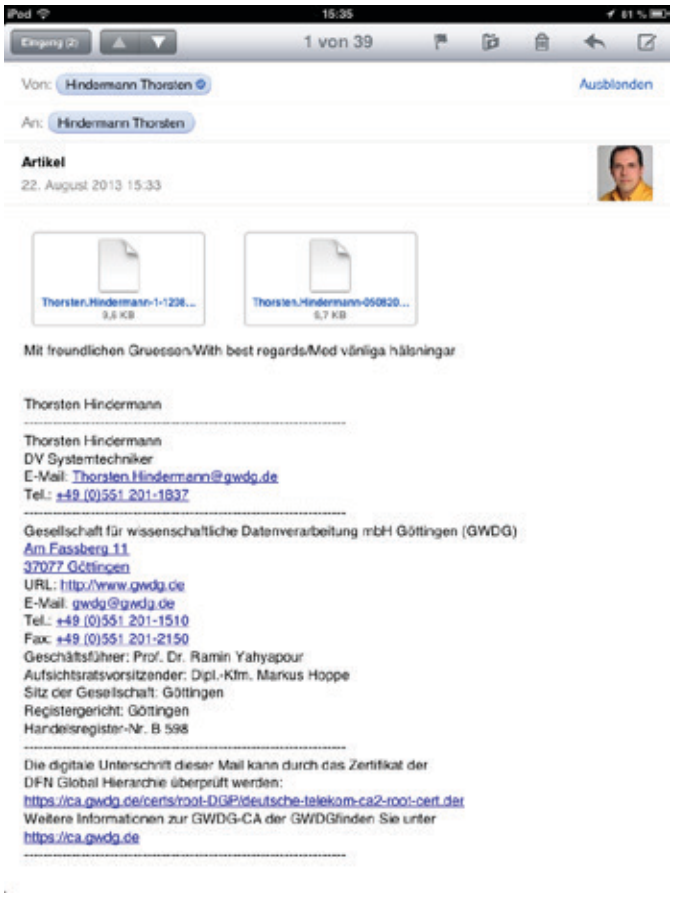


Abb. 6

Als erster Schritt steht der Besuch der Webseite *http://www.gwdg.de/index.php?id=1744* auf dem Programm. Hier bitte die Seite soweit hochstreichen, bis die Überschrift „Wurzelzertifikat“ erscheint. Den Link „.DER“ in diesem Abschnitt antippen. Das Betriebssystem wechselt selbstständig zum „Profil installieren“ in den Einstellungen. In dem Dialog auf die Schaltfläche „Installieren“ tippen. Es erscheint ein weiterer Hinweis; hier ebenfalls auf die Schaltfläche „Installieren“ tippen. Nun in der Dialog-Kopfzeile rechts auf die blaue Schaltfläche „Fertig“ tippen. Das iOS-Betriebssystem wechselt automatisch wieder zurück zur Ausgangswebseite (s. Abb. 7 und 8).

Nun zur Überschrift „DFN-PCA“ weiter hochstreichen. Auch hier den Link „.DER“ antippen und die gleiche Prozedur, wie vorangegangen beschrieben, durchführen.

Jetzt muss der Anwender auswählen, in welcher Gesellschaft er beheimatet ist: Max-Planck-Gesellschaft oder Universität Göttingen. Dementsprechend unter den genannten Überschriften den entsprechenden Link „.DER“ antippen und die oben beschriebene Prozedur wiederholen.

Jetzt das in der E-Mail an sich selbst gesendete Zertifikat antippen. Auch hier wechselt das iOS-Betriebssystem automatisch zu „Profil installieren“ in den „Einstellungen“. Hier wiederum auf die Schaltfläche „Installieren“ tippen. Es erscheint wieder ein

Abb. 7

Abb. 8

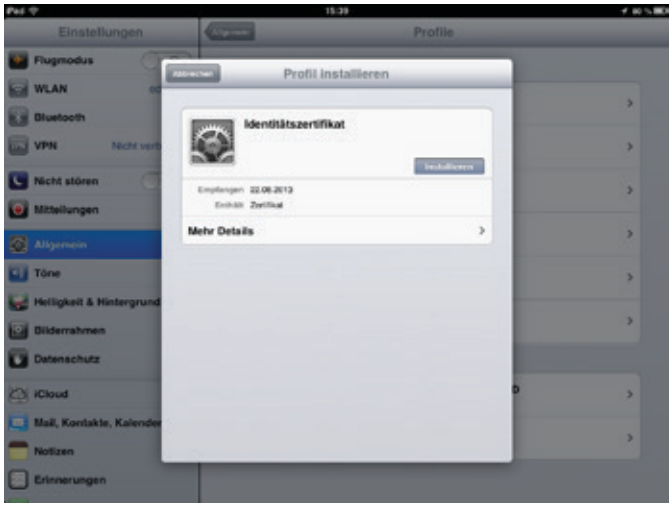


Abb. 9

Hinweis, auch hier wieder auf die Schaltfläche „Installieren“ tippen (s. Abb. 9 und 10).

Nun wird zur Eingabe des Kennworts aufgefordert, mit der die Sicherungsdatei des Zertifikats verschlüsselt worden ist. Nachdem das Kennwort eingegeben worden ist, in der Kopfzeile des Dialogs rechts auf die blaue Schaltfläche „Weiter“ tippen (s. Abb. 11).

In der jetzt erscheinenden Bestätigungsseite des Dialogs in

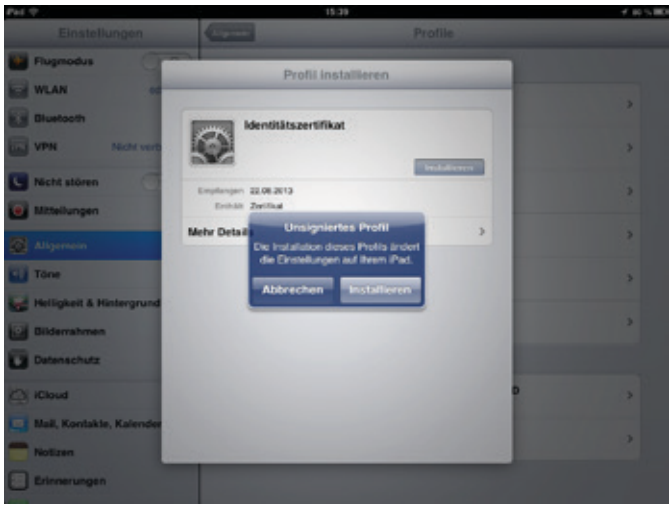


Abb. 10

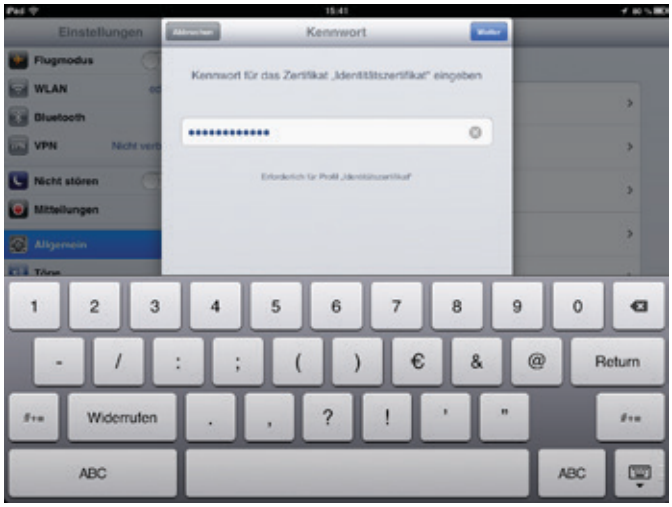


Abb. 11

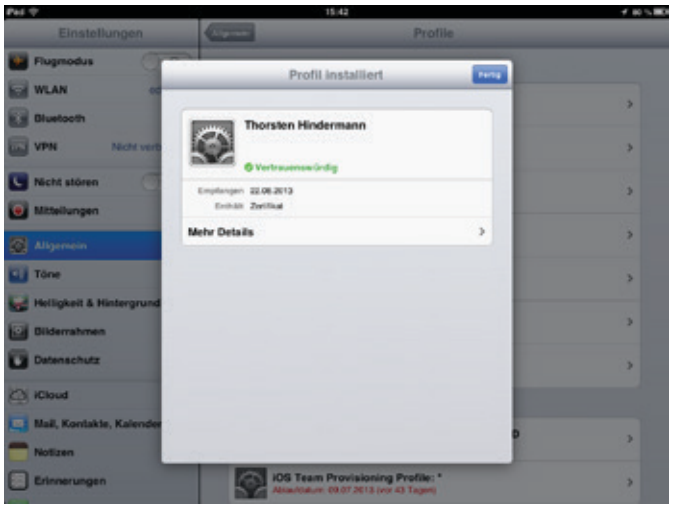


Abb. 12

der Kopfzeile rechts auf die blaue Schaltfläche „Fertig" tippen. Das Betriebssystem wechselt automatisch wieder zurück in die E-Mail. app (s. Abb. 12).

Jetzt muss noch die Verwendung des Zertifikats eingerichtet werden. Dazu in die betriebssystem-integrierte Anwendung (engl. kurz App) „Einstellungen" wechseln (s. Abb. 13).

Hierzu links in der Navigationsspalte auf „E-Mail, Kontakte, Kalender" tippen und rechts in der Inhaltsspalte das entsprechende

Abb. 13

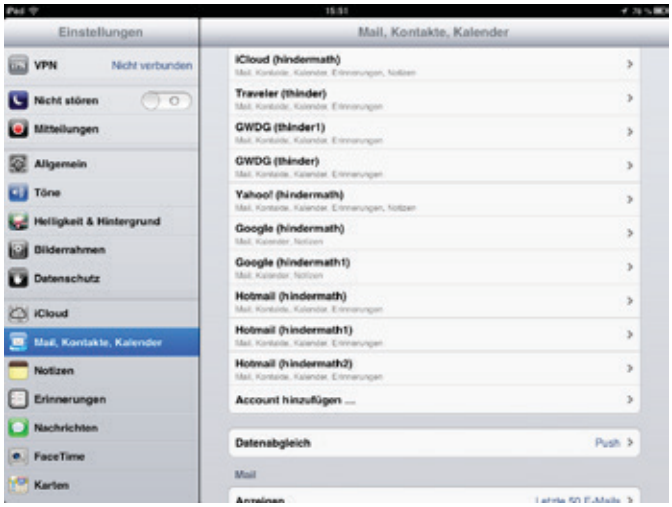


Abb. 14

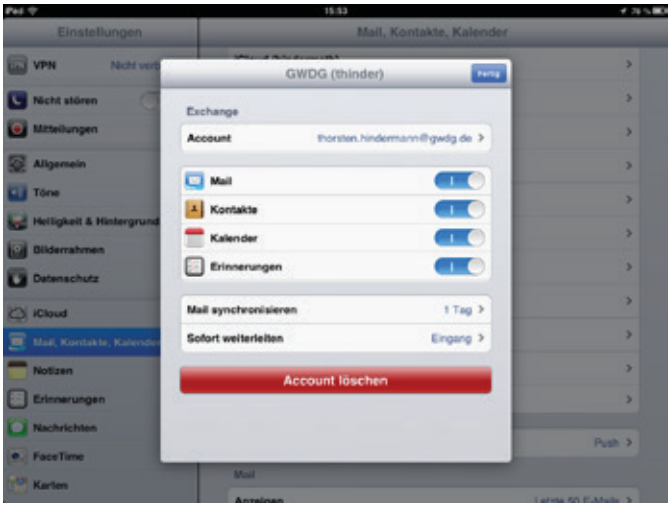


Abb. 15

Postfach antippen (s. Abb. 14).

In dem nun erscheinenden Dialog auf die Schaltfläche „Account vorname.nachname@domain.de >" tippen (s. Abb. 15).

In der aktuellen Dialogseite in der Gruppe „S/MIME" den Schalter im Gruppenelement „S/MIME" durch einen Fingerstrich nach rechts in die Stellung „Einschalten" bringen (s. Abb. 16).

Nun auf das Gruppenelement „Signieren Nein >", das gleichzeitig eine Schaltfläche ist, tippen. In der dann erscheinenden

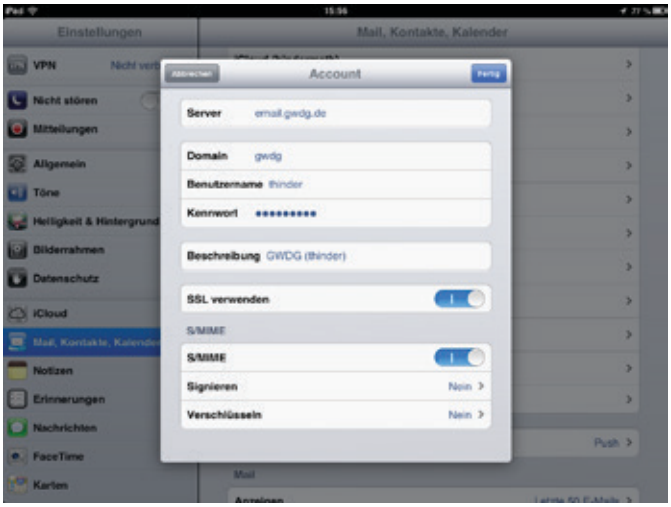


Abb. 16

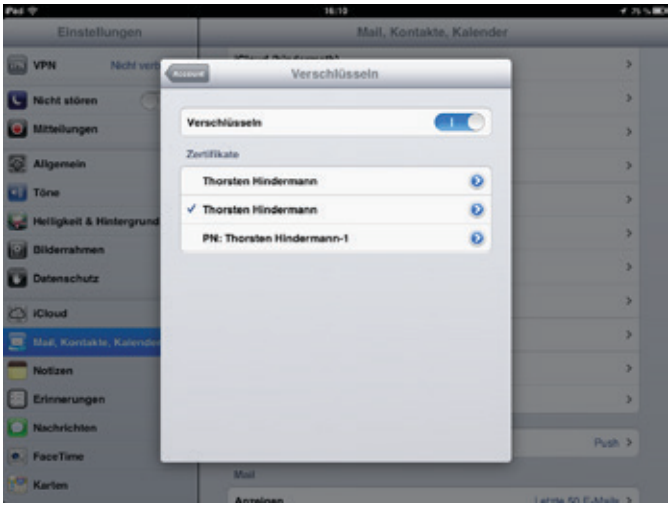


Abb. 18

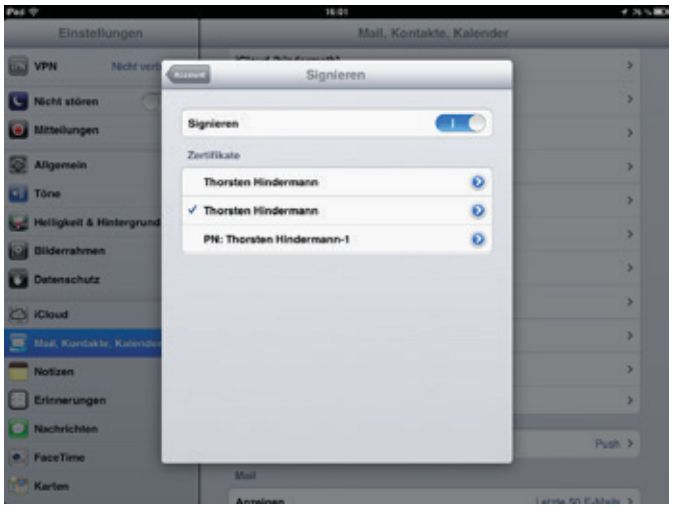


Abb. 17

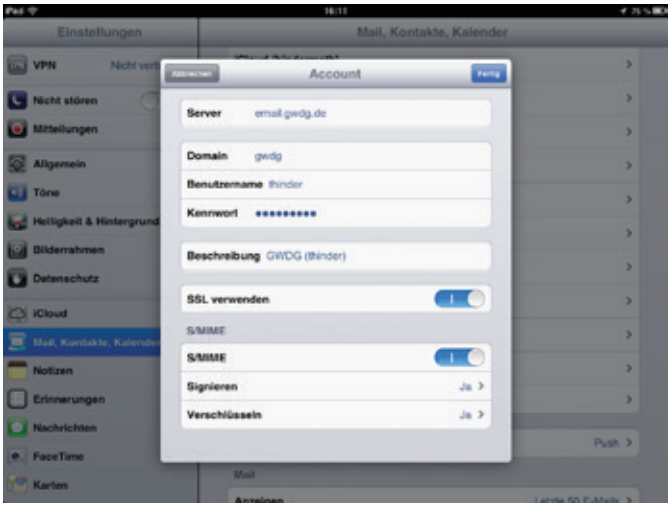


Abb. 19

Dialogseite „Signieren“ den Schalter im Element „Signieren“ durch einen Fingerstrich nach rechts in die Stellung „Einschalten“ bringen (s. Abb. 17).

Jetzt das gerade installierte Zertifikat durch Antippen auswählen. Nach der Wahl kann in der Dialog-Kopfzeile links auf „Account“ getippt werden. Leider kann bis zur iOS-Betriebssystemversion 6.1.3 beim Verfassen einer E-Mail nicht gewählt werden, ob die E-Mail verschlüsselt werden soll oder nicht. Wenn nun gewünscht wird, das eine oder mehrere E-Mails das mobile Gerät verschlüsselt verlassen sollen, dann muss wieder zu dieser Stelle zurückgekehrt werden und zusätzlich das Gruppenelement „Verschlüsseln Nein >“, das ebenfalls gleichzeitig eine Schaltfläche ist, angetippt werden. In der nun erscheinenden Dialogseite „Verschlüsseln“ den Schalter im Element „Verschlüsseln“ durch einen Fingerstrich nach rechts in die Stellung „Einschalten“ bringen.

Jetzt das gerade installierte Zertifikat durch Antippen auswählen. Nach der Wahl kann in der Dialog-Kopfzeile links auf „Account“ getippt werden (s. Abb. 18).

Sind alle Einstellungen getätigt, dann in der Dialog-Kopfzeile „Account“ rechts auf die blaue Schaltfläche „Fertig“ tippen. Und dann noch einmal auf die blaue Schaltfläche „Fertig“ in der Dialog-Kopfzeile „<Bezeichnung des ausgewählten E-Mail-Accounts>“ tippen (s. Abb. 19).

Ab diesem Zeitpunkt werden alle E-Mail-Nachrichten signiert und/oder verschlüsselt versendet, entsprechend der gerade

Abb. 20

getroffenen/eingestellten Auswahl. Werden E-Mails nur signiert, unterscheidet sich der E-Mail-Verfassen-Dialog nicht weiter von dem Dialog ohne E-Mail-Signierung. Ist nun die E-Mail-Verschlüsselung eingeschaltet und es wird ein Empfänger ausgewählt, mit dem verschlüsselte E-Mails ausgetauscht werden können, dann sieht der Dialog folgendermaßen aus (s. Abb. 20).

Die angekommene E-Mail in diesem Bild ist signiert und verschlüsselt (s. Abb. 21).

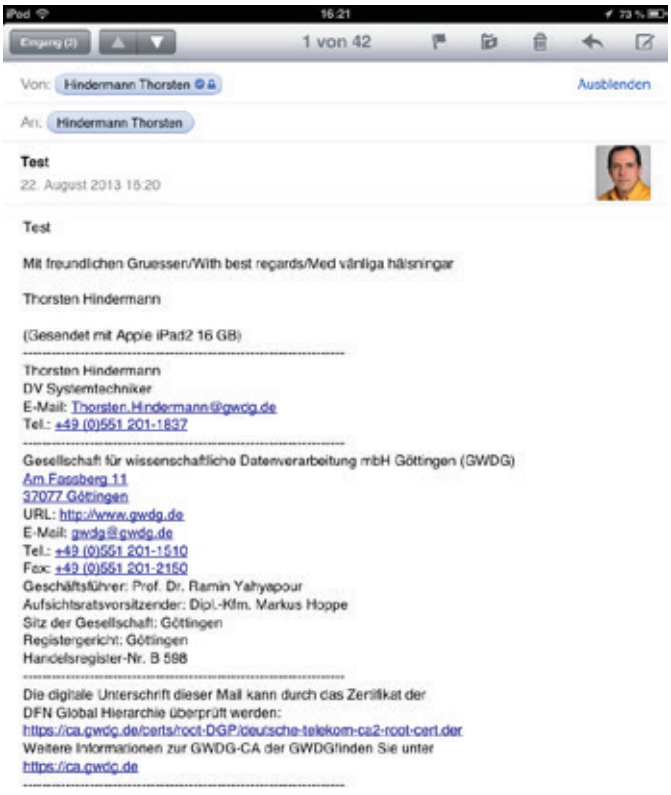


Abb. 21

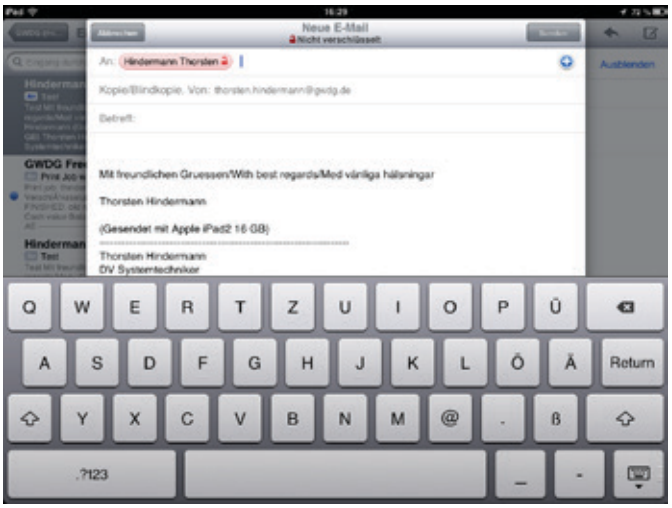


Abb. 22

Stellt die E-Mail.app fest, dass mit dem Empfänger E-Mails nicht verschlüsselt ausgetauscht werden können, wird in roter Farbe nebst passendem Symbol angezeigt, dass die E-Mail zu diesem Empfänger nicht verschlüsselt versendet wird (s. Abb. 22).

Wenn ein E-Mail-Empfänger mehr über das Zertifikat einer eingegangenen E-Mail wissen möchte, muss dieser einfach den E-Mail-Sendernamen in der „Von:"-Zeile antippen. In dem nun angezeigten überlagernden Dialog „Absender" auf die Schaltfläche „Zertifikat anzeigen" tippen. Jetzt kann sich der Empfänger den öffentlichen Schlüssel des Senders mit einem Antippen auf die Schaltfläche „Installieren" auf sein Gerät speichern. Sollen weitere Informationen des Senderzertifikats angezeigt werden, nun auf die Schaltfläche „Weitere Details >" tippen und dort die oberste Schaltfläche „Name des Zertifikatinhabers >" antippen. Einzelheiten des Senderzertifikats werden angezeigt (s. Abb. 23 bis 26).

Abb. 23

Abb. 24

Abb. 25

THUNDERBIRD VERSION 17

Wie das Zertifikat in den Zertifikatspeicher von Thunderbird importiert werden kann, wurde in einem Abschnitt weiter oben beschrieben (s. Teil 2 in den GWDG-Nachrichten 10/2013, S. 12).

Nun den Menüeintrag „Extras > Konten-Einstellungen..." anklicken. Wenn mehrere E-Mail-Konten eingerichtet sind, das

Abb. 26

entsprechend zu konfigurierende E-Mail-Konto in der Navigationsspalte links auswählen. In den dort aufgelisteten Untereinträgen zu dem Konto „S/MIME-Sicherheit" anklicken. Um nun für die digitale Unterschrift (Signierung) ein Zertifikat zu bestimmen, auf die Schaltfläche „Auswählen..." in der Gruppe „Digitale Unterschrift" klicken (s. Abb. 27)

Abb. 27

und in dem jetzt angezeigten Dialog das vorher importierte Zertifikat auswählen. Wenn bisher keine Zertifikate für die Signierung/Verschlüsselung angegeben wurden, bietet Thunderbird nun an, das Signaturzertifikat auch für die Verschlüsselung zu verwenden. An dieser Stelle auf „Ja" klicken. Wenn gewünscht, noch die Auswahlmöglichkeit „Nachrichten digital unterschreiben (als Standard)" auswählen, damit alle E-Mails von nun an signiert, also digital unterschrieben, versendet werden (s. Abb. 28).

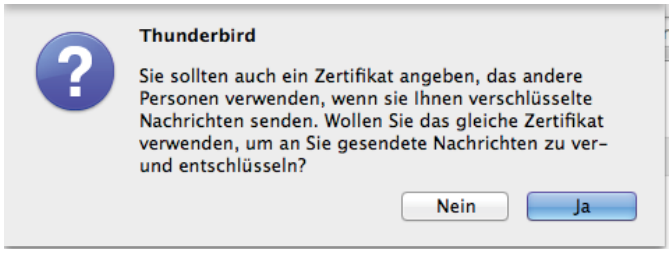


Abb. 28

Nachdem alle Einstellungen für das entsprechend ausgewählte

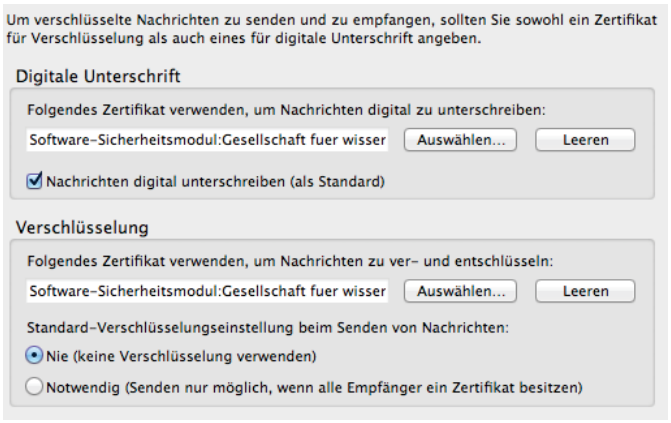


Abb. 29

E-Mail-Konto getroffen worden sind, sieht der fertig ausgefüllte Dialog wie folgt aus (s. Abb. 29).

Anmerkung: Soll ein anderes Zertifikat zur Verschlüsselung von E-Mails genommen werden, in der Gruppe „Verschlüsselung" auf die Schaltfläche „Auswählen..." klicken und das entsprechende Zertifikat auswählen und „OK" klicken.

Wenn nun auf eine E-Mail geantwortet wird oder gar eine neue E-Mail verfasst wird, die entsprechende Aktion in Thunderbird ausführen. In dem neu erscheinenden Bearbeitungsfenster für die E-Mail auf den Menüeintrag „Ansicht" klicken. Ist ein Haken neben der „Kontakte-Sidebar" sichtbar, ist dieser Bereich links neben dem Bearbeitungsbereich zu sehen. Falls der Haken noch nicht gesetzt ist, einfach auf „Kontakte-Sidebar" klicken (s. Abb. 30).

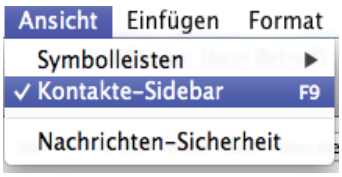


Abb. 30

Über den Menüeintrag „Optionen" ist es nun möglich, die Auswahl zu treffen, ob die E-Mail digital unterschrieben und noch zusätzlich verschlüsselt werden soll. Um diese Auswahlmöglichkeiten ein und auszuschalten, in dem Optionen-Menü „Nachricht unterschreiben" bzw. „Nachricht verschlüsseln" anklicken. Ist die Auswahl aktiv, ist daneben ein Haken zu sehen, andernfalls ist diese Möglichkeit deaktiviert. Optisch sind zusätzlich in der Statuszeile im Bearbeitungsfenster noch zwei Symbole zu sehen oder auch nicht, je nach Auswahl (s. Abb. 31 und 32).

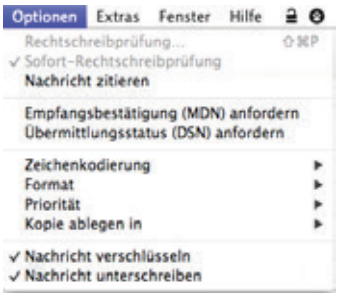


Abb. 31

Abb. 32

Wird nun der öffentliche Schlüssel eines E-Mail-Empfängers für die Verschlüsselung einer E-Mail gebraucht, der diesen im DFN LDAP-Verzeichnisdienst veröffentlicht hat, in der Kontakte-Seitenspalte unter „Adressbuch:" den zuvor eingerichteten Eintrag „DFN-PKI" auswählen. Wahlweise im Eingabefeld für die „Suche nach:"

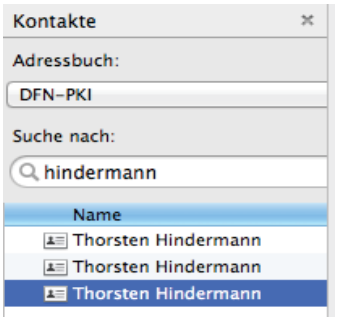


Abb. 33

den Namen oder die E-Mail-Adresse des E-Mail-Empfängers eingeben. Wird dieser angezeigt, entsprechend anklicken und im unteren Bereich auswählen, ob der Eintrag „An:", „Kopie (CC):" oder „Blindkopie (BCC):" verwendet werden soll (s. Abb. 33).

IBM NOTES 9

E-Mail signieren

Im eigenen Postfach eine neue E-Mail beginnen. Minimum: Empfänger-E-Mail-Adresse und einen Test eingeben. Im einfachsten Fall die vier magischen Buchstaben „Test".

Über dem Eingabefeld für die Empfänger auf „Zustelloptionen..." klicken (s. Abb. 34).

Abb. 34

In dem daraufhin erscheinenden Dialogfeld darauf achten, dass das Häkchen bei „Signieren" angehakt ist (s. Abb. 35).

Abb. 35

Weiterhin wird unter dem Eingabefeld für den Betreff auch noch der Hinweis in Grau in kleiner Schrift angezeigt (s. Abb. 36).

Abb. 36

Aufgrund der Einstellungen unter den Sicherheitseinstellungen sollte dieser Haken nun im Standard für jede ausgehende E-Mail gesetzt sein. Nun nur noch auf „Sende" klicken. Damit wird die Internet-E-Mail mit einer X.509-Signatur aus Lotus Notes an den Empfänger gesendet.

E-Mail verschlüsseln

Um eine E-Mail verschlüsselt an einen Empfänger zu senden, muss als erstes der öffentliche Schlüssel des Empfängers in das Notes-Adressbuch importiert werden.

Dazu im Arbeitsbereich auf das Adressbuch doppelt klicken und dann auf dem Registerreiter „Kontakt suchen..." in der Adressbuchansicht „Meine Kontakte" klicken (s. Abb. 37).

Abb. 37

Der „Personen suchen"-Dialog öffnet sich. In diesem dann in dem Auswahlfeld „Verzeichnis:" das DFN-Verzeichnis mit der Bezeichnung DFN-PKI auswählen. Dies wurde ja im zweiten Teil des mehrteiligen Artikels beschrieben (s. die GWDG-Nachrichten 10/2013, S. 13). Jetzt den Empfänger suchen, mit dem sensitive Daten ausgetauscht werden sollen. Den Namen, Teile des Namens oder die E-Mail-Adresse eingeben und dann auf „Suchen" klicken. Wenn der entsprechende Empfänger gefunden wurde, diesen per Klick auswählen (s. Abb. 38).

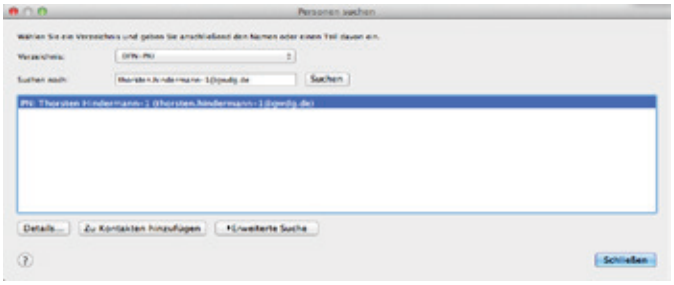


Abb. 38

Mit einem Klick auf „Details..." können noch Details des Empfängers angesehen werden. Am wichtigsten ist dabei zu überprüfen, ob das Internetzertifikat vorhanden ist. Dazu auf der mehrfach geteilten Schaltfläche/Registerreiter „Zertifikate" anklicken und das Vorhandensein des Internetzertifikats prüfen (s. Abb. 39).

Abb. 39

Wenn alles in Ordnung ist, diesen Dialog mit einem Klick auf „Schließen" beenden und jetzt auf „Zu Kontakten hinzufügen" klicken, damit der ausgewählte E-Mail-Empfänger zu den Kontakten hinzugefügt wird (s. Abb. 38).

Diese Aktion wird mit folgendem Hinweis quittiert, der mit einem Klick auf „OK" bestätigt wird (s. Abb. 40).

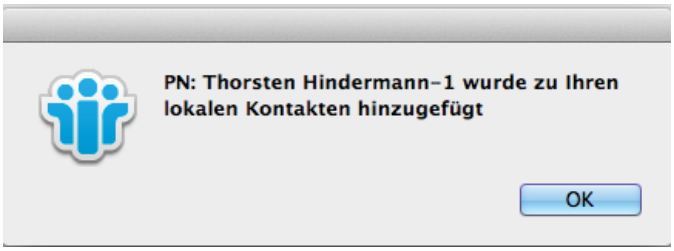


Abb. 40

Nun den „Personen suchen"-Dialog mit einem Klick auf „Schließen" beenden (s. Abb. 38).

Das Adressbuch sieht in diesem Fall nun wie folgt aus (s. Abb. 41).

Abb. 41

Und die Detailansicht zum ausgewählten Kontakt sieht folgendermaßen aus (s. Abb. 42).

Nun das Bearbeitungsfenster für eine neue E-Mail-Nachricht

Abb. 42

öffnen. Auf die anklickbare Schaltfläche/Link „An:“ klicken. Der „Adresse auswählen“-Dialog öffnet sich. Den E-Mail-Empfänger auswählen und durch Klick auf „An >“, „Kopie >“ und „Blindkopie >“ entsprechend einordnen. Wenn der/alle Empfänger ausgewählt und eingeordnet sind, den Dialog mit einem Klick auf „OK“ schließen (s. Abb. 43).

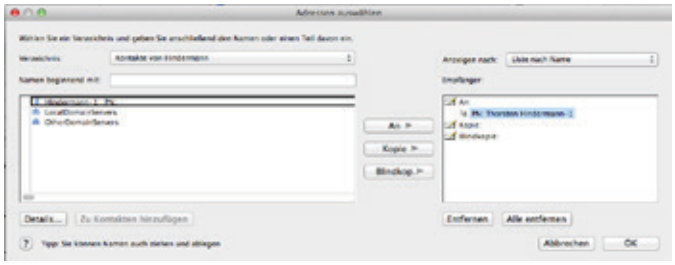


Abb. 43

Anmerkung: In der Auswahl „Verzeichnis:“ sollte das eigene Adressbuch ausgewählt sein, dass die Bezeichnung „Kontakte von <Nachname>“ hat.

Auf dem Registerreiter mit den Aktionen für die gerade in Arbeit befindliche E-Mail auf „Zustelloptionen...“ klicken. Daraufhin öffnet sich der „Zustelloptionen“-Dialog (s. Abb. 44).

Abb. 44

In diesem Dialog nun noch unter der Gruppe „Sicherheitsoptionen“ die Auswahl „Verschlüsseln“ anhaken und den Dialog mit „OK“ schließen. Als Bestätigung sind die eingestellten Sicherheitsmöglichkeiten unter dem/den Empfänger- und Betreff-Eingabefeld(ern) noch einmal als Textausgabe sichtbar (s. Abb. 45).

Wenn jetzt alles eingestellt ist und die E-Mail-Nachricht vollständig geschrieben ist, wird die E-Mail mit einem Klick auf „Senden“ entsprechend den Einstellungen abgesichert zum Empfänger gesendet. Das Ergebnis dieser Aktion sieht dann in der

Abb. 50

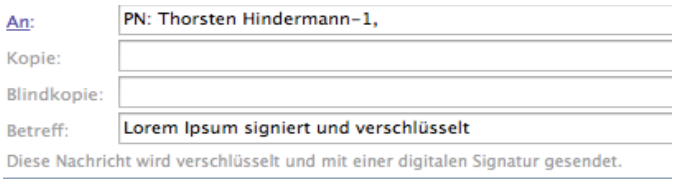


Abb. 45

Abb. 46

Notes-E-Mail-Anwendung wie folgt aus (s. Abb. 46).

Erster Empfang einer signierten/verschlüsselten E-Mail

Wenn nun die erste mit einem X.509-Zertifikat signierte E-Mail empfangen wurde und diese angeklickt wird, ist es notwendig, für die erhaltenen Informationen mit der eigenen Notes-ID ein Gegenzertifikat auszustellen. Dazu einfach den angezeigten Dialog mit „Gegenzertifizieren“ bestätigen (s. Abb. 47).

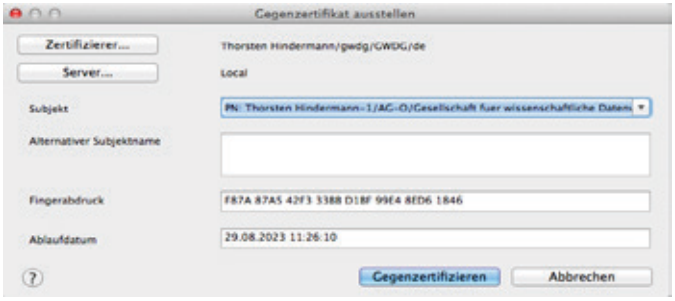


Abb. 47

In der Notes-Statuszeile wird dann ab sofort beim Klick auf signierte E-Mails in der Meldungszeile nur noch folgender Text angezeigt (s. Abb. 48).

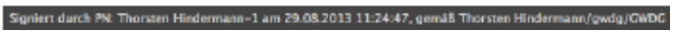


Abb. 48

In der empfangenen, signierten E-Mail wird in den Kopfzeilen die Information angezeigt, dass diese E-Mail signiert wurde (s. Abb. 49).

Abb. 49

Der Empfang einer signierten und/oder verschlüsselten E-Mail funktioniert genau so wie der Empfang einer nur signierten E-Mail. In den Details der Kopfinformationen zur empfangenen E-Mail kann entnommen werden, ob die E-Mail signiert und/oder verschlüsselt wurde. Dazu einfach rechts außen in den Kopfinformation auf „Details anzeigen“ klicken. „Details anzeigen“ wandelt sich im Moment des Klicks um zu „Details verbergen“ (s. Abb. 50).


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen