GWDG NACHRICHTEN 10|13

Firefox Sync-Server

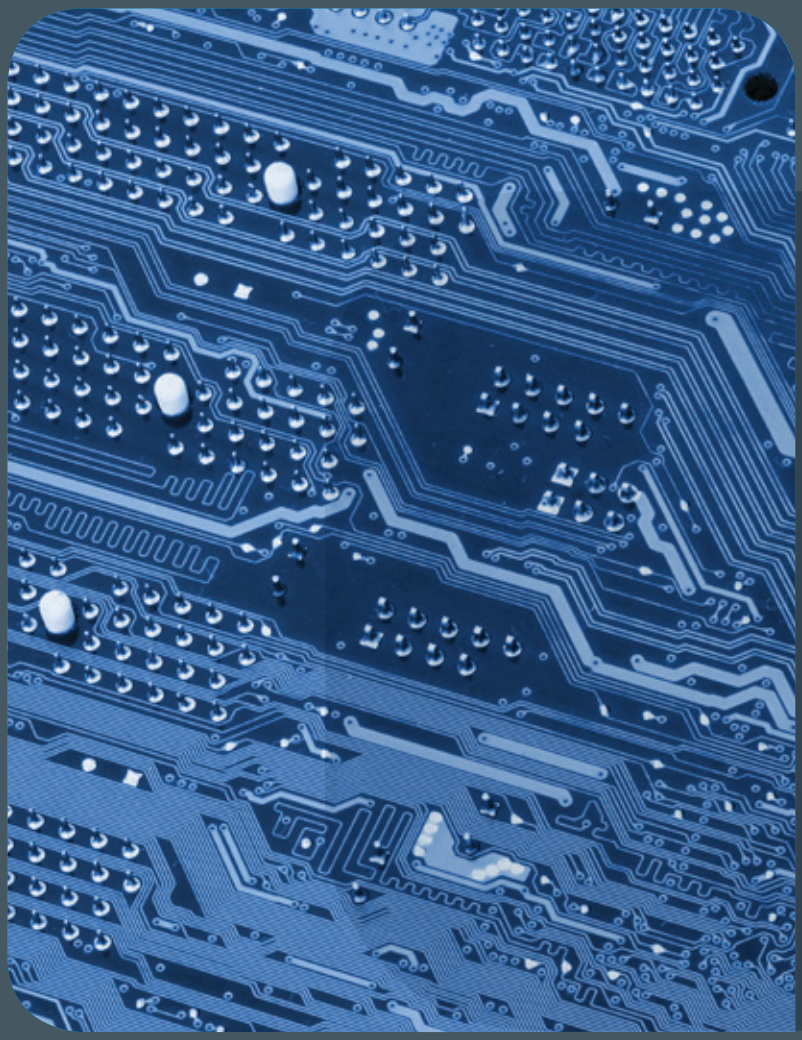
Fernlöschen eines Smartphones

IdeenExpo

E-Mail-Verschlüsselung

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



GWDG
NACHRICHTEN

10|13 Inhalt

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
36. Jahrgang
Ausgabe 10/2013

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
500

Fotos:
© xiaoliangge - Fotolia.com (1, 11)
© Kheng Guan Toh - Fotolia.com (6)
© MPIbpc-Medienservice (3, 19)
© Pressestelle Uni Göttingen (9, 10)
GWDG (2, 10)

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

Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de
0551 201-1545

Liebe Kunden und Freunde der GWDG,

die wissenschaftliche Datenverarbeitung muss sich ständig neuen Herausforderungen stellen und nach entsprechenden Lösungen hierfür suchen. Ein intensiver Austausch von Ideen und Erfahrungen sowie eine kooperative IT sind hierbei enorm wichtig und nützlich. Ein gutes Beispiel hierfür ist das jährliche DV-Treffen der Max-Planck-Institute, das in der letzten Septemberwoche zum mittlerweile 30. Mal stattgefunden hat – in diesem Jahr, wie schon so oft, wieder in Göttingen. Es hat sich im Laufe der Jahre erfolgreich zu einer der bedeutendsten Plattformen für die Kommunikation und den Informationsaustausch zwischen den einzelnen IT-Abteilungen der Max-Planck-Institute sowie den zentralen IT-Dienstleistern der MPG entwickelt.

Ein wichtiges Thema des abwechslungsreichen Programms war der Umgang mit großen Datenmengen und die Datenanalyse. Beide Aufgaben gewinnen quer über alle Wissenschaftsdisziplinen immer mehr an Bedeutung und erfordern neben geeigneten Datenmanagement-Konzepten, über die schon in vergangenen Ausgaben der GWDG-Nachrichten berichtet wurde, auch entsprechend qualifiziertes Personal. Sogenannten Data Scientists kommt hierbei zukünftig eine entscheidende Rolle zu. Die universitäre Lehre wie auch wissenschaftliche IT-Dienstleister sind hier gefordert, das weitgehend noch fehlende Know-how aufzubauen und für entsprechende Schulung und Ausbildung zu sorgen. Auch die GWDG wird dem mit entsprechenden Maßnahmen Rechnung tragen.

Ich wünsche Ihnen viel Freude beim Lesen dieser Ausgabe der GWDG-Nachrichten.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Neuer Dienst bei der GWDG: Synchronisierungs-Server für den Firefox-Webbrowser

Text und Kontakt:
Dr. Roland Baier
roland.baier@gwdg.de
0551 201-1822

Die GWDG bietet als neuen Dienst einen Synchronisierungs-Server für Firefox-Webbrowser an. Der Server ermöglicht es, die Daten und Einstellungen von Firefox (z. B. Lesezeichen, Chronik oder Passwörter) auf mehreren Geräten auf demselben Stand zu halten. Der Firefox Sync-Server bei der GWDG kann kostenlos von jedem Kunden der GWDG genutzt werden. Die Funktionalität zum Synchronisieren ist im Firefox-Webbrowser bereits integriert (ab Version 4); es muss lediglich noch ein Benutzerkonto auf dem Firefox Sync-Server erzeugt und konfiguriert werden. Dieser Artikel informiert, wie man selbständig ein Benutzerkonto für Firefox Sync einrichtet und wie man weitere Rechner mit diesem Benutzerkonto verbindet, so dass die Daten des Webbrowsers auf sichere Weise über alle Rechner synchronisiert werden können.

EINLEITUNG

Es gibt eine Menge an Daten und Einstellungen, die man in einem Webbrowser speichern kann. Neben den Programmeinstellungen (z. B. Schriftarten oder Farben) sind das auch Angaben, die im Zuge der Benutzung des Browsers anfallen und für die spätere Verwendung gespeichert werden, wie z. B. Lesezeichen, die Chronik der besuchten Webseiten, benötigte Passwörter, Registerkarten etc.

Wenn man auf mehr als einem Gerät mit einem Webbrowser arbeitet (z. B. mit dem „Hauptrechner“ am Arbeitsplatz und daneben noch mit weiteren (Mobil-)Geräten), dann ist es oft wünschenswert, stets dieselbe „Arbeitsumgebung“ im Browser vorzufinden. Dies lässt sich durch Synchronisierung der Browserdaten erreichen. Für diverse Browsertypen werden die erforderlichen Synchronisierungs-Tools und -Server auch schon längst angeboten. Eine Übersicht dazu findet man in Wikipedia unter *http://en.wikipedia.org/wiki/Comparison_of_browser_synchronizers*.

Der beliebte Webbrowser Firefox hat die Funktionalität zum Synchronisieren seit Version 4 bereits an Bord („Firefox Sync“, frühere Bezeichnung „Mozilla Weave“), und der Anbieter Mozilla stellt hierzu auch einen allgemein zugänglichen Firefox Sync-Server zur Verfügung. Die zu synchronisierenden Daten werden verschlüsselt in einer Datenbank auf diesem Sync-Server gespeichert. Weitere Informationen dazu findet man auf der Webseite *https://support.mozilla.org/de/kb/was-ist-firefox-sync*.

Interessant ist nun, dass Mozilla darüber hinaus auch Open Source Software anbietet, mit der man seinen eigenen Sync-Server betreiben kann, was nicht zuletzt sicherstellt, dass man Herr der eigenen Daten bleibt: *https://docs.services.mozilla.com/howtos/run-sync.html*.

In der GWDG wurde unter Verwendung dieser Software ein solcher Firefox Sync-Server in Betrieb genommen, der nunmehr von jedem Kunden der GWDG genutzt werden kann. Die Datenspeicherung erfolgt auf einer MySQL-Datenbank in der GWDG.

Zur Nutzung ist kein Antrag erforderlich und es entstehen keine Kosten (es werden auch keine „Arbeitseinheiten“ berechnet). Die selbständige Einrichtung eines Benutzerkontos auf dem Sync-Server bei der GWDG ist leicht durchzuführen und wird nachfolgend beschrieben.

New GWDG service: Firefox sync server

As a newly developed service, GWDG provides a synchronisation server for the Firefox web browser. It allows you to keep your personal browser data and settings (e. g. bookmarks, history or passwords) in sync between different devices. The GWDG Firefox sync server is available to all GWDG customers. As the synchronisation feature is a built-in functionality in the Firefox web browser (Version 4 and later), all you need is a user account on the GWDG Firefox sync server. This article describes how to register for a user account and to connect your devices to this account in order to synchronise your web browser data securely between all devices.

Folgende Schritte sind erforderlich, um den GWDG Sync-Server für Firefox zu nutzen:

- Ein Benutzerkonto auf dem Sync-Server erstellen
- Konfiguration von Firefox Sync
- Weitere Rechner für die Synchronisierung mit dem Benutzerkonto verbinden

EIN BENUTZERKONTO AUF DEM FIREFOX SYNC-SERVER DER GWDG ERSTELLEN

- Klicken Sie im Firefox-Menü auf „Extras > Sync einrichten …“ oder auf „Extras > Einstellungen > Registerkarte Sync > Firefox Sync einrichten“.
- Klicken Sie nun auf „Neues Benutzerkonto anlegen“.
- Geben Sie eine E-Mail-Adresse und ein Passwort ein. Verwenden Sie bitte eine existente und funktionierende E-Mail-Adresse, da diese bei einem Passwort-Reset benötigt wird.
- Legen Sie die „Sync-Einstellungen“ mit Hilfe der diesbezüglichen Schaltfläche unten links fest.
- Tragen Sie nun den Sync-Server ein. Dazu in der Dropdown-Liste den Eintrag „Eigenen Server verwenden“ auswählen und dann die Adresse *https://ffsync.gwdg.de* eintragen.
- Der „Captcha“-Block verschwindet nach dieser Eingabe.
- Klicken Sie dann auf „Weiter“.
- Im Browser erscheint eine Seite mit der Überschrift „Setup abgeschlossen“ und einem Fortschrittsbalken, der schließlich (meist erst nach einiger Zeit) grün wird.
- Die zu synchronisierenden Daten von Firefox werden auf den Sync-Server hochgeladen und in der Datenbank gespeichert und stehen damit für die Synchronisierung bereit.

KONFIGURATION VON FIREFOX SYNC

Bereits bei der Erstellung des neuen Sync-Benutzerkontos kann man festlegen, welche Elemente von Firefox bei der Synchronisierung berücksichtigt werden sollen (standardmäßig sind alle Elemente ausgewählt). Diese Einstellung kann auch später noch geändert werden. Klicken Sie dazu im Firefox-Menü auf „Extras > Einstellungen > Registerkarte Sync“.

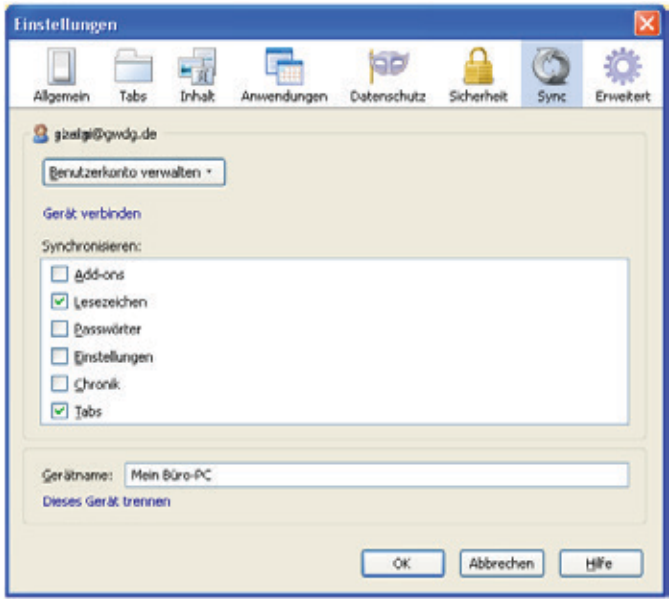
In dem nun erscheinenden Fenster (s. Abb. 1) können die zu synchronisierenden Elemente ausgewählt werden. Eine Änderung dieser Auswahl wird im Zuge der Synchronisierung automatisch auf alle an der Synchronisierung teilnehmenden Rechner (mit Firefox) übertragen.

Hinweis zu „Chronik“: Dies umfasst das Verzeichnis der früher besuchten Webseiten wie auch die Aufzeichnung der früher in Web-Formulare eingetragenen Angaben.

Zur Frage, ob man auch „Passwörter“ synchronisieren sollte, und zur Sicherheit des Verfahrens folgen im Anschluss einige Bemerkungen.

Ist Firefox Sync sicher?

Die zur Synchronisierung vorgesehenen Firefox-Daten werden bereits im Webbrowser verschlüsselt, mit dem sog. Wiederherstellungs-Schlüssel („Recovery-Key“), der bei der Erstellung eines Benutzerkontos durch das Sync-Programm im Webbrowser



1_ Einstellungen für Firefox Sync im Browser

generiert wird und dort verbleibt.

Auf den Sync-Server werden nur die verschlüsselten Daten übertragen und in einer Datenbank gespeichert, nicht aber der Wiederherstellungs-Schlüssel.

Mozilla konstatiert auf einer Webseite zum Thema Sicherheit der Sync-Daten: „Alle Ihre Daten werden so sicher gespeichert, dass nur Sie diese lesen können“: *https://support.mozilla.org/de/kb/wie-sicher-sind-meine-sync-daten*

Soll man auch Passwörter synchronisieren?

Die kurze Antwort auf diese Frage lautet: Jeder muss für sich entscheiden, ob und welche Passwörter er in Firefox speichert und ob gespeicherte Passwörter synchronisiert werden sollen.

Firefox kann bekanntlich so konfiguriert werden, dass es Passwörter (für den Zugang zu geschützten Webseiten) speichern kann (Firefox-Menü: „Extras > Einstellungen > Registerkarte Sicherheit“).

Wenn man von dieser Möglichkeit Gebrauch macht, dann ist dringend anzuraten, diese sensiblen Daten in Firefox mit einem „Master-Passwort“ vor unberechtigtem Ausspähen zu schützen.

Firefox Sync speichert, wenn der Browser an einem Sync-Server angemeldet ist, automatisch zwei Passwörter, und zwar auch dann, wenn in den Firefox-Einstellungen die Option „Passwörter speichern“ nicht aktiviert ist! Gespeichert werden das Passwort für das Sync-Benutzerkonto (Eintrag: *chrome://weave (Mozilla Services Password)*) sowie der Wiederherstellungs-Schlüssel (Eintrag: *chrome://weave (Mozilla Services Encryption Passphrase)*).

Nutzer von Firefox Sync sollten daher unbedingt ein „Master-Passwort“ in Firefox festlegen, und zwar auf allen Rechnern und Mobilgeräten, die an der Synchronisierung teilnehmen!

Noch ein Hinweis: Das Firefox „Master-Passwort“ wird nicht synchronisiert!

Weitere Einstellungen für Firefox Sync

Wie in Abb. 1 zu sehen, kann man einen „Gerätname“ eintragen, der den Rechner identifiziert.

Soll die Synchronisierung gestoppt werden, dann klickt man auf „Dieses Gerät trennen“. Damit wird der Rechner am Sync-Server abgemeldet. Um die Synchronisierung wieder zu starten, muss

man den Rechner erneut anmelden, so wie es im nachfolgenden Kapitel beschrieben ist.

2_ Verwaltungsfunktionen für das-Benutzerkonto auf dem Sync-Server

Unter der Schaltfläche „Benutzerkonto verwalten" findet man einige nützliche Funktionen (s. Abb. 2).

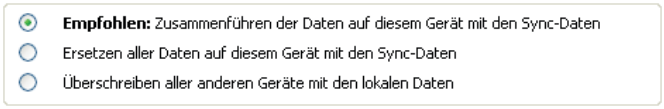
Quota anzeigen: Der verbrauchte Speicherplatz wird angezeigt, aufgeschlüsselt nach den Firefox-Elementen. Jedes Benutzerkonto auf dem GWDG SyncServer verfügt über ein Speicherkontingent von derzeit 10 MByte zum Speichern der eigenen Sync-Daten.

Passwort ändern...: Damit kann man das Passwort für das Benutzerkonto auf dem Sync-Server ändern. Wenn Firefox nicht am Sync-Server angemeldet ist und daher diese Funktion nicht zur Verfügung steht, dann kann man die Webseite *https://ffsync.gwdg.de/weave-password-reset aufrufen*, um ein neues Passwort zu setzen. Dabei wird eine E-Mail mit Instruktionen an die E-Mail-Adresse des Benutzerkontos gesendet.

Achtung: Nach einer Änderung des Passworts können andere Geräte nicht mehr synchronisieren, sie müssen erst wieder angemeldet werden.

Mein Wiederherstellungs-Schlüssel: Es handelt sich dabei um den bereits oben genannten Schlüssel (auch „Recovery Key" genannt), mit dem die Firefox-Daten verschlüsselt werden, bevor sie zum Sync-Server gehen. Dieser Schlüssel ist sehr wichtig und sollte unbedingt notiert und aufbewahrt werden, wozu man auch die angebotenen Funktionen „Drucken..." und „Speichern..." nutzen kann. Geht der Schlüssel verloren, dann können die gespeicherten Sync-Daten nicht mehr entschlüsselt werden und sind somit wertlos!

Sync zurücksetzen...: Damit legt man fest, auf welche Weise die Synchronisierung erfolgen soll (s. Abb. 3).



3_ In Firefox Sync verfügbare Methoden der Synchronisierung

WEITERE RECHNER FÜR DIE SYNCHRONISIERUNG MIT DEM SYNC-BENUTZERKONTO VERBINDEN

Um einen Rechner oder ein Mobilgerät in die Synchronisierung einzuschließen, muss man Firefox mit einem Sync-Benutzerkonto verbinden. Hierfür gibt es zwei Vorgehensweisen: entweder mit Hilfe eines Freischaltcodes oder ohne Freischaltcode.

Mit Hilfe eines Freischaltcodes

Dazu muss man am „Hauptrechner" sein und das andere Gerät (z. B. ein Notebook) dabei haben.

Freischaltcode erzeugen

Klicken Sie auf dem neuen Gerät im Firefox-Menü auf „Extras > Sync einrichten... > Ich habe ein Benutzerkonto" oder auf „Extras > Einstellungen > Registerkarte Sync > Firefox-Sync einrichten > Ich habe ein Benutzerkonto". Notieren Sie sich den Freischaltcode.

Freischaltcode auf dem „Hauptrechner" anwenden

Klicken Sie auf dem Hauptrechner im Firefox-Menü auf „Extras > Einstellungen > Registerkarte Sync > Gerät verbinden" und geben Sie den Freischaltcode ein.

Das Passwort des Benutzerkontos und der Wiederherstellungs-Schlüssel werden auf das neue Gerät übertragen und in Firefox gespeichert. Daher sollten Sie ggf. in Firefox noch ein „Master-Passwort" festlegen.

Ohne Freischaltcode.

Der „Hauptrechner" wird dazu nicht benötigt. Klicken Sie auf

dem neuen Gerät im Firefox-Menü auf „Extras > Sync einrichten… > Ich habe ein Benutzerkonto“. Klicken Sie dann auf „Ich habe das Gerät nicht bei mir“. Nun müssen die Daten für das Benutzerkonto eingetragen werden: E-Mailadresse, Passwort und Wiederherstellungs-Schlüssel. Und schließlich ist noch der „Eigene Server“ einzugeben.

WEITERE HINWEISE UND HILFESTELLUNGEN

Probleme bei der Erstellung des Benutzerkontos

Leider funktioniert Firefox Sync nicht immer ganz reibungslos. Speziell zu Beginn, bei der Erstellung eines Benutzerkontos, hakt es schon mal. Manchmal wird die Adresse des „Eigenen Sync-Servers“ oder die E-Mail-Adresse als ungültig bemäkelt. Über diese Probleme hilft meist ein wenig Spielen mit den Eingaben hinweg, wie etwa das Entfernen des abschließenden Schrägstrichs im URL oder das Ändern und Zurückändern der E-Mail-Adresse.

Oft ist zu beobachten, dass nach Abschluss der Konto-Erstellung zwar die Webseite mit der Überschrift „Setup abgeschlossen“ erscheint, aber der Fortschrittsbalken sich nicht grün färbt. Synchronisieren funktioniert nicht, und die Sync-Einstellungen sind nicht zu sehen. Stattdessen erscheint im betreffenden Fenster ein Hinweis „Ungültiger Benutzername oder Passwort – Aktualisieren – Zurücksetzen – Dieses Gerät trennen“, auch wurden zwei neue Logfiles erzeugt.

Die drei im Hinweis (s. o.) angebotenen Aktionen helfen nicht weiter. Durch Beenden und Neustart von Firefox kann das Problem manchmal behoben werden. In hartnäckigen Fällen hilft längeres Warten (ca. 1 Stunde), mit gelegentlichen Synchronisierungs-Versuchen.

Vermutlich ist die Sync-Software noch nicht ganz fehlerfrei, es bleibt zu hoffen, dass die geschilderten Probleme in späteren Programmversionen verschwinden werden.

Fragen und Antworten zu Firefox Sync

Wie oft wird synchronisiert?

Automatisch alle 60 Minuten, oder sofort mit dem Menübefehl „Jetzt synchronisieren“ in Firefox.

Wie ändert man ggf. das Zeitintervall?

Dazu gibt man in Firefox den URL *about:config* ein, sucht in der dann erscheinenden Tabelle nach dem Eintrag *services.sync.syncInterval* und ändert den betreffenden Wert. Der Standardwert ist 3.600.000 Millisekunden (= 60 Minuten) und bedarf normalerweise keiner Änderung.

Welche Firefox-„Einstellungen“ (Preferences) werden synchronisiert?

Synchronisiert werden diejenigen Einstellungen des Typs *services.sync.prefs.sync.<pref>* in der über *about:config* zugänglichen Tabelle, welche den Wert *true* haben. Dieser Liste können weitere Preferences hinzugefügt werden. Wenn z. B. für eine Firefox-Extension eine Preference namens *extension.frobnaz.foobar* existiert, welche ebenfalls synchronisiert werden soll, dann kreiert man eine neue Boolesche-Preference *services.sync.prefs.sync.extension.frobnaz.foobar* und gibt ihr den Wert *true*.

Wie kann ich die Betriebsbereitschaft des Firefox Sync-Servers überprüfen?

Der Aufruf der Webseite *https://ffsync.gwdg.de/__heartbeat__* liefert eine leere Webseite zurück (HTTP-Statuscode 200), wenn der Sync-Server funktioniert, oder eine Fehlermeldung bei einer Störung des Sync-Servers.

Eine erfolgreiche Abfrage der „Quota“ (s. o.) ist zugleich ein Beleg dafür, dass der Sync-Server und die Datenbank funktionieren.

Wie kann ich ein neues Passwort setzen?

Das ist weiter oben unter „Weitere Einstellungen für Firefox Sync“ beschrieben.

Ich habe mein Passwort / meinen Wiederherstellungs-Schlüssel verloren.

Das Passwort und der Wiederherstellungs-Schlüssel werden im Passwort-Speicher von Firefox gespeichert und können dort eingesehen werden. Das Passwort kann wie weiter oben beschrieben geändert werden.

Ein verlorener Wiederherstellungs-Schlüssel hat zur Folge, dass die bisher gespeicherten Firefox-Daten nicht mehr lesbar sind. Man kann einen neuen Schlüssel generieren, es bleibt aber beim Verlust der alten Daten auf dem Sync-Server.

Wie kann ich mein Benutzerkonto löschen?

Zuerst das „Gerät trennen“, in den Sync-Einstellungen von Firefox. Dann die Webseite *https://ffsync.gwdg.de/weave-delete-account* aufrufen und dort Username (= E-Mail-Adresse) und Password eingeben.

Nach erfolgreicher Löschung des Sync-Benutzerkontos erscheint die Meldung „Account removed.“ auf der Webseite.

Der Administrator des Firefox Sync-Servers kann in Ausnahmefällen ein Benutzerkonto und die zugeordneten Firefox-Daten in der MySQL-Datenbank löschen.

Gibt es Logfiles für Firefox-Sync?

Ja, man findet sie am einfachsten durch Eingabe des URLs *about:sync-log* in Firefox.

Es handelt sich dabei um Error-Logfiles, die bei Fehlern von Firefox Sync angelegt werden. Sie werden im Laufe der Zeit automatisch wieder gelöscht.

Wie kann ich die Synchronisierung auf einem Gerät stoppen?

Man klickt im Firefox-Menü auf „Extras > Einstellungen > Registerkarte Sync > Dieses Gerät trennen“.

Um die Synchronisierung zu aktivieren, muss das Gerät wieder neu mit dem Benutzerkonto verbunden werden, wie oben beschrieben.

Wo findet man die „gesyncten“ Lesezeichen?

Als zusammenhängender Block in den Firefox-Lesezeichen.

Wo findet man die „gesyncten“ Registerkarten (Tabs)?

Dazu den URL *about:sync-tabs* eingeben oder im Firefox-Menü den Befehl „Chronik > Tabs von anderen Geräten“ anklicken.

Anhand des angezeigten Gerätenamens lässt sich erkennen, von welchem Rechner die Tabs stammen.

Wo findet man die „gesyncte“ Chronik?

Sie wird mit der Chronik (Strg h) im gerade verwendeten Firefox-Browser vereinigt.

Fernlöschen eines Smartphones

Text und Kontakt:
Michael Reimann
michael.reimann@gwdg.de
0551 201-1826

Smartphones sind inzwischen zu unverzichtbaren Begleitern geworden. Somit ist es auch besonders ärgerlich, wenn sie einmal verloren gehen sollten. Neben dem Materialwert schmerzt ganz besonders die Tatsache, dass womöglich die sich darauf befindlichen Daten in falsche Hände geraten könnten.

Zwei Möglichkeiten gibt es, auf ein derartiges Ereignis zu reagieren: Ist das Smartphone einfach nur verloren gegangen, wird man versuchen, das Gerät zu lokalisieren. Wurde es gar entwendet, empfiehlt sich das Fernlöschen der darauf befindlichen Daten, um einem Missbrauch zuvor zu kommen. Voraussetzung für diese Maßnahmen ist natürlich, dass das Gerät noch über das Netz erreichbar ist. Ist ein Zugriff auf das verlorene Gerät nicht mehr möglich, sollte man zumindest die SIM-Karte sperren lassen. Hier bieten alle größeren Mobilfunkprovider Möglichkeiten zu einer Sperrung an, entweder über entsprechende Rufnummern oder über ein Kundenportal.

Bei den beiden am häufigsten verbreiteten Smartphone-Architekturen (Android und iOS) sollen hier kurz die zur Verfügung stehenden Möglichkeiten der Fernlöschung aufgezeigt werden.

ANDROID

Erst im August diesen Jahres hat Google den neuen **Android Geräte-Manager** für alle Geräte mit der Android-Version ab 2.2 bereitgestellt. Er ermöglicht die Ortung des Gerätes, kann es gegebenenfalls für mehrere Minuten auf voller Lautstärke klingeln lassen und vermag nötigenfalls die Daten durch Fernlöschung dem Zugriff zu entziehen. Der dafür zuständige neue Menüpunkt findet sich in den Einstellungen unter „Sicherheit > Geräteadministration > Android Gerätemanager". Wird er aktiviert, lassen sich über den Google-Service der GPS-Standort auslesen, alle Daten löschen und das Gerät sperren. Hierzu muss dann lediglich die Webseite *http://www.android.com/devicemanager* angesteuert werden.

Der Android Geräte-Manager setzt bei seiner Ortung eine Internetverbindung voraus und funktioniert aber selbst dann noch, wenn die SIM-Karte bereits ausgetauscht, das Gerät aber noch nicht ferngelöscht wurde.

APPLES IPHONE/IPAD

Apple bietet seit 2010 mit **Find my iPhone** eine ähnliche Lösung an, die jetzt mit der neuen Betriebssystemversion iOS 7 noch verbessert wurde. Wird diese Funktion in „Einstellungen > iCloud > Mein iPhone/iPad suchen" aktiviert, kann auch hier das verlorene Gerät über eine Webseite geortet und gegebenenfalls ferngelöscht werden. Zusätzlich wird der Schutz gegen Missbrauch durch die neuen Sicherheitsfunktionen erhöht, indem immer letztlich die Kenntnis der Apple ID und des dazugehörigen Passwortes des Besitzers erforderlich ist, um das Gerät einem anderen Zweck zuzuführen.

EXCHANGE-SERVER DER GWDG

Wichtige Maßnahmen wie das Fernlöschen bietet übrigens auch der Exchange-Server der GWDG an, unabhängig von dem verwendeten Mobilgerätetyp. Die neue Version 2010 des Exchange-Servers bietet hier insofern einen Komfortgewinn, als dass der Nutzer diese Maßnahmen selber einleiten kann, indem er dazu im Web-Interface (*http://email.gwdg.de*) und dort im Menü „Optionen > Alle Optionen anzeigen..." den Eintrag „Telefon > Mobiltelefone" auswählt. Hier finden sich alle derzeit vom Nutzer verwendeten mobilen Geräte aufgelistet, zu denen übrigens auch Windows-8-Systeme gezählt werden, sofern sie mit dem mitgelieferten Windows-Mail-Programm auf den Exchange-Server zugreifen. Der Menüpunkt „Details" offenbart genauere Informationen zu dem jeweiligen Gerät, was schon allein deshalb sinnvoll ist, damit nicht aus Versehen das falsche Gerät gelöscht wird. Im Falle eines Verlustes kann dann für das betreffende Gerät über den Menüpunkt „Gerätezurücksetzung" eine Fernlöschung initiiert werden, so dass beim nächsten Synchronisationsvorgang der Löschauftrag ausgeführt wird. Wichtig für den Erfolg dieser Maßnahme ist natürlich, dass das Gerät noch über das Netz erreichbar und eine Synchronisation mit Exchange-Server möglich ist. Eine Ortung des mobilen Gerätes ist auf diesem Wege nicht vorgesehen. Wird eine solche gewünscht, sollte hierfür auf die jeweiligen Lösungen der Anbieter zurückgegriffen werden.

Remote cancellation of a smartphone

Smartphones have become indispensable companions. Therefore, it is particularly unpleasant when they are lost, and perhaps the data contained on them could be misused. What can we do about it?

FAZIT

Mit den derzeit verfügbaren technischen Möglichkeiten ist es also gar nicht so unwahrscheinlich, ein verloren gegangenes Mobilgerät wiederzufinden bzw. bei drohendem Missbrauch vorsorglich die darauf befindlichen Daten zu löschen. Das gelingt aber immer nur dann, wenn die Diebe nicht über das entsprechende Spezialwissen verfügen, um diese Maßnahmen zu durchkreuzen. Um es ihnen aber so schwer wie möglich zu machen, ist es generell empfehlenswert, das Gerät stets über eine Code-Sperre zu sichern (Apple: „Einstellungen > Allgemein > Code-Sperre“, Android: „Einstellungen > Sicherheit > Display-Sperre“).

GWDG auf der IdeenExpo

Text und Kontakt:
Daniel Adler
daniel.adler@gwdg.de
0551 201-2134
Maik Srba
maik.srba@gwdg.de
0551 39-21108

Auf dem Messegelände Hannover fand Ende August unter dem Motto „Deine IDEEN verändern“ zum vierten Mal die IdeenExpo statt. Sie verfolgt das Ziel, Mädchen und Jungen gleichermaßen für die vielfältigen Themen der sogenannten MINT-Fächer (Mathematik, Informatik, Naturwissenschaften und Technik) zu begeistern. Auch die GWDG war in diesem Jahr daran beteiligt. Die Universität Göttingen, die Niedersächsische Staats- und Universitätsbibliothek Göttingen (SUB), die GWDG und das XLAB – Experimentallabor für junge Leute präsentierten sich auf der IdeenExpo auf einem knapp 300 Quadratmeter großen Stand.

Die GWDG war dieses Jahr in Zusammenarbeit mit der SUB mit einem Stand auf dem gelben Pfad Wissenschaft/Technologie unter dem Motto „Computer-Technik im Wandel der Zeit“ mit den Schwerpunkten „Datenschutz im Web 2.0“ und „Retro-Computing von damals bis heute“ vertreten.

WEB-2.0-SPIEL

Nach dem Motto „Wir hängen den Leuten etwas an – POST ITs!“übertrug das Web-2.0-Spiel der SUB und der GWDG digitale Kulturtechnik aus dem Web-2.0-Alltag (Facebook, Twitter, Flickr etc.) ins Analoge zurück.

Es vermittelte spielerisch positive wie negative Aspekte

GWDG on the IdeenExpo

Under the slogan „Your IDEAS impact“ the IdeenExpo took place in late August at the Hannover Exhibition Grounds for the fourth time. It aims to inspire girls and boys alike for the many themes of the so-called MINT disciplines (mathematics, computer science, natural sciences and technology). Also, the GWDG participated this year in it. The University of Göttingen, the Göttingen State and University Library (SUB), the GWDG and the XLAB – Experimental laboratory for young people presented themselves on the IdeenExpo on a nearly 300-square-meter stand.

sozialer Medien, die zu einem sorgsameren Umgang mit persönlichen Inhalten anregen sollten. Dazu hatten unsere zahlreichen Gäste viele tolle Kunstwerke mit analogen Geräten wie Kugelschreiber und Zettel erzeugt und digital verewigt. Die Fotosammlung ist unter *http://www.flickr.com/photos/100016054@N04/* zu finden.

RETRO-COMPUTING

Als weiteres Exponat wurden die Anfänge der Heim-Computer ausgestellt und zum aktiven Mitwirken eingeladen. Zum einen wurde der Commodore 64 (C64) inkl. Datasetten-Massenspeicher in einer Glassvitrine ausgestellt. Zum anderen stand aber auch ein weiterer „Brotkasten" fertig aufgebaut samt Monitor und Floppy-Station bereit, mit dem die Anfänge der Videospielkultur gezeigt und gespielt wurde.

Neben der großen Freude an den schönen Pixel-Kunstwerken aus dieser Videospielära zeigten viele junge Besucher auch Interesse an den technischen Hintergründen und waren sehr erstaunt über die 30 Jahre alte Technologie. Und auch die älteren Gäste kannten meistens den C64 und schwelgten in Nostalgie.

RASPBERRY PI

Nach dieser Reise in die Vergangenheit haben wir die Gäste mit der „Himbeere" wieder in das Jahr 2013 zurückgeführt. Der Raspberry Pi ist ein sehr günstiger kreditkartengroßer Ein-Platinen Computer, der sich für sehr viele Einsätze eignet.

Er wurde ursprünglich von dem C64-„Elite"-Entwickler und zwei Professoren aus Cambridge entwickelt, um junge Menschen wieder an das Informatik-Studium heranzuführen. Mittlerweile gibt es eine breitgestreute Community.

Wir haben u. a. den C64 Emulator Vice unter einem Linux-Desktop dazu verwendet, wenn einmal die Schlange vor dem C64 zu lang wurde. Der Raspberry Pi wurde entweder als Spielemaschine akzeptiert oder sorgte sogar für interessante Gespräche über die Rechnerentwicklung, Einsatzmöglichkeiten solcher Minisysteme etc. Als weitere Anwendungsfälle denkbar sind der Pi als Linux-Desktop oder XBMC / Media-Player. Zudem bietet er Hardware-Bastlern sehr viele Ausbaumöglichkeiten.

Zu diesem Zweck hatte die GWDG auch ein kleines Kontingent an Ausdrucken des kostenlosen Magazins MagPi besonders interessierten Besuchern mitgeben können.

Insgesamt ist festzuhalten, dass „PacMan" mehr den je ein absoluter Knüller bei Groß und Klein war und damit „der" Publikumsmagnet. Aber auch „Monte Zuma", „Donkey Kong", „Summer Games", „JumpMan" sowie „H.E.R.O." erfreuten sich großer Beliebtheit. Auch waren die kleinen Besucher nicht tippfaul – viele haben sich dazu hinreißen lassen, den C64 selbst zu bedienen, um Spiele von der Floppy-Disk zu laden.

Fazit: Das große Engagement aller beteiligten Mitarbeiter der SUB und GWDG hat sich gelohnt und sie wurden mit jungen freudig-leuchtenden Augen belohnt.

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

Email 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.

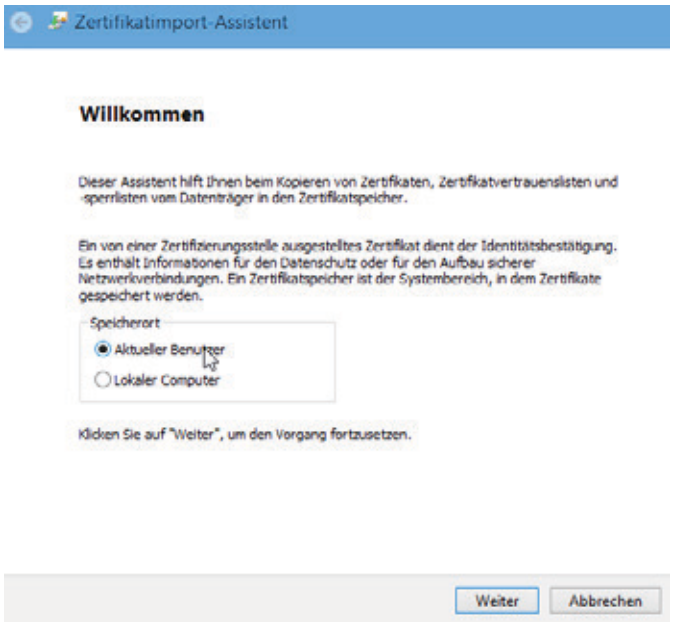


Abb. 1

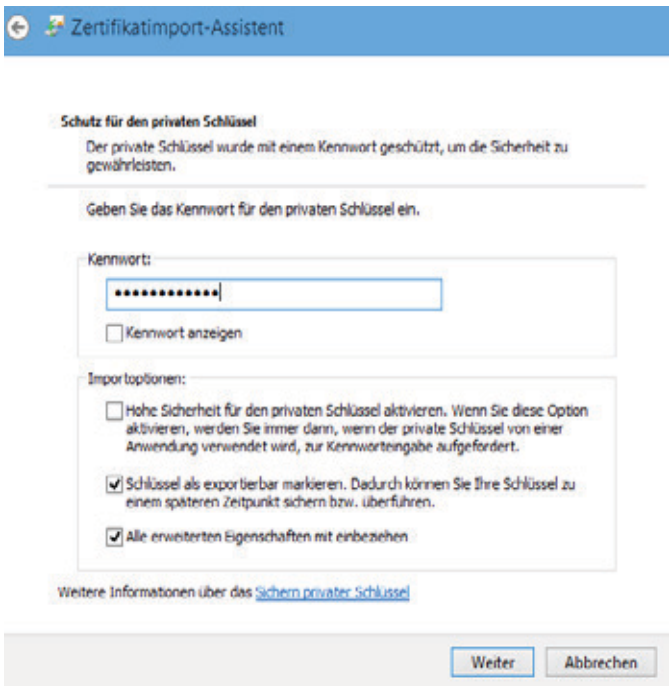


Abb. 2

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.

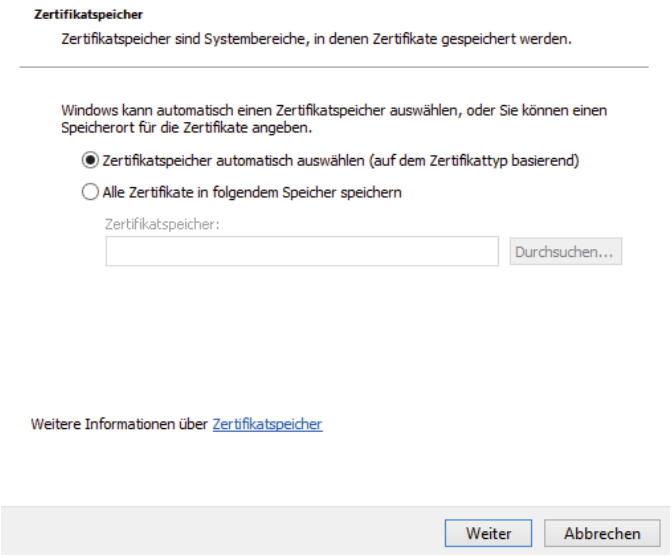


Abb. 3

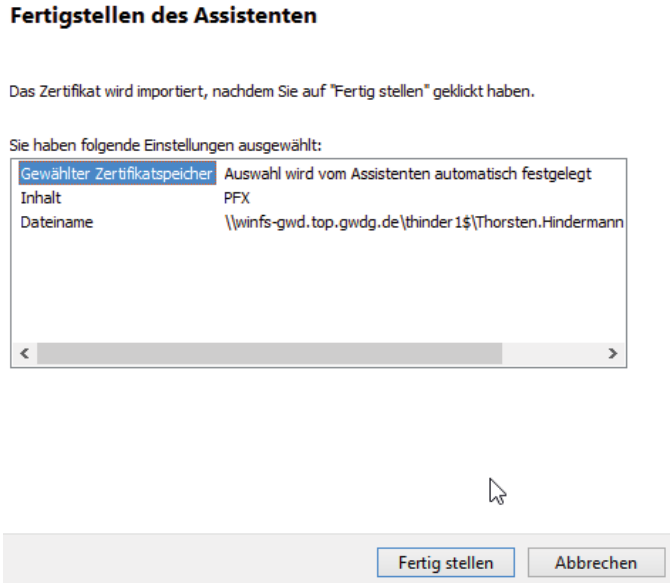


Abb. 4

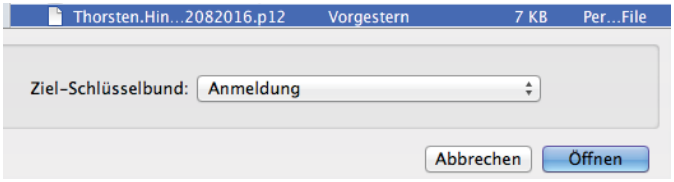


Abb. 5

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).

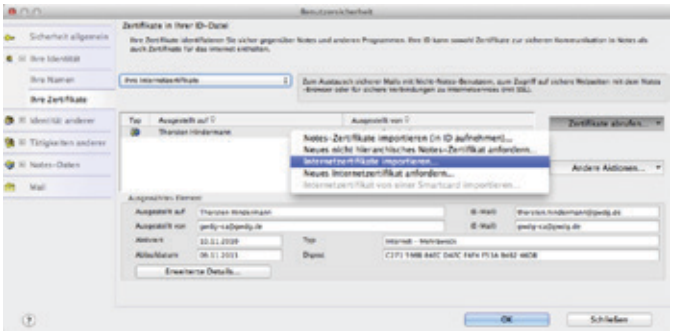


Abb. 6

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).

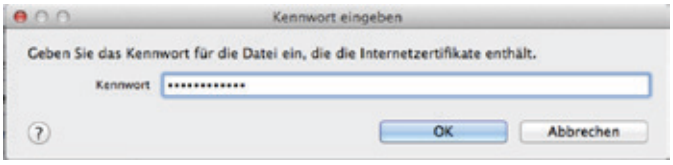


Abb. 8

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).

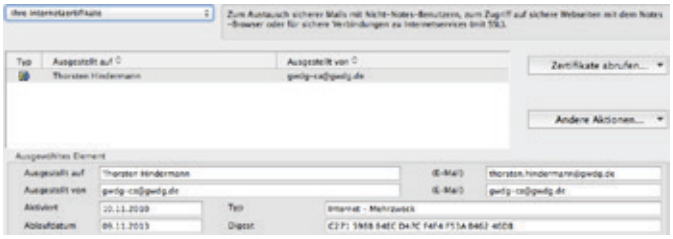


Abb. 9

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).

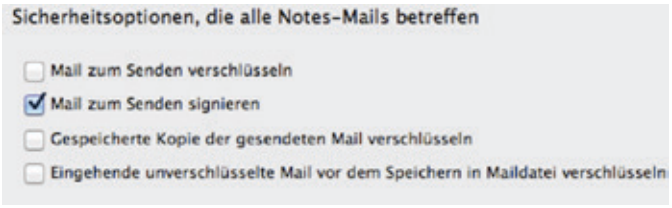


Abb. 10

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

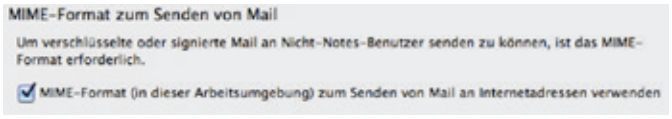


Abb. 11

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

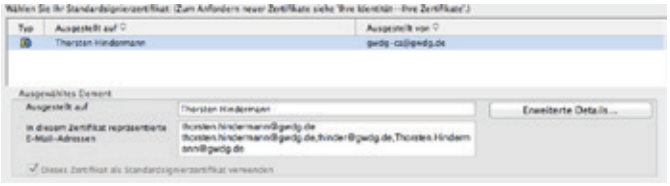


Abb. 12

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).

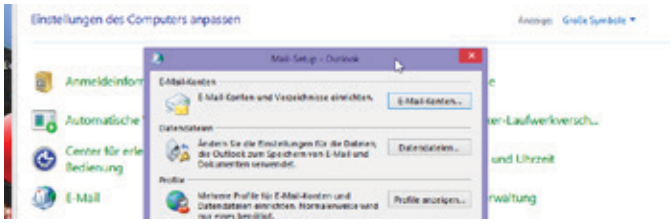


Abb. 13

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

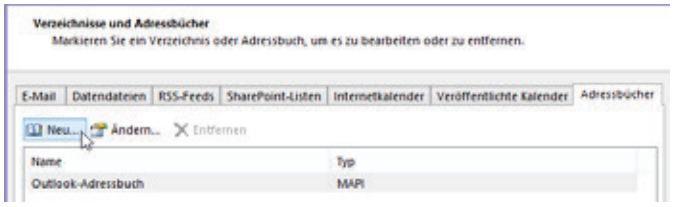


Abb. 14

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

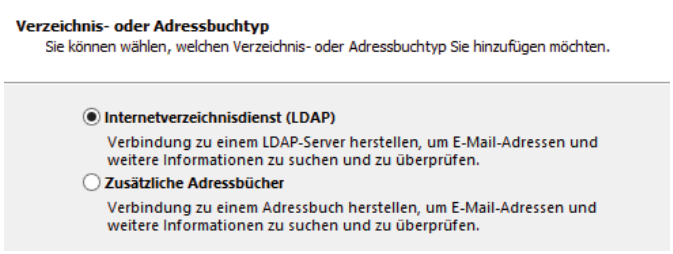


Abb. 15

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

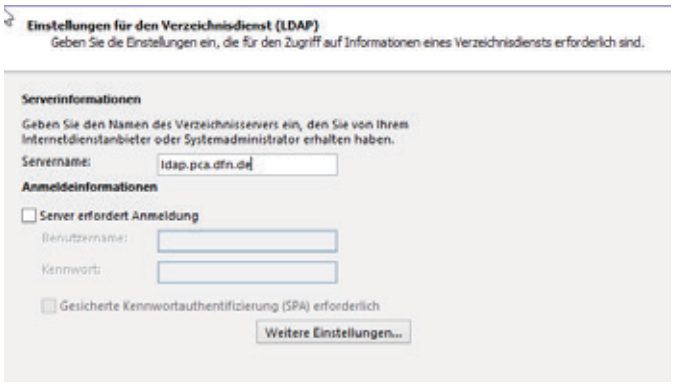


Abb. 16

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).

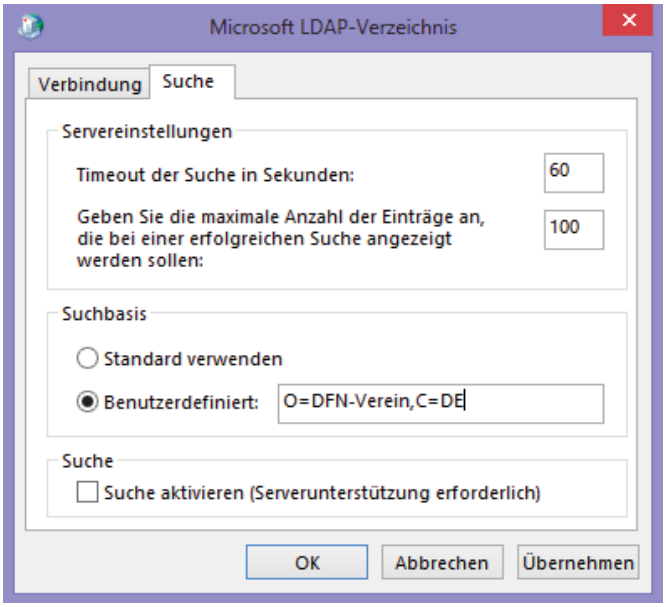


Abb. 17

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.

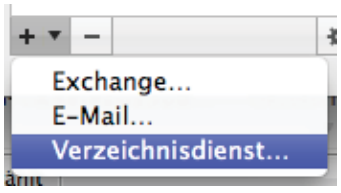


Abb. 18

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).

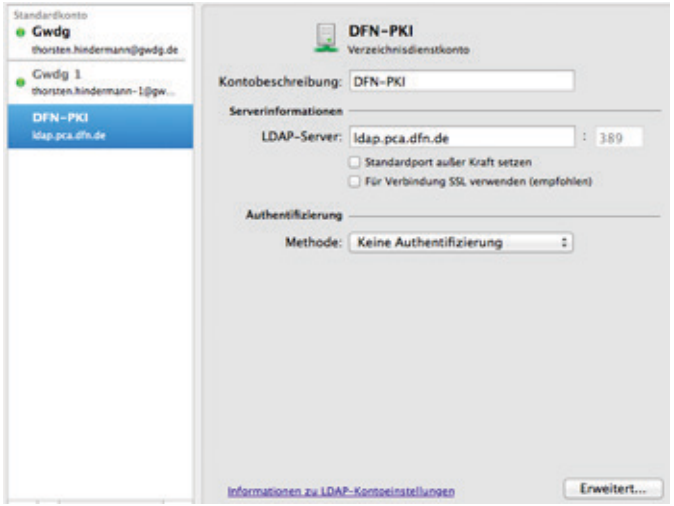


Abb. 20

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

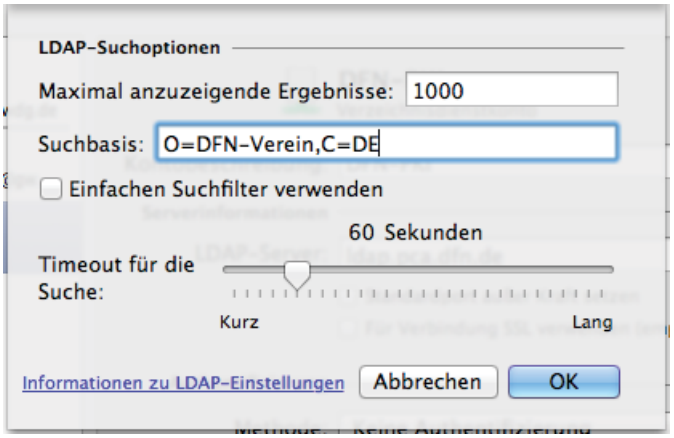


Abb. 21

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).

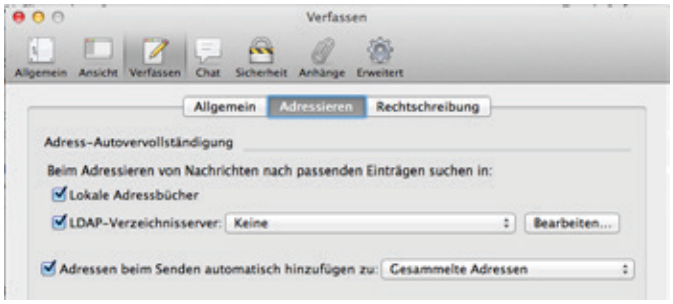


Abb. 25

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

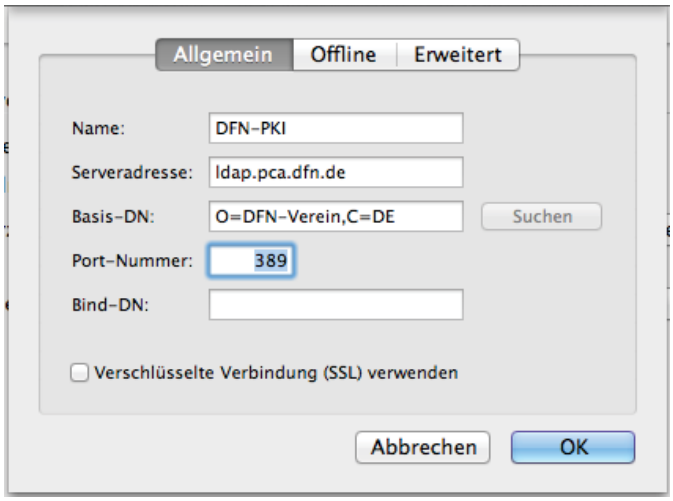


Abb. 26

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

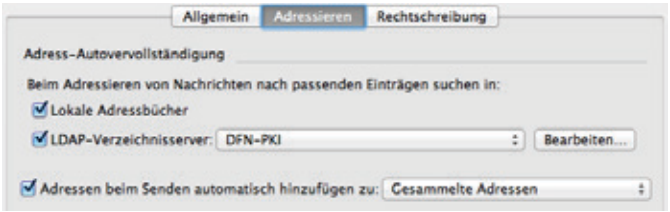


Abb. 27

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).

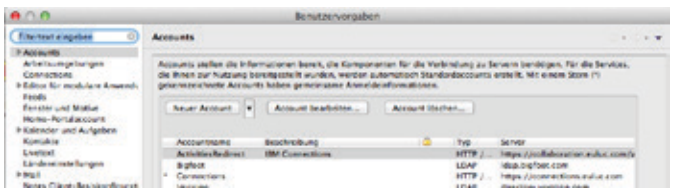


Abb. 28

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).

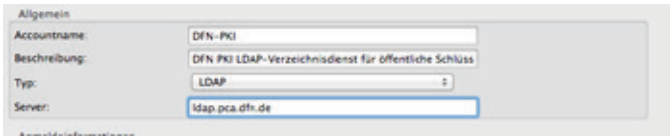


Abb. 29

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).

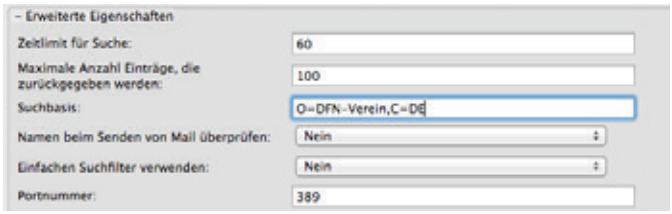


Abb. 30

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).

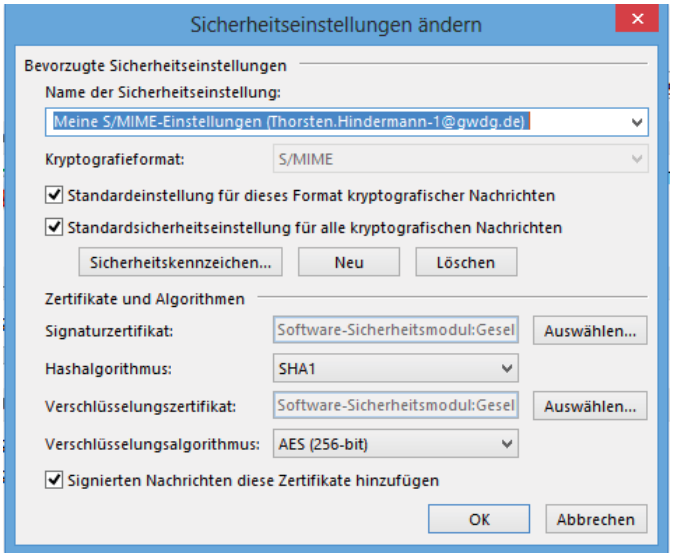


Abb. 31

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).

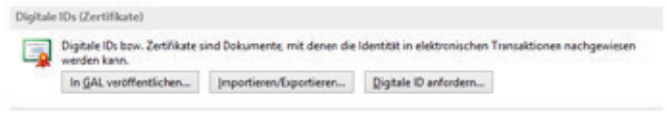


Abb. 32

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

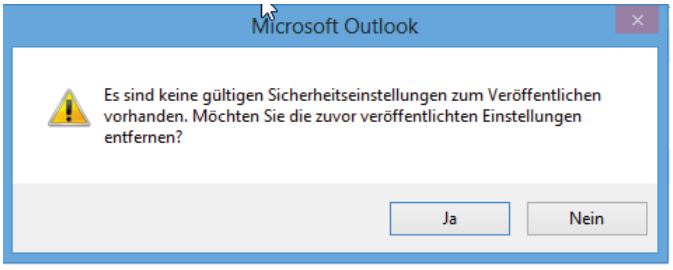


Abb. 33

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

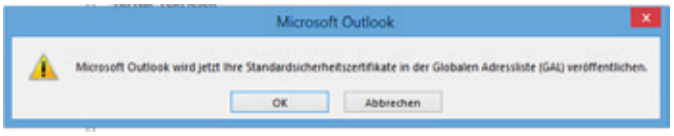


Abb. 34

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).

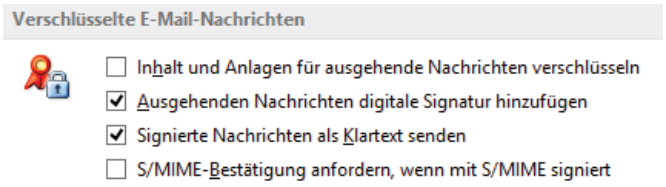


Abb. 36

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).

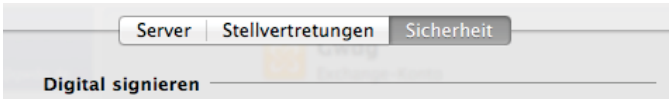


Abb. 37

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).

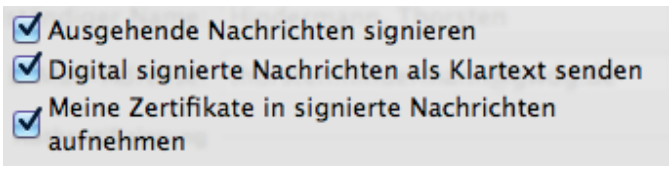


Abb. 38

INFORMATIONEN:
support@gwdg.de
0551 201-1523

Oktober bis Dezember 2013

Kurse

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
CLIENT-MANAGEMENT MIT BARAMUNDI	Becker, Körmer, Quentin, Rosenfeld	17.10.2013 9:00 – 12:30 und 13:30 – 15:30 Uhr	10.10.2013	4
INDESIGN – AUFBAUKURS	Töpfer	22.10. – 23.10.2013 9:30 – 16:00 Uhr	15.10.2013	8
UNIX FÜR FORTGESCHRITTENE	Dr. Sippel	04.11. – 06.11.2013 9:15 – 12:00 und 13:15 – 15:30 Uhr	28.10.2013	12
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	13.11. – 14.11.2013 9:00 – 12:00 und 13:00 – 15:30 Uhr	06.11.2013	8
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	19.11. – 20.11.2013 9:30 – 16:00 Uhr	12.11.2013	8
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	21.11.2013 9:00 – 12:30 und 13:30 – 15:30 Uhr	14.11.2013	4
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	27.11.2013 9:15 – 16:30 Uhr	20.11.2013	4
EINFÜHRUNG IN DAS IP-ADRESSMANAGEMENTSYSTEM DER GWDG FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	28.11.2013 10:00 – 12:00 Uhr	21.11.2013	2
UNIX/LINUX-ARBEITSPLATZRECHNER – INSTALLATION UND ADMINISTRATION	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	02.12. – 03.12.2013 9:15 – 12:00 und 13:30 – 16:00 Uhr	25.11.2013	8

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
UNIX/LINUX-SERVER – GRUNDLAGEN DER ADMINISTRATION	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	04.12. – 05.12.2013 9:15 – 12:00 und 13:30 – 16:00 Uhr	27.11.2013	8
UNIX/LINUX – SYSTEMSICHERHEIT FÜR ADMINISTRATOREN	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	06.12.2013 9:15 – 12:00 und 13:30 – 15:00 Uhr	29.11.2013	4
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	11.12. – 12.12.2013 9:00 – 12:00 und 13:00 – 15:30 Uhr	04.12.2013	8

Teilnehmerkreis
Das Kursangebot der GWDG richtet sich an alle Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus einigen anderen wissenschaftlichen Einrichtungen.

Anmeldung
Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@ gwdg.de* erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/antragsformulare* ein Formular zur Verfügung. Telefonische Anmeldungen können leider nicht angenommen werden.

Kosten bzw. Gebühren
Unsere Kurse werden wie die meisten anderen Leistungen der GWDG in Arbeitseinheiten (AE) vom jeweiligen Institutskontingent abgerechnet. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

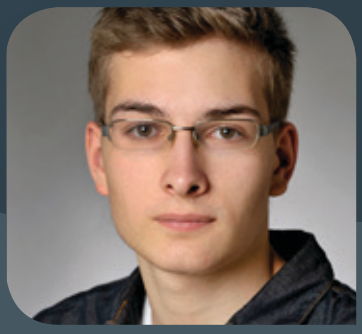
Absage
Sie können bis zu acht Tagen vor Kursbeginn per E-Mail an *support@gwdg.de* oder telefonisch unter 0551 201-1523 absagen. Bei späteren Absagen werden allerdings die für die Kurse berechneten AE vom jeweiligen Institutskontingent abgebucht.

Kursorte
Alle Kurse finden im Kursraum oder Vortragsraum der GWDG statt. Die Wegbeschreibung zur GWDG sowie der Lageplan sind unter *http://www.gwdg.de/lageplan* zu finden.

Kurstermine
Die genauen Kurstermine und -zeiten sowie aktuelle kurzfristige Informationen zu den Kursen, insbesondere zu freien Plätzen, sind unter *http://www.gwdg.de/kurse* zu finden.

Personalia

NEUER AUSZUBILDENDER NIKOLAS KOPP



Am 1. September 2013 hat Herr Nikolas Kopp seine 3½-jährige Ausbildung zum „Elektroniker für Geräte und Systeme" in der Arbeitsgruppe „Basisdienste und Organisation" bei der GWDG begonnen. Nach dem Schulpraktikum in der 10. Klasse, das er bei der GWDG absolviert hatte, war sein Interesse für diesen Beruf geweckt. Am Eichsfeld-Gymnasium Duderstadt hat er den erweiterten Sekundarabschluss I erworben. Herr Kopp ist per E-Mail unter *nikolas.kopp@gwdg.de* und telefonisch unter 0551 201-1533 zu erreichen.

Gutsch


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen