

GWDG NACHRICHTEN 11|13

E-Mail-Verschlüsselung

iOS 7 für iPhone und iPad

30. DV-Treffen der
Max-Planck-Institute

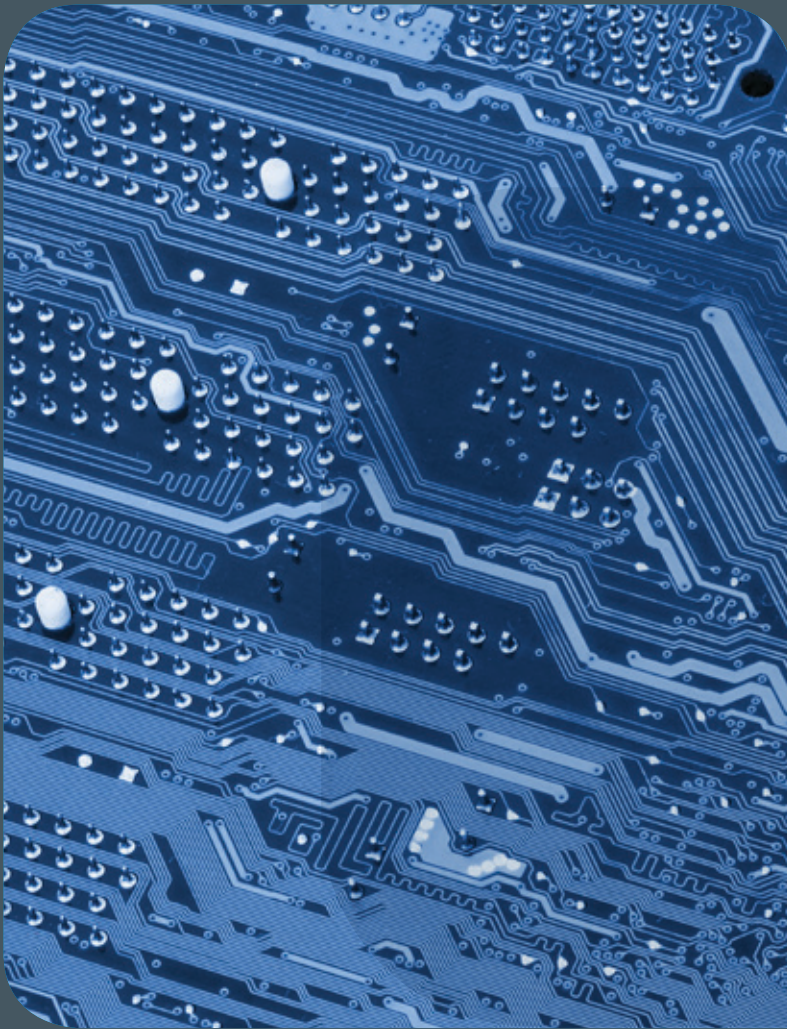
MOMoT

Kurse 2014

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG



GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen



GWDG NACHRICHTEN

11|13 Inhalt

.....
4 **E-Mail-Verschlüsselung mit X.509-Zertifikaten**

– Teil 3: Outlook-E-Mail-Anwendungen

9 **iOS 7 für iPhone und iPad** 11 **30. DV-Treffen der**

Max-Planck-Institute in Göttingen

13 **MOMoT: A GÉANT Open Call project**

17 **Kurz & knapp** 18 **Personalia** 20 **Kurse**

Impressum

.....
Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
36. Jahrgang
Ausgabe 11/2013

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
500

Fotos:
© Nmedia - Fotolia.com (1)
© emevil - Fotolia.com (10)
© Edelweiss - Fotolia.com (12)
© xiaoliangge - Fotolia.com (13)
© vege - Fotolia.com (19)
© MPLbpc-Medienservice (3, 18, 19)
GWDG (2, 11, 17, 20)

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,

dass die Energiekosten einen steigenden Anteil der Gesamt-IT-Kosten ausmachen, ist mittlerweile allgemein bekannt. Neben Maßnahmen zur Energieeinsparung zeichnet sich auch ab, dass künftig ein optimierter Stromeinkauf und eine optimierte Stromerzeugung wichtig werden, um diesen Kostensteigerungen entgegenzuwirken.

Weniger beachtet wird jedoch, dass sich aufgrund von einigen Quasi-Monopolstellungen bei Software teilweise massive Kostensteigerungen abzeichnen. Die Gründe hierfür sind ganz unterschiedlich: Manche Produkte haben sich als erste Wahl bewährt oder als De-facto-Standard entwickelt. In anderen Bereichen ist ein Produktwechsel mit großem Aufwand und hohen Kosten verbunden. Dies führt zu einer Abhängigkeit, die Anbieter zunehmend ausnutzen, um höhere Preise durchzusetzen.

Die Gegenmaßnahmen sind zwar beschränkt, aber damit dennoch wichtig. So wird stärker zu hinterfragen sein, ob eine bestimmte Software unbedingt notwendig ist und ob in manchen Fällen nicht auch eine alternative Lösung, ggf. mit Abstrichen, ausreichend ist. Solche Alternativen müssen aktiv verfolgt und entwickelt werden. Vor Verhandlungen mit Software-Anbietern ist frühzeitig ein realistisches Alternativszenario zu entwickeln, um handlungsfähig zu bleiben. Open Source könnte hier eine wichtige Bedeutung zukommen, die man aktiv fördern kann.

Dennoch wird wichtige und notwendige Software natürlich anhand der Bedürfnisse aus der Wissenschaft ausgewählt und bereitgestellt werden müssen.

Damit ist jedoch auch klar: Günstiger wird es künftig nicht.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

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 application s

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 angeschlossenen (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 Schlüssel 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.

„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).

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).

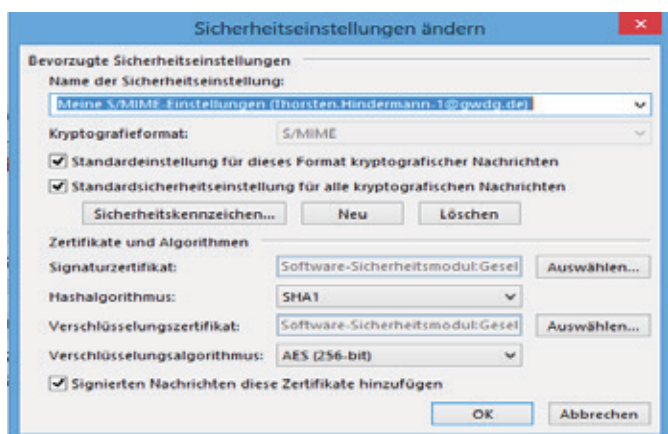


Abb. 1

Hinweis: Existiert zu diesem Zeitpunkt mehr als ein Zertifikat, dann jeweils unter Gruppe „Zertifikate und Algorithmen“ bei

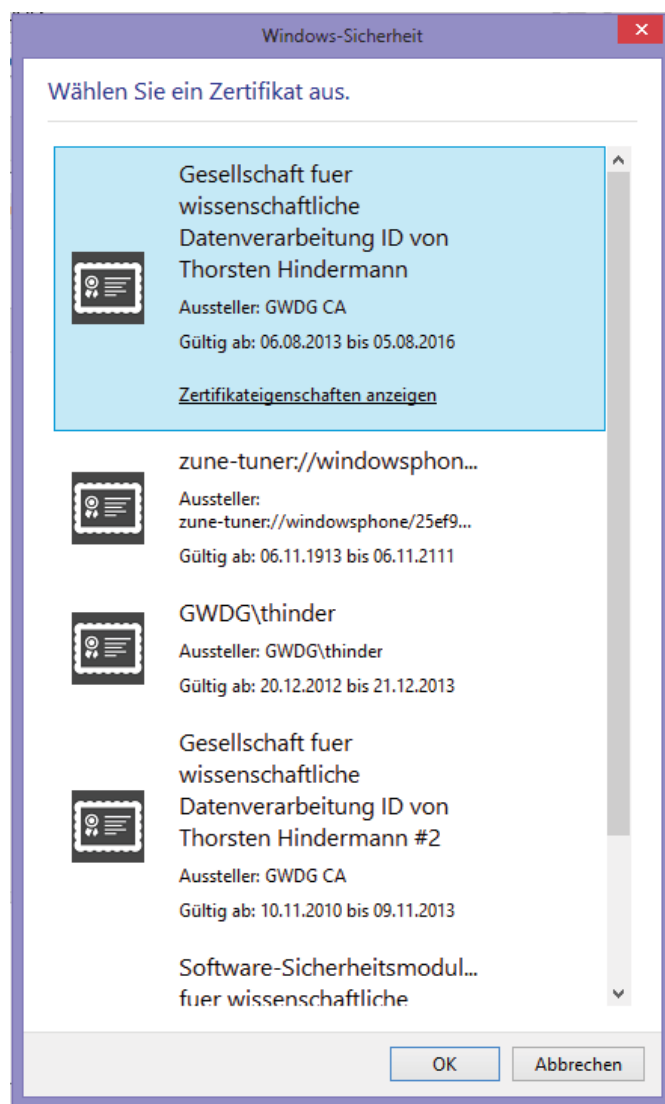


Abb. 2

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).

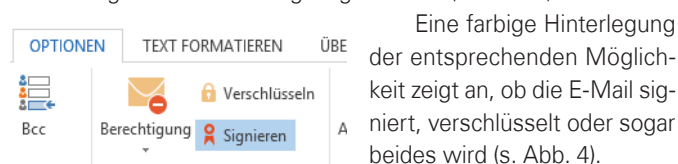


Abb. 3

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 eingetragene 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).

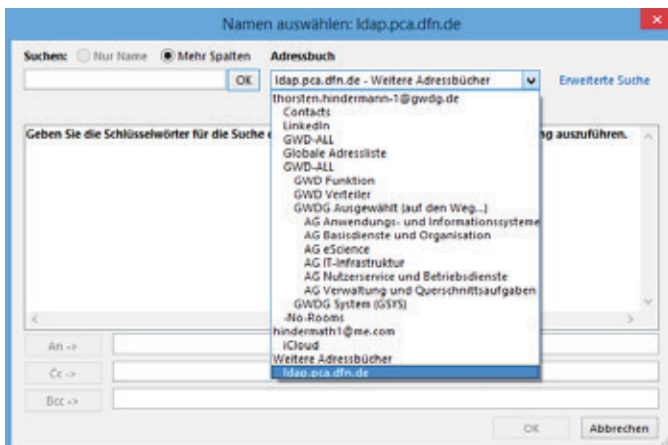


Abb. 6

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).

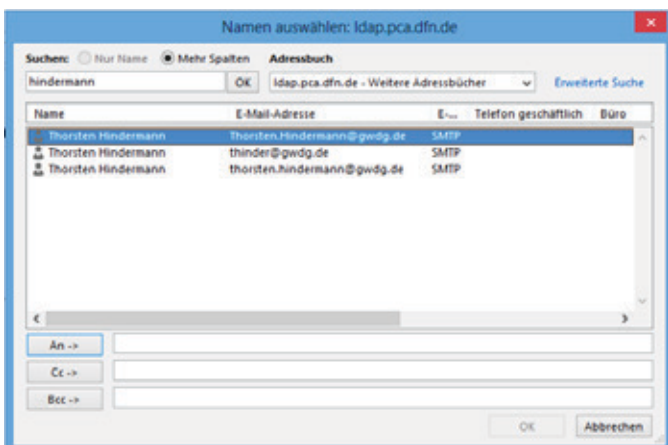


Abb. 7

2011 für Mac OS X

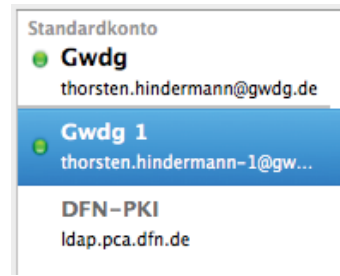


Abb. 8

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).

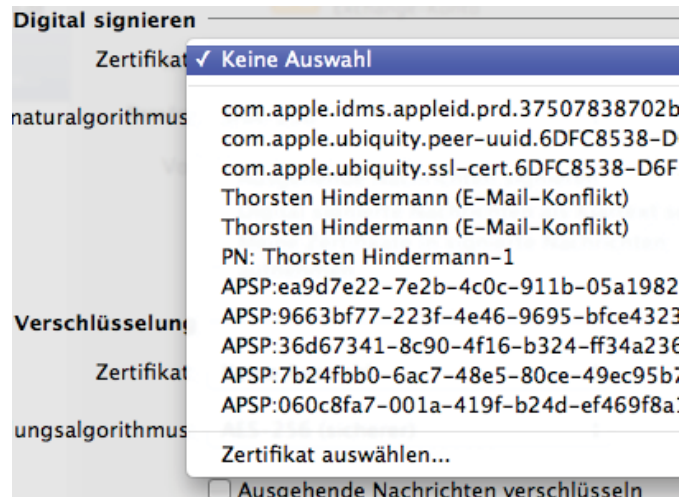


Abb. 9

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).

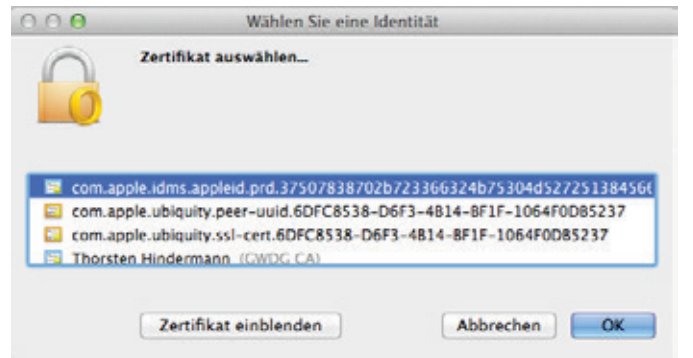


Abb. 10

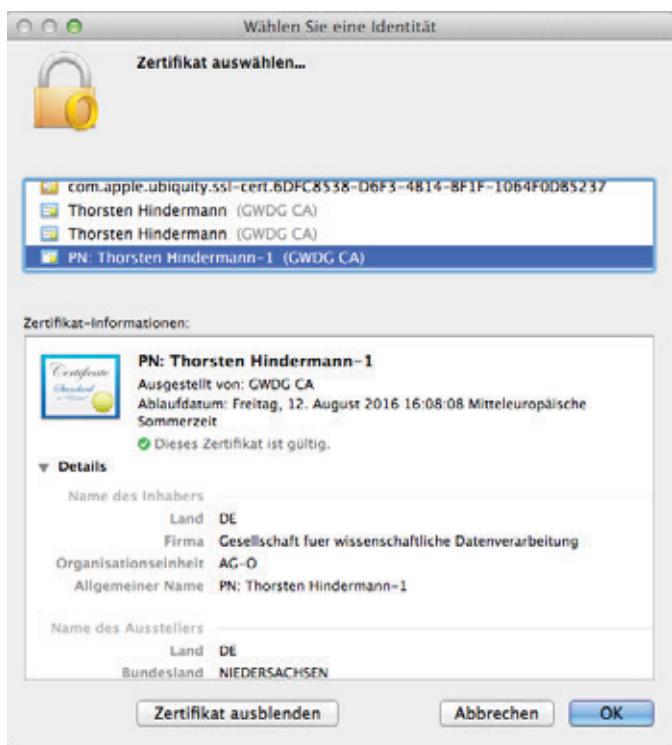


Abb. 11

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).

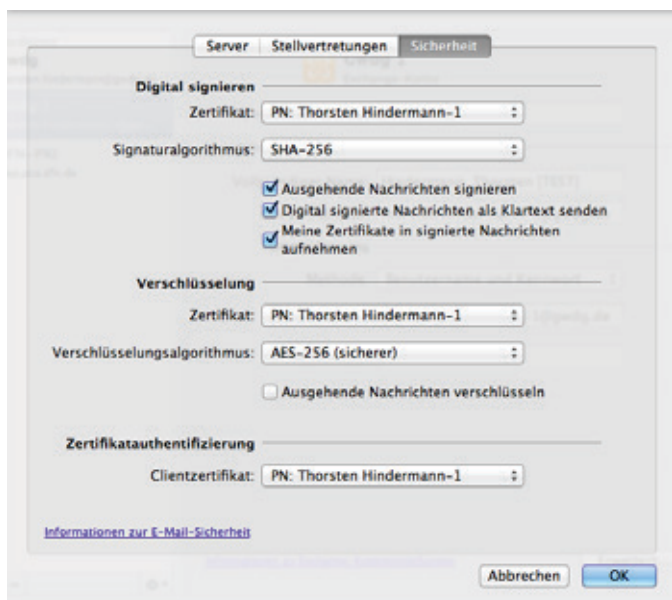


Abb. 12

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).

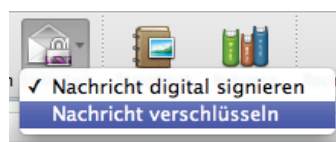


Abb. 13

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-Verzeichnissever 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-Verzeichnissever mit der Beschriftung „DFN-PKI Verzeichnis“ ausgewählt werden.

Jetzt den E-Mail-Empfänger 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).

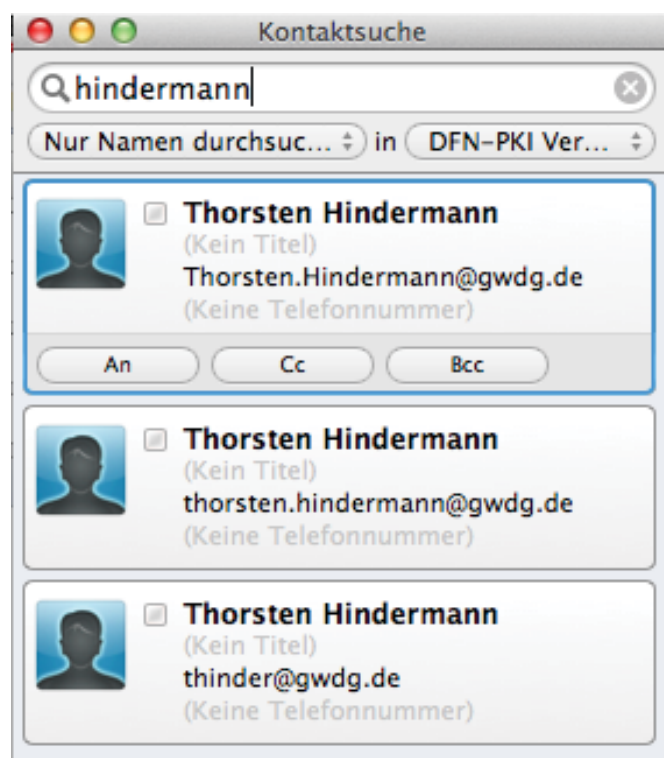


Abb. 15

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.

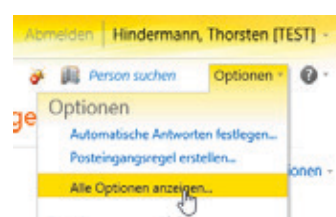
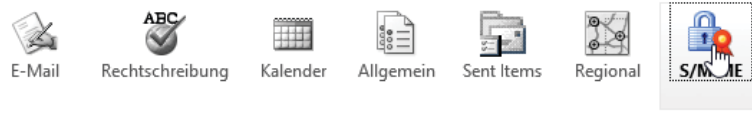


Abb. 16

Als erstes muss der Anwender überprüfen, ob das ActiveX-Steuerelement installiert ist. Dazu im OWA auf „Optionen > Alle Optionen anzeigen...“ klicken (s. Abb. 16).

E-Mail > Optionen

- Konto
- E-Mail organisieren
- Gruppen
- Einstellungen**
- Telefon
- Blockieren oder zulassen



E-Mail-Sicherheit

Mit S/MIME können Sie zu sendende E-Mail-Nachrichten verschlüsseln und digital signieren, verschlüsselte Inhalte in empfangenen Nachrichten anzeigen und die digitalen Signaturen von Absendern überprüfen.

Auf diesem Computer ist das S/MIME-Steuerelement nicht installiert. Sie können es herunterladen, indem Sie auf den Link unten und dann im angezeigten Internet Explorer-Dialogfeld auf "Ausführen" klicken.

[S/MIME-Steuerelement herunterladen](#)

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-Gruppenrichtlinie 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).

Zertifikat für die Nachrichtensignierung auswählen ^

- Outlook Web App gestatten, automatisch das beste Zertifikat auszuwählen
- Zertifikat manuell auswählen

Zurzeit ausgewähltes Zertifikat: **Keine**

[Signaturzertifikat auswählen](#)

Abb. 19

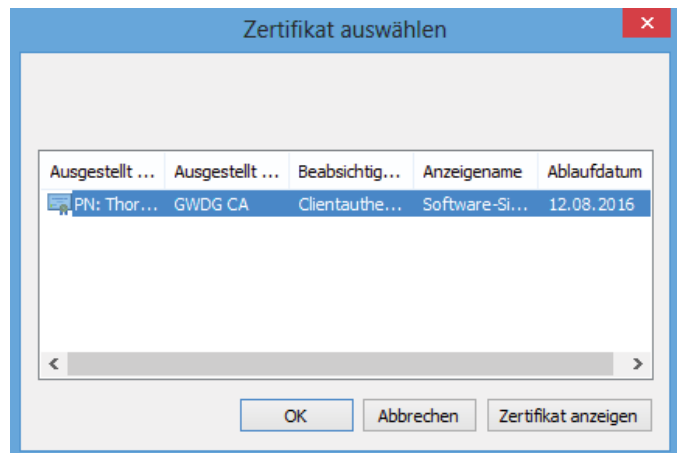


Abb. 20

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).



Abb. 22

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

iOS 7 für iPhone und iPad

Text und Kontakt:

Michael Reimann
michael.reimann@gwdg.de
0551 201-1826

Apple hat am 18. September 2013 für seine mobilen Geräte iPhone (ab 4), iPad (ab 2. Generation), iPad mini und iPod Touch (5. Generation) die Aktualisierung des Betriebssystems auf iOS 7 bereitgestellt. Dieses umfangreiche Update wird für alle Kunden kostenlos angeboten und wurde nach Aussage des Herstellers bereits nach nur vier Tagen von 200 Millionen Anwendern geladen. Es enthält zahlreiche neue Funktionen, von denen die interessantesten hier kurz vorgestellt werden sollen.

NEUES DESIGN

Am auffälligsten ist sicherlich die völlig überarbeitete neue Benutzeroberfläche und in diesem Zusammenhang die Hinwendung zu einem flachen, transparenten Design unter weitgehendem Verzicht auf skeuomorphe Designelemente. Darunter versteht man grafische Elemente, die Objekte aus der Wirklichkeit nachempfinden, wie z. B. die Ledereinbände des Kalenders, die Bücherregale und die Notizpapieroptik. Die komplett neue Design-Ausrichtung führte auch dazu, dass sich viele Entwickler mit Neuauflagen ihrer Anwendungen im App Store präsentierten, was zu einer wahren Update-Flut führte. Darunter befinden sich auch Anwendungen, die nicht nur das neue Bedienkonzept verinnerlichen, sondern darauf aufbauend auch neue Funktionen implementieren.

AKTIVIERUNGSSPERRE

Ein wichtiger Aspekt in iOS 7 ist die Sicherheit und darunter der verbesserte Diebstahlschutz. Neben der bereits vorhandenen Möglichkeit, verlorene Geräte über die iCloud zu orten, zu löschen und zu sperren, wurde jetzt mit der neuen Aktivierungssperre ein Weg gefunden, über den ein Zurücksetzen entwendeter Geräte und die anschließende Neuaktivierung nicht mehr so ohne Weiteres möglich sind. Die überarbeitete „Mein iPhone suchen“-Funktion (in: „Einstellungen > iCloud > Mein iPhone suchen“) verbindet diese Aktionen nun mit der Apple ID und dem dazugehörigen Passwort. Ohne deren Kenntnis ist somit ein Löschen oder Wiederherstellen des Gerätes unmöglich. Damit wird der unrechtmäßige Besitz oder gar die Veräußerung des Gerätes erheblich erschwert. Das bedeutet aber zugleich auch, dass diese Sperre immer deaktiviert werden muss, bevor das Gerät rechtmäßig den Besitzer wechselt. Potenzielle Käufer sollten ebenfalls darauf achten, dass die Verknüpfung der Aktivierungssperre mit der Apple ID zuvor entfernt wurde. Sinnvoll ist in derartigen Fällen vermutlich ohnehin gleich eine Komplettlöschung (über: „Einstellungen > Allgemein > Zurücksetzen“ und dort dann „Inhalte & Einstellungen löschen“). Die Sperre lässt sich vom Besitzer übrigens

auch über die „Mein iPhone suchen“-Funktion in <https://www iCloud.com> aus der Ferne aufheben, vorausgesetzt es besteht eine Netzwerkverbindung. Näheres hierzu erläutert Apple auch in einem speziellen Support-Dokument: http://support.apple.com/kb/HT5661?viewlocale=de_DE

CONTROL CENTER

Um sich nicht in dem inzwischen doch recht umfangreichen Einstellungsmenü zu verlieren, wurden in iOS 7 nun die wichtigsten Systemeinstellungen herausgezogen und in dem neuen „Control Center“ an einem zentralen Ort zusammengeführt. Dies erreicht man mit einer Wischgeste von der Unterseite des Bildschirms nach oben und erhält so unter anderem Zugriff auf den Flugmodus, WLAN, Bluetooth, den „Nicht Stören“-Modus, die Bildschirmhelligkeit und Lautstärke sowie die Möglichkeit, auf Air-Play-Geräte zuzugreifen. Aus Sicherheitsgründen sollte man den Zugriff vom Sperrbildschirm aus unterbinden (in: „Einstellungen > Kontrollzentrum > Zugriff im Sperrbildschirm“), da in der Vergangenheit immer wieder Wege entdeckt wurden, darüber tiefer ins System vorzudringen. Eine solche Schwachstelle hat bereits zum Update auf 7.0.2 geführt.

MITTEILUNGSZENTRALE

Die der aus Android bekannten Benachrichtigungsleiste nachempfundene Mitteilungszentrale wurde in iOS 7 noch einmal erweitert und bietet je nach Konfiguration eine Zusammenfassung

iOS 7 for iPhone and iPad

Apple has released iOS 7 on 18 September 2013 for its mobile devices iPhone, iPad and iPod Touch (5th Gen.). This large update is offered for free for all customers and was downloaded by 200 million users after only four days. Here we will show some of the important features.



verschiedener (tagesaktueller) Ereignisse (Termine, Erinnerungen und aktuelles Wetter) sowie die Meldungen der in der Mitteilungsansicht aufgenommenen Anwendungen. Sie findet sich erstmalig auch im Sperrbildschirm, dies kann aber auf Wunsch deaktiviert werden (in: „Einstellungen > Mitteilungen“).

WEITERENTWICKELTES MULTITASKING

In iOS 6 gestaltete es sich doch recht umständlich, im Hintergrund laufende Anwendungen zu ermitteln und sie gegebenenfalls zu beenden. Dieser Vorgang wurde in iOS 7 verbessert, indem nun durch den gewohnten Doppelklick auf den Home-Button für jede im Hintergrund laufende App kleine Vorschaubilder erscheinen, die sich mittels einer horizontalen Wischgeste durchblättern lassen, um so entweder das Wechseln oder auch das Beenden von Apps zu erleichtern. Letzteres geschieht durch ein einfaches Nach-oben-Wischen. Weiterhin lässt es sich für die jeweiligen Apps bestimmen, ob sie im Hintergrund verschiedene Aktivitäten ausführen dürfen. Dies muss allerdings vom Entwickler vorgesehen sein. Einstellen lässt sich das in „Einstellungen > Allgemein > Hintergrundaktualisierung“. So lassen sich Anwendungen, die durch umfangreiche Hintergrundprozesse zuviel Ressourcen und damit auch kostbare Akku-Kapazität verbrauchen, leichter bändigen.

WEITERE NEUERUNGEN

Nutzer des Exchange 2010 Servers wird es freuen, dass in iOS 7 neben E-Mails, Terminen, Kontakten und Aufgaben endlich auch Notizen unterstützt und entsprechend synchronisiert werden können.

Die **Spotlight-Suche** ist jetzt auf allen Homescreens verfügbar und wird mit einer einfachen Wischgeste nach unten geöffnet.

Die in unregelmäßigen Abständen anfallenden Updates für die Apps werden jetzt erstmalig auch automatisch geladen. Wer diese Standardeinstellung nicht möchte, kann sie über „Einstellungen > iTunes & App Store > Updates“ auf Wunsch wieder deaktivieren.

Der Sprachassistent **Siri** ist nun dem Beta-Stadium entwachsen und bietet neben anderen Stimmen auch einen größeren Funktionsumfang.

Mit **AirDrop** lassen sich jetzt Inhalte einfacher auf andere Geräten über WLAN (im Ad-hoc-Modus) oder Bluetooth

übertragen. Die Datenübertragung ist vollständig verschlüsselt, beschränkt sich vorerst aber nur auf die Modelle iPhone 5, 5c, 5s, iPad mini, iPad 4 und iPod Touch (5. Generation).

UPDATE AUF 7.0.3

Aufgrund der oben bereits erwähnten Sicherheitslücke im iOS 7 war es möglich, den Sperrbildschirm zu überwinden und auf sensible Daten und Dienste zuzugreifen. Apple korrigierte dies sehr zügig mit einem Update auf 7.0.2. Kurz darauf wurde jedoch bereits eine weitere Schwachstelle entdeckt, die ebenfalls zur Umgehung der Bildschirmsperre genutzt werden konnte. Und auch hier reagierte Apple relativ zügig mit dem Update auf 7.0.3, das zudem noch weitere Fehler und Sicherheitslücken beseitigte. Auch wenn diese Gefahr erst einmal gebannt ist, empfiehlt es sich dennoch, die folgenden beiden Restriktionen vorzunehmen:

- Der Zugriff auf das Kontrollzentrum vom Sperrbildschirm aus sollte unterbunden werden (über: „Einstellungen > Kontrollzentrum > Zugriff im Sperrbildschirm“).
- Der Sprachassistent Siri sollte ebenfalls nicht vom Sperrbildschirm aus erreichbar sein, da er bisweilen doch ein wenig „geschwätzig“ ist (über: „Einstellungen > Allgemein > Code-Sperre > Siri“).

Ansonsten ist es nach wie vor dringend zu empfehlen, die Code-Sperre zu aktivieren. Wer bereits im Besitz des neuen iPhone 5S ist, kann stattdessen auch den dort verbauten Fingerabdruck-Scanner nutzen. Der bietet sicherlich keine absolute Sicherheit und wurde auch bereits überlistet. Aber als komfortable Alternative zu der von vielen Nutzern ungeliebten Code-Sperre taugt er allemal.

FAZIT

Die zahlreichen Vorteile von iOS 7, von denen hier nur eine kleine Auswahl aufgezeigt werden konnte, machen das Update empfehlenswert. Hinzu kommt, dass mit iOS 7 auch wieder viele, teils sogar kritische Sicherheitslücken geschlossen wurden. Dieser Gesichtspunkt wird gerade für mobile Geräte immer wichtiger, da durch deren ständig steigende Leistungsfähigkeit auch die Begehrlichkeit der Angreifer immer mehr geweckt wird. ■

30. DV-Treffen der Max-Planck-Institute in Göttingen

Text und Kontakt:
Dr. Thomas Otto
thomas.otto@gwdg.de
0551 201-1828

Einmal im Jahr treffen sich IT-Spezialisten aus nahezu allen Max-Planck-Instituten und weiteren Einrichtungen der Max-Planck-Gesellschaft zu ihrem traditionellen DV-Treffen. Das Treffen fand in diesem Jahr zum 30. Mal statt und kehrte von den Ausflügen nach Bonn in den beiden letzten Jahren zum Jubiläumstreffen zurück nach Göttingen. Tagungsort war das InterCityHotel am Bahnhof und die GWDG fungierte wie immer, wenn das DV-Treffen in Göttingen stattfindet, als lokaler Organisator. Knapp 160 Teilnehmer erlebten vom 24. bis 26. September ein abwechslungsreiches Programm mit vielen interessanten Vorträgen zu aktuellen IT-Themen.

BREITES THEMENSPEKTRUM

Das DV-Treffen der Max-Planck-Institute richtet sich an alle IT-Mitarbeiter und IT-Interessierte innerhalb der Max-Planck-Gesellschaft. Sinn und Zweck des Treffens sind vor allem der Austausch von Ideen und Erfahrungen, das Erkunden von Trends und neuen Entwicklungen und nicht zuletzt das Knüpfen von Kontakten zwischen den Instituten.

In zahlreichen Vorträgen und drei parallelen Workshops wurde ein breites Spektrum von aktuellen Themen behandelt. Hierzu gehörten u. a. ITIL, IT-Sicherheit, Datenmanagement, Open-Source-Lösungen, IPv6 und Identity Management. Die zentralen IT-Dienstleister der Max-Planck-Gesellschaft – GWDG, RZG und MPDL – informierten über ihre Neuigkeiten und stellten dabei

insbesondere neue Dienste für die Max-Planck-Institute vor. Im Rahmen einer zweistündigen Podiumsdiskussion wurde das Thema „IT-Organisation im Spannungsfeld zwischen Cloud-Computing und Institutsautonomie“ kontrovers erörtert.

Alle Vorträge machten wieder eines besonders deutlich: Ohne eine leistungsfähige und innovative IT-Infrastruktur ist keine Spitzenforschung in allen Wissenschaftsbereichen der Max-Planck-Gesellschaft möglich. Die IT-Abteilungen der Max-Planck-Institute stellen zusammen mit den wissenschaftlichen Rechenzentren der MPG die dafür notwendige IT-Infrastruktur bereit. Das DV-Treffen spielt dabei eine wichtige Rolle als Plattform für die Kommunikation und den Informationsaustausch zwischen allen beteiligten IT-Einrichtungen. Das wurde wieder einmal mehr deutlich.



VERLEIHUNG DES COMMUNITY AWARDS

Seit dem Jahr 2010 wird bei den DV-Treffen der IT Community Award verliehen. Er würdigt Personen, die einen wesentlichen Beitrag zur Förderung des Community-Gedankens in der IT der MPG geleistet haben. Mit diesem Preis soll die Anerkennung der IT Community zum Ausdruck gebracht werden, dass der Beitrag vielen geholfen hat, ihre Arbeit besser und erfolgreicher zum Ziel zu bringen. In diesem Jahr gibt es zwei Preisträger: Armin Burkhard vom MPI für Festkörperforschung aus Stuttgart für seinen langjährigen Einsatz bei den TSM-Rahmenvertragsverhandlungen und Michael Reimann von der GWDG für die Pflege von wichtigen Mailinglisten wie z. B. gwdg-sec, die den IT-Alltag für viele vereinfachen.

Das nächste 31. DV-Treffen soll im kommenden Jahr vom 16. bis 18. September im Harnack-Haus in Berlin stattfinden. ■

30. IT Meeting of the Max Planck Institutes in Göttingen

Once a year, IT specialists meet from almost all Max Planck Institutes and other institutes of the Max Planck Society for their traditional IT meeting. The meeting was held this year for the 30th time. After the excursions to Bonn in the last two years it returned to Göttingen for the anniversary meeting. The venue was the InterCityHotel at the station and the GWDG acted as the local organizer as always, if the IT meeting is held in Göttingen. Nearly 160 participants experienced a varied program with many interesting presentations on current IT topics from 24 to 26 September.



Servervirtualisierung

Der einfache Weg zum Server!

Ihre Anforderung

Sie benötigen zur Bereitstellung eines Dienstes einen Webserver, Datenbankserver oder Applikationsserver. Ihnen fehlen Platz, Hardware, Infrastruktur oder Manpower. Gleichzeitig soll der Server möglichst hochverfügbar und performant sein.

Unser Angebot

Wir bieten Ihnen die Möglichkeit des Hostings von virtuellen Servern unter VMware.

Ihre Vorteile

- > Leistungsfähiges VMware-Cluster mit zugehörigem Massenspeicher
- > Hohe Ausfallsicherheit und Verfügbarkeit durch redundante Standorte und Netzwerkverbindungen sowie USV-Absicherung

- > Bereitstellung aller gängigen Betriebssysteme zur Basisinstallation
- > Umfassender administrativer Zugang zu Ihrem Server im 24/7-Selfservice
- > Möglichkeit der automatisierten Sicherung des Servers auf unsere Backupsysteme
- > Zentrales Monitoring durch die GWDG
- > Große Flexibilität durch Virtualisierungstechnologien wie Templates, Cloning und Snapshots
- > Schutz vor Angriffen aus dem Internet durch leistungsfähige Firewallsysteme sowie ein Intrusion Prevention System

Interessiert?

Um einen virtuellen Server zu beantragen, nutzen Sie bitte die Webadresse

>> www.gwdg.de/virtuelle-server



MOMoT: A GÉANT Open Call project

Text und Kontakt:

Dr. Siamak Azodolmolky
siamak.azodolmolky@gwdg.de
0551 201-2160

In response to the GÉANT's Open Call for project proposal, GWDG (eScience research group) and Technical University of Denmark (Department of Photonics Engineering, DTU Fotonik) prepared and submitted a project proposal, which is successfully accepted and has been effectively started since 24 October 2013. This project proposal is titled "Multi-Domain Optical Modelling Tool" (MOMoT). It will investigate the potential of providing an Alien Wavelength (AW) service in the GÉANT network, which will contribute to the fulfilment of the requirements for the Digital Agenda for Europe. MOMoT investigates the actual interests and needs for an AW service platform. Tailored to these needs, a multi-domain modelling tool will be developed, which will facilitate the deployment of Alien Wavelengths in the NRENs and the GÉANT network throughout Europe. In the future, this web-based tool can be also used by GWDG's customers to evaluate the quality of their network, especially in interconnection scenarios. This article provides a brief introduction to the MOMoT project and its major outcomes.

INTRODUCTION

GÉANT is the pan-European research and education network that interconnects Europe's National Research and Education Networks (NRENs). It connects over 50 million users at 10,000 institutions across Europe, supporting research in areas such as energy, the environment, space and medicine. The GÉANT network and associated services comprise the GN3plus project, made up of 41 partners and co-funded by the European Union under EU FP7 program. The work of the GN3plus project is divided into 14 Activities within three areas of work: Research; Service Development and Delivery; Coordination and outreach. Networking Activities (NAs) support all GN3plus Activities with the full extent of both internal and external communications, international liaison, promotion, and

business development. Service Activities (SAs) develop and supply the GÉANT services to the research and education community. Joint Research Activities (JRAs) are targeted at critical analyses of future network and application technologies with a view to future deployment of emerging technologies across the network and services. A summary of GN3plus activities and the overall structure of them are shown in the figure on the next page.

Specialised Advisory Boards offering support to the Activity Leaders ensure that decision making is highly efficient and the voice of the stakeholder community is heard at operational level. The Quality Assurance and Public and External Relations Committee (QASPER) carry out the quality assurance of GN3plus deliverables, both for the European Commission and internally. It also ensures that the results of the programme and its deliverables are promoted effectively. In

JRA1: Network Architectures for Horizon 2020		SA1: Core Backbone Services	
		SA2: Testbeds as a Service	
JRA2: Technology Testing for Specific Service Applications		SA3: Network Service Delivery	
		SA4: Network Support Services	
JRA3: Identity & Trust Technologies for GÉANT Services		SA5: Application Services	
		SA7: Support to Clouds	
SA6: Service Management & Operation			
NA1: Management	NA2: Communications & Promotion	NA3: Status & Trends	NA4: International & Business Development

line with its description of work, GN3plus announced its first open call for proposal on 1 April 2013, which was closed on 29 May 2013. There were 18 topics in the mentioned Open Call. eScience research group of GWDG (AG E) and department of Photonics of Technical University of Denmark shaped a consortium to prepare a project proposal targeting the Multi-domain Optical Modelling tool topic. In the GÉANT network, both photonic services and alien wavelengths present the challenge of delivering the same predictability and security as regular transmission services. In order to ensure these features, design and development of a multi-domain optical modelling tool is required. The proposal, coded as MOMoT, went through technical review and was successfully accepted. The effective start date of MOMoT is 24 October 2013 and its duration is 18 months. In the next section we briefly introduce this project and its technical goals.

MULTI-DOMAIN OPTICAL MODELING TOOL (MOMOT)

The MOMoT project will investigate the potential of providing an Alien Wavelength (AW) service in the GÉANT network which will contribute to the fulfilment of the requirements for the GN3plus open call and Digital Agenda for Europe. An Alien Wavelength is a Wavelength Division Multiplexed (WDM) frequency of light used for digital transport that is neither originating nor terminating on the system under consideration and is not native to the system and/or administrative domain under consideration. An alien wavelength could be an optical signal (wavelength or lambda), in the C, L, S, E, O or U band in the ITU grid, with 200, 150, 100, 50 and 25 GHz channel spacing on the WDM grid. An alien wavelength could be a signal from one vendor to another, from one network to another network domain in the same carrier network or from one carrier to another carrier network. In the scope of MOMoT project, a multi-domain modelling tool will be developed which will facilitate the deployment of Alien Wavelengths in the NRENS and the GÉANT network throughout Europe. Providing such a service will support

GÉANT’s main purpose of providing a seamless communication infrastructure throughout the European research community and to assure that research institutions can access and benefit as much as possible from the available resources. MOMoT will focus on:

- Assuring that existing traffic remains non-disrupted
- Assuring signal quality of alien wavelength throughout the network (i.e., Quality of Transmission)
- Privacy for NRENS (network topology)
- Planning and deployment of alien wavelengths

MOMoT proposes to develop a basic, functional and practical web-based modelling tool that will enable NRENS to evaluate the deployment of alien wavelengths. This means that a focus will be put on developing a tool that is functional and sufficient in serving the NRENS in exploiting the potential benefits of alien wavelengths, but without time extensive and complicated computations that requires detailed network data that would be impossible to collect and keep up-to-date. This approach is necessary and vital in the considered multi-domain network which encompasses a full variety of vendors and operators.

The partners of this proposal complement each other in a way that is very beneficial and assures the best grounds for reaching the objectives of GN3Plus Open Call. DTU will bring in extensive

MOMoT

Im Oktober dieses Jahres ist das Projekt „Multi-Domain Optical Modelling Tool“ (MOMoT), welches von GÉANT gefördert wird, gestartet. Die GWDG untersucht hier gemeinsam mit der Danmarks Tekniske Universitet die Möglichkeit, innerhalb des GÉANT-Netzwerkes einen Alien Wavelength (AW) Dienst bereitzustellen. Ein Ergebnis dieses Projektes wird ein webbasiertes Modellierungswerkzeug für Alien Wavelengths sein.

experience in network planning, multi-domain modelling as well as having practically worked with alien wavelength modelling (licensed tools) and live experiments in the GÉANT network for 2 years. GWDG has built up a yearlong experience within development of modelling tools which focus on physical aspects, including transmission impairments, and will bring in the expertise needed to develop a successful multi-domain modelling tool.

The idea for AWs began to draw attention within the NREN community around 2006-2007 when CESNET demonstrated the first deployment of an AW. Despite the numerous experiments in labs and field trials, very few deployments in production networks have been reported. Furthermore, there are no confirmed and public statements from network operators or equipment vendors for endorsement of the idea and commitment in the process of developing the idea further for practical use. Within the GÉANT community, the topic of deploying AWs has been around for about half a decade, where tasks focused on experiments, field trials and evaluation of the practical perspectives of deploying AWs as a service have been performed. Despite some positive features of the technology though, there does not seem to be a great interest within the NREN community which makes the further development of the technology almost useless. The main challenge with the AW paradigm as a service is uncertainty. Lack of control, lack of planning and deployment procedures, together with the fear of disruption of production services are pointed out as main drawbacks and show-stoppers.

MOMoT project will focus on designing and developing a tool for basic evaluation of AW deployment scenarios. In particular, the tool will take as input parameters the current state of a network, together with parameters related to existing services, and will evaluate the impact an AW deployment will have on the network, on its own performance and on the existing services. Such a tool will serve as a “back-of-the-envelope” calculation and evaluation of the feasibility to deploy an AW in a given network scenario. The tool will be developed with speed and effectiveness held in mind so instead of doing fully detailed and time consuming multi-channel simulations, a safe-zone approach will be applied meaning that the actual need for multi-channel simulation will be assessed. In the safe-zone cases, where multi-channel effects can be ruled out a single channel simulation will be sufficient whereas in other cases where there is risk of multi-channel effects, the user would be warned about this before proceeding. The project will investigate different means for quick assessment of multi-channel effects, such as table lookup and extrapolations based on off-line simulations. In particular, the objectives for this project are to:

- Establish a clear picture and overview of the needs and requirements for a multi-domain modelling tool with respect to AW services in the GÉANT community;
- Identify requirements and setting up specifications for the multi-domain modelling tool;
- Develop a modelling tool prototype, including a user interface;
- Perform proof of concept demonstrations in live GÉANT network.

Our approach to meet these objectives is to identify the expectations, requirements and general interests in using an AW service within the GÉANT community via targeted surveys. An important aspect of preparing for an AW service is to investigate the actual needs and requirements so this can be aligned properly with the

service and in turn with the planning and modelling tool that will be specified and developed. Once the prototype is developed and tested thoroughly in local testing environments a real network scenario of an AW deployment will be used to verify the tool's operation and demonstrate its functionality.

The earliest reported lab and field trials with the concept of Alien Wavelengths date back to 2006. Several network operators have reported their findings with experiments and measurements in different conferences and workshops during recent years. Nevertheless, the amount of interest and thus reported work seem to indicate that the idea is considered more as a peculiarity rather than a serious candidate for a next-generation service type. The main driving force among the network operators seems to be cost reduction (due to minimizing the usage of transponders on the border between domains and/or using cheaper transponders from third party vendors). Those who are not in favour of the idea point out that the AW is a disruptive technology and in order to be considered as a carrier-grade service requires a lot of changes in the current transport systems, both in terms of operational procedures, business models and sometimes even architectural design. Currently all reported field trials and the few deployments in operational networks indicate that custom-engineering is the main way to go when planning and deploying an AW service. As one of the main challenges in the deployment and exploitation of AWs it is pointed out that a modelling tool for predicting (i.e., initial evaluation of) the performance of the service and its impact on the existing services is needed. The main focus of designing such a tool should be on the impact of the physical impairments, which should be carefully considered in a (transparent) optical network. In transparent optical networks, as the signal propagates in a transparent way it experiences the impact of a variety of quality degrading phenomena that are introduced by different types of signal distortions. These impairments accumulate along the path and limit the system reach and the overall network performance. There are distortions of almost “deterministic” type related only to the pulse stream of a single channel, such as self-phase modulation (SPM), Group Velocity Dispersion (GVD) or the optical filtering. The other category includes degradations having a statistical nature such as Amplified Spontaneous Emission (ASE) noise, WDM nonlinearities (Four-Wave-Mixing (FWM) and Cross-Phase-Modulation (XPM)), Polarization Mode Dispersion (PMD) and crosstalk (XT). This project will design and develop such a tool, which will help the NREN community in the process of planning AW deployments in their networks. The tool will go beyond state of the art by being vendor independent. Depending on the application scenario, AWs can be deployed in both intra- and inter-domain application scenarios. This tool will focus explicitly on a multi-domain deployment scenario (i.e., the interface between two NRENs).

The goal of MOMoT is to provide a simple yet effective tool for initial evaluation of the feasibility of AW deployment, given a specific scenario. The tool will rely on as detailed as possible information provided by the users (the interconnecting networks) and thus, well-defined interfaces and specific format for the input information will be designed at the first phase in the project. The unified interface will make it possible for every network operator, regardless of his specific WDM transport network segment to participate in the design process with relevant input, where considerations for preserving confidentiality of the provided information will be taken.

The overall problem for modelling alien wavelength

transmission performances not only over the GÉANT network but in general, is that either the available tools are licensed (i.e., expensive) or they are proprietary, and thus tailored for specific vendor's system design. The challenge with AW is that the optical signal comes from a transponder which is foreign for the host WDM system, thus, the tool used by the WDM system's vendor might not be able to simulate the AW signal. As a result, no commercial or non-commercial tool exists that will enable NRENS to predict AW performance or possible implications on existing traffic from inserting the AW in a cost-effective manner. The goal of this project is to develop a modelling tool for the GÉANT community, beyond state of the art, which can estimate and predict AW performance and assess implications on existing traffic in the network path. The tool will be based on simple empirical formulas, possibly combined with database sources, which can quickly estimate if a path is viable or not. It will be developed with a web interface so NRENS can request an AW deployment evaluation and, based on factors such as the actual network topology, physical parameters and available spectral grids, a path and estimation on performance will be calculated. The tool will be license free and vendor independent.

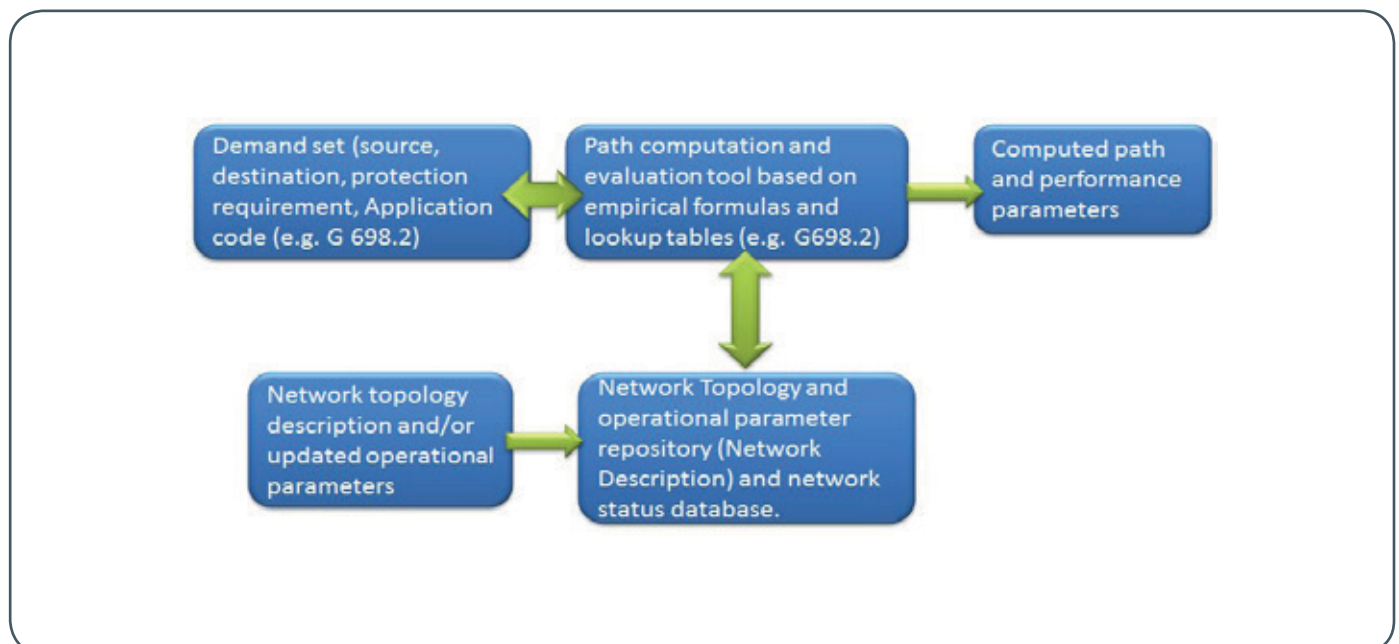
Modelling tools in general provide an efficient way to estimate the signal performance over an optical path while having global knowledge of the network topology and traffic. The extent to which the physical layer impairments degrade the quality of transmission (QoT) of the system depends on the operating and topological features of the optical network. Combining a different set of values for parameters ranging from the distance to the intrinsic characteristics of the network components and from the bit rate to the power budget, the resulting Q factor seeks to evaluate the system's QoT.

In the absence of impairment monitors, the modelling tool to be developed in this project will partially use fast analytical models in combination with single channel numerical modelling that provide relatively fast performance estimation at a certain level of accuracy. The proposed approach would be based on the Split-Step Fourier (SSF) method that is commonly used to solve the non-linear Schrödinger Equation (NLSE) which regulates the propagation of the optical signal through the non-linear medium. In a nutshell the SSF

method treats the linear and non-linear part of the equation separately by breaking the solution in very small steps. The non-linear part is solved in the time domain while the linear in the frequency domain. Therefore, at every step the method has to switch between the domains using Fast Fourier Transforms (FFT). However, the efficiency and the speed of the SSF method depend highly on the size of the step and the number of the FFTs. Clearly, the smaller the size of the step is, the greater the number of the required FFTs. It has been shown though, that most of the computational time is consumed when evaluating the FFTs. Especially when it comes to a multi-channel transmission, the numerical simulations become extremely time-consuming. This happens because in order to correctly capture the effect of Cross Phase Modulation (XPM) and Four Wave Mixing (FWM) the step size has to be very small.

This project builds upon the strong competences of the partners in the fields of optical transport technologies, systems/networks modelling and software design and implementation. The project is divided into three phases, outlining three main scientific and technical activities, and thus three main technical work packages: 1) Requirement specifications, 2) design and implementation of the modelling tool, and 3) performance evaluation and validation of the tool. The network topology and the specification of the links and nodes along with certain physical layer parameters constitute initialization data for the tool and thus will be provided by the network provider wishing to evaluate the AW performance. The exact set of parameters will be defined based on the requirement analysis and specifications. In addition to the network setup, a "demand" consisting of a source/destination pair, protection requirements and application code (according to ITU-T G698.2) will be fed to the tool for the more advanced tool function. Using the network topology, operation parameters and the demand set on one hand and the empirical formulas and lookup tables (G694.1 or G.698.2) the modelling tool will evaluate a set of performance parameters, indicative for the AW deployment. The high-level operation of this tool is shown in the following figure.

The potential benefits and the challenges of the Alien Wavelength technology are an on-going debate among vendors, network providers and standardization bodies in the field. Even though initial



standardization in the field is present, widespread deployment is still missing. MOMoT aims at bringing awareness to the potentials of the AW technology, by facilitating its deployment via a modelling tool, which will provide an initial indication of the feasibility of deploying an AW under a given networking scenario. Unlike any tools available on the market today, the MOMoT modelling tool will be able to function as a vendor-independent tool. It is web-based and can be used by GWDG and its customers to evaluate the QoT of its network especially in interconnection scenarios involving the DFN (The NREN of Germany). The generated know-how through this project, moreover, will be an asset in eScience research group for further development or contributions in similar projects.

EXTRA READING MATERIALS

1. S. Azodolmolky, M. Klinkowski, E. Marin, D. Careglio, J. Solé-Pareta, and I. Tomkos. A survey on physical layer impairments aware routing and wavelength assignment algorithms in optical networks. *Comput. Netw.*, 53(7):926-944, May 2009.
2. S. Azodolmolky, et al.: Experimental demonstration of an impairment aware network planning and operation tool for transparent/translucent optical networks. In *Journal of Lightwave Technology*, 29(4):439-448, February 15, 2011.
3. S. Azodolmolky, P. Kokkinos, M. Angelou, E. M. Varvarigos, and I. Tomkos. DICONET NPOT: An impairments aware tool for planning and managing dynamic optical networks. In *J. Netw. Syst. Manage.*, 20(1):116-133, March 2012.
4. Fagertun, Anna Manolova; Ruepp, Sarah; Pedersen, Martin N; Skjoldstrup, Bjarke: "Field Trial of 40 Gb/s Optical Transport Network using Open WDM Interfaces", in *Proc. of CLEO-PR & OECC/PS conference, Japan, July 2013*.
5. A. Manolova, S. Ruepp, L. Dittmann, E. Calle, J. Marzo: "Restoration in Multi-Domain GMPLS-based Networks", In Press, Corrected Proof, in *Journal of Computer Communications*, Elsevier, doi:10.1016/j.comcom.2010.04.034, April 2010.
6. A. Manolova, S. Ruepp, R. Romeral, S. Rodriguez: "Routing Protocol Extension for Resilient GMPLS Multi-Domain Networks", in *WSEAS Transactions on Communications*, Issue 3, Volume 9, March 2010 ISSN:1109-2742. ■

Kurz & knapp

GWDG-Stand bei der Immatrikulationsfeier am 20. Oktober 2013

Wie schon in den Jahren zuvor, war die GWDG auch in diesem Jahr mit einem Informationsstand bei der Immatrikulationsfeier der Universität Göttingen am 20.10.2013 vertreten, um sich den neuen Studierenden vorzustellen.

Zusammen mit vielen anderen Einrichtungen der Universität, des Studentenwerks und der Stadt sowie Göttinger Kulturinitiativen präsentierte die GWDG im „Forum Studium – Beratung, Betreuung, Kontakte rund ums Studium“ ihr Angebot und gab damit den Studienanfängerinnen und Studienanfängern eine gute Gelegenheit zum ersten Kennenlernen der GWDG.



Das wurde auch rege genutzt. Mitarbeiterinnen und Mitarbeiter der GWDG beantworteten zahlreiche Fragen zum Leistungsangebot der GWDG. Zu den üblichen Fragen zu Rechnern und Internetzugängen sowie Kursen, dem WLAN und Datensicherheit kamen dieses Jahr vermehrt Fragen zum Lehrangebot und der Möglichkeit von Praktika und Hilfskrafttätigkeiten bei der GWDG.

Der Festvortrag wurde von der neuen Vizepräsidentin für Studium und Lehre der Universität Göttingen, Prof. Dr. Ruth Florack, gehalten.

Heider

Kursprogramm 2014 erschienen

Das Kursprogramm der GWDG für das Jahr 2014 ist erschienen. Es bietet wieder ein umfangreiches Angebot an Kursen zur effizienten Nutzung von Hardware, Software und Netzen. Im Vergleich zum Vorjahr hat es einige Änderungen gegeben. Neu ins Kursprogramm aufgenommen wurden folgende Kurse:

- Einführung in Windows 8
- Installation und Administration von Windows 8
- Quickstarting R: Eine anwendungsorientierte Einführung in das Statistikpaket R

Näherer Informationen zum Kursangebot der GWDG sind unter <http://www.gwdg.de/kurse> zu finden. Wenn Sie Wünsche nach weiteren Kursen haben, die nicht im aktuellen Kursprogramm enthalten sind, können Sie gerne eine entsprechende E-Mail an support@gwdg.de senden.

Otto

ABSCHIED VON BENJAMIN TETZLAFF

Herr Benjamin Tetzlaff hat nach 3 1/4-jähriger Tätigkeit die GWDG verlassen. Seine Arbeit als technischer Mitarbeiter in der Arbeitsgruppe „Anwendungs- und Informationssysteme“ (AG A) hatte im Wesentlichen zwei Schwerpunkte: Zum einen arbeitete er im Bereich von Datenbank-Design und Datenbank-Webentwicklung für das Bioinformatikprojekt MetScout in enger Zusammenarbeit mit dem MPI für biophysikalische Chemie, zum anderen war er in der Systemadministration und Anwendungsbetreuung für das Bibliothekssystem Aleph der Max-Planck-Gesellschaft tätig. Zum 1. Oktober 2013 hat Herr Tetzlaff eine Stelle an der Medizinischen Hochschule Hannover angenommen. Die GWDG dankt Herrn Tetzlaff für seine engagierte und erfolgreiche Arbeit bei der GWDG und wünscht ihm in seinem neuen Aufgabenbereich weiterhin viel Erfolg.

Heise



NEUER MITARBEITER RALPH KRIMMEL

Seit dem 16. September 2013 hat die Arbeitsgruppe „Anwendungs- und Informationssysteme“ (AG A) einen neuen Mitarbeiter: Herr Ralph Krimmel. Herr Krimmel hat an der Georg-August-Universität Göttingen einen Bachelorabschluss in Biologie mit Schwerpunkt Bioinformatik erworben und beendet gegenwärtig sein Masterstudium der Angewandten Informatik. Er war bereits als studentische Hilfskraft im Bereich Bioinformatik und Angewandte Informatik an mehreren Instituten erfolgreich tätig. Bei der GWDG arbeitet Herr Krimmel in zwei Bereichen: zum einen in der Systemadministration und Anwendungsbetreuung für das Bibliothekssystem Aleph der Max-Planck-Gesellschaft, zum anderen im Bereich „GWDG Cloud Share“, dem Dateisynchronisationsdienst unter Verwendung der Software „PowerFolder“. Er ist unter der Tel.-Nr. 0551 201-1821 zu erreichen, seine E-Mail-Adresse lautet: ralph.krimmel@gwdg.de.

Heise



ZWEI NEUE STUDENTISCHE HILFSKRÄFTE NIKOLAJ KOPP UND ARMIN DETTLAFF

Herr Nikolaj Kopp und Herr Armin Dettlaff verstärken seit einigen Wochen die Arbeitsgruppe „Nutzerservice und Betriebsdienste“ (AG H) bei Ihren täglichen Aufgaben. Herr Kopp studiert Informatik an der Georg-August-Universität Göttingen und wird u. a. abends und an Wochenenden in der Information der GWDG Dienst tun, um Nutzerinnen und Nutzer während der Öffnungszeiten bei Bedarf zu unterstützen und vor allem auch die Systeme der GWDG zu überwachen. Elektro- und Informationstechnik sind die Studienfächer von Herrn Dettlaff an der Hochschule für Angewandte Wissenschaft und Kunst in Göttingen. Herr Dettlaff wird primär telefonisch und per Ticket-System bei der Beratung und Betreuung in den Bereichen Windows-Betriebssysteme und Active Directory sowie der E-Mail-Programme Outlook und Thunderbird tätig sein. Beide werden im Rahmen Ihrer zeitlichen Möglichkeiten auch bei Problemfällen mit Arbeitsplatzrechnern in den Instituten vor Ort helfen, in denen noch keine lokalen IT-Ansprechpartner zur Verfügung stehen. Wir wünschen beiden eine interessante und lehrreiche Tätigkeit bei der GWDG.

Heuer



GoeMobile/eduroam

Unser WLAN für Ihren mobilen Einsatz!



Ihre Anforderung

Sie möchten mit Ihrem mobilen Endgerät im Institut, auf dem Campus oder an einem von über 7.000 Standorten in Europa und noch vielen weiteren Standorten weltweit ins Internet? Sie benötigen einen oder mehrere WLAN-Gastzugänge für Gastwissenschaftler?

Unser Angebot

Gleich welches Betriebssystem auf Ihrem mobilen Endgerät installiert ist, mit einem gültigen GWDG-, Studierenden- oder Gast-Account bieten wir Ihnen die Möglichkeit, an jedem der über 630 Standorte auf dem Campus in Göttingen das GoeMobile zu nutzen. eduroam bietet zusätzlich die Möglichkeit, sich auch an fremden Hochschulen oder Forschungseinrichtungen mit dem GWDG- oder Studierenden-Account am dortigen WLAN anzumelden. Gast-Accounts für Veranstaltungen mit bis zu 1.000 Teilnehmern stellen wir Ihnen auf Anfrage innerhalb kürzester Zeit zur Verfügung.

Ihre Vorteile

- > Nutzen Sie Ihr eigenes mobiles Gerät.
- > Nutzen Sie Ihren GWDG- oder Studierenden-Account an allen Bildungs- und Forschungseinrichtungen, die sich am eduroam-Projekt beteiligen.
- > Sie benötigen an fremden Hochschulen und Forschungseinrichtungen, die sich am eduroam beteiligen, keinen Gastzugang.
- > Bei der Nutzung von eduroam am Standort Göttingen werden Ihre Daten bei der Funkübertragung per WPA2 verschlüsselt.
- > Gastwissenschaftler können mit ihren eigenen mobilen Endgeräten das GoeMobile nutzen.
- > Stellen Sie Ihren Tagungsgästen kostenlose Internetzugänge für die Dauer der Tagung zur Verfügung.

Interessiert?

Wenn Sie unser WLAN nutzen möchten, werfen Sie bitte einen Blick auf die Webadresse

>> www.gwdg.de/wlan



INFORMATIONEN:
support@gwdg.de
0551 201-1523

November 2013
bis Dezember 2014

Kurse

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
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 GWDC	Buck	21.11.2013 9:00 – 12:30 und 13:30 – 15:30 Uhr	14.11.2013	4
DIE IT-SICHERHEITSRICHTLINIEN DER UNIVERSITÄT GÖTTINGEN – EINFÜHRUNG FÜR ANWENDER	Dr. Beck	21.11.2013 14:15 – 15:30 Uhr	14.11.2013	0
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 GWDC FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	28.11.2013 10:00 – 12:00 Uhr	21.11.2013	2
UNIX/LINUX-ARBEITSPLATZRECHNER – INSTALLATION UND ADMINISTRATION	Gerdas, Dr. Heuer, Körmer, Dr. Sippel	02.12. – 03.12.2013 9:15 – 12:00 und 13:30 – 16:00 Uhr	25.11.2013	8
UNIX/LINUX-SERVER – GRUNDLAGEN DER ADMINISTRATION	Gerdas, Dr. Heuer, Körmer, Dr. Sippel	04.12. – 05.12.2013 9:15 – 12:00 und 13:30 – 16:00 Uhr	27.11.2013	8

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
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
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	15.01.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	08.01.2014	4
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	28.01.2014 9:15 – 16:30 Uhr	21.01.2014	4
EINFÜHRUNG IN WINDOWS 7	Buck	06.02.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	30.01.2014	4
GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP	Töpfer	11.02. – 12.02.2014 9:30 – 16:00 Uhr	04.02.2014	8
INDESIGN – GRUNDLAGEN	Töpfer	18.02. – 19.02.2014 9:30 – 16:00 Uhr	11.02.2014	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	20.02.2014 9:15 – 12:00 und 13:00 – 16:00 Uhr	13.02.2014	4
WINDOWS-CLIENT-MANAGEMENT MIT BARAMUNDI	Becker, Körmer, Quentin, Rosenfeld	27.02.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	20.02.2014	4
INSTALLATION UND ADMINISTRATION VON WINDOWS 7	Buck	06.03.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	27.02.2014	4
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	11.03. – 12.03.2014 9:30 – 16:00 Uhr	04.03.2014	8
INDESIGN – AUFBAUKURS	Töpfer	18.03. – 19.03.2014 9:30 – 16:00 Uhr	11.03.2014	8
GRUNKURS UNIX/LINUX MIT ÜBUNGEN	Hattenbach	25.03. – 27.03.2014 9:15 – 12:00 und 13:30 – 16:00 Uhr	18.03.2014	12
ADMINISTRATION VON PCS IM ACTIVE DIRECTORY DER GWDG	Buck	02.04.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	26.03.2014	4
USING THE GWDG SCIENTIFIC COMPUTE CLUSTER – AN INTRODUCTION	Dr. Boehme, Ehlers	07.04.2014 9:30 – 16:00 Uhr	31.03.2014	4
PARALLELRECHNERPROGRAMMIERUNG MIT MPI	Prof. Haan	08.04. – 09.04.2014 9:15 – 17:00 Uhr	01.04.2014	8
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	24.04.2014 9:15 – 16:30 Uhr	17.04.2014	4
UNIX FÜR FORTGESCHRITTENE	Dr. Sippel	28.04. – 30.04.2014 9:15 – 12:00 und 13:15 – 15:30 Uhr	21.04.2014	12
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	08.05.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	01.05.2014	4

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	14.05. – 15.05.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	07.05.2014	8
EINFÜHRUNG IN DAS IP-ADRESSMANAGEMENTSYSTEM DER GWDC FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	22.05.2014 10:00 – 12:00 Uhr	15.05.2014	2
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VOR-KENNTNISSEN	Cordes	18.06. – 19.06.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	11.06.2014	8
DATENSCHUTZ – VERARBEITUNG PERSONENBEZOGENER DATEN AUF DEN RECHENANLAGEN DER GWDC	Dr. Grieger	25.06.2014 9:00 – 12:00 Uhr	18.06.2014	2
EINFÜHRUNG IN WINDOWS 8	Buck	02.07.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	25.06.2014	4
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	08.07. – 09.07.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	01.07.2014	8
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	22.07.2014 9:15 – 16:30 Uhr	15.07.2014	4
INSTALLATION UND ADMINISTRATION VON WINDOWS 8	Buck	30.07.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	23.07.2014	4
GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP	Töpfer	15.09. – 16.09.2014 9:30 – 16:00 Uhr	08.09.2014	8
ADMINISTRATION VON PCS IM ACTIVE DIRECTORY DER GWDC	Buck	18.09.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	11.09.2014	4
INDESIGN – GRUNDLAGEN	Töpfer	23.09. – 24.09.2014 9:30 – 16:00 Uhr	16.09.2014	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	29.09.2014 9:15 – 12:00 und 13:00 – 16:00 Uhr	22.09.2014	4
GRUNKURS UNIX/LINUX MIT ÜBUNGEN	Hattenbach	30.09. – 02.10.2014 9:15 – 12:00 und 13:30 – 16:00 Uhr	23.09.2014	12
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	06.10. – 07.10.2014 9:30 – 16:00 Uhr	29.09.2014	8
DIE SHAREPOINT-UMGEBUNG DER GWDC	Buck	09.10.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	02.10.2014	4
INDESIGN – AUFBAUKURS	Töpfer	13.10. – 14.10.2014 9:30 – 16:00 Uhr	16.10.2014	8
WINDOWS-CLIENT-MANAGEMENT MIT BARAMUNDI	Becker, Körmer, Quentin, Rosenfeld	16.10.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	09.10.2014	4

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	20.10.2014 9:15 – 16:30 Uhr	13.10.2014	4
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	29.10. – 30.10.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	22.10.2014	8
UNIX FÜR FORTGESCHRITTENE	Dr. Sippel	10.11. – 12.11.2014 9:15 – 12:00 und 13:15 – 15:30 Uhr	03.11.2014	12
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	19.11. – 20.11.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	12.11.2014	8
EINFÜHRUNG IN DAS IP-ADRESSMANAGEMENTSYSTEM DER GWDG FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	26.11.2014 10:00 – 12:00 Uhr	19.11.2014	2
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	04.12.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	27.11.2014	4
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	10.12. – 11.12.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	03.12.2014	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 Institutskontingents 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 Institutskontingents 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.



Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen