Sichere Email mit S/MIME unter iOS[1]

Übersicht

Gegeben:

1) iOS 7,8,9-Gerät mit konfiguriertem Email-Account und aktiver Internetverbindung.
2) Ein oder mehrere persönliche eigene S/MIME-Zertifikate (PFX- / P12-Dateien).
3) Root- / CA-Zertifikate der Zertifizierungsstelle (CER- / DER-Dateien).

   Um die Aussteller-/CA-Zertifikate müssen Sie sich normalerweise nur kümmern, falls Ihr persönliches S/MIME-Zertifikat von einer (z.B. Firmen-internen) Zertifizierungsstelle ausgestellt wurde, die nicht schon standardmäßig in den Keystores der Hersteller enthalten ist. Für weit verbreitete Zertifizierungsstellen (z.B. VeriSign, TC TrustCenter, Comodo) ist dies in der Regel nicht erforderlich, da diese von den Betriebssystem-, Browser- oder Mail-Client-Herstellern auf dem Gerät schon vorinstalliert sind.

4) Desktop-PC **mit** Email-Account zum Versenden der eigenen S/MIME-Zertifikate.

Apples Betriebssystem iOS implementiert seit Version 5 den S/MIME-Standard zum Versenden von digital signierten- und / oder verschlüsselten Emails im eingebauten **Email-**Programm „Mail“.

Diese Anleitung führt Sie **Schritt-für-Schritt** durch die Konfiguration und Benutzung von S/MIME unter iOS 7. Die Anleitung ist jedoch auch für die älteren Versionen des Betriebssystems gültig.

Vorgehensweise:

In drei Schritten sichere Email einrichten:

1. Installieren des Zertifikats im Mail-Client.
2. Email-Account für S/MIME konfigurieren.
3. Erster Kommunikationsteilnehmer sendet eine signierte Mail, der zweite kann schon verschlüsselt antworten.

[1] Dies ist das 4. Dokument in der Reihe "Sichere Email mit S/MIME" (© 2016).

Inhaltsverzeichnis

SICHERE EMAIL MIT S/MIME UND „MAIL“ UNTER IOS

Sichere Email mit S/MIME unter iOS 1
Übersicht 1
Schritt 1: Installieren der Zertifikate 4
Schritt 2: Email-Account für S/MIME konfigurieren 9
Schritt 3: Senden und Empfangen verschlüsselter Emails 12
Anhang: Weitere Infos 16
A) Nutzung eines Mac 16

Begriffserklärungen:

S/MIME	Protokoll für sichere Email
Mail	Name des Standard-Mail-Clients unter iOS
Sichere Email	Mails, die signiert und verschlüsselt statt im Klartext verschickt werden.

Bemerkung: „E-Mail“ wird hier meist als „Email“ geschrieben.

Dokument-Status:

- Datum: 19.4.2016
- Version: 1.1.0
- Autoren: Michael Schober, Dennis Walter (NOVOSEC AG) und Bernhard Esslinger (Uni Siegen)
- Mit Unterstützung vom CrypTool-Projekt www.cryptool.org
- Sprache: Deutsch
- Lizenz: Keine bzw. Public-Domain bzw. GNU Free Documentation License

- Aufbereitung: Schritt-für-Schritt mit vielen Bildschirmfotos (Screenshots)
- Zielgruppe: Jedermann
  (Privat- und Heimanwender, die Ende-zu-Ende-verschlüsselt per Email kommunizieren wollen).

Dieses Dokument ist das **vierte** in der Reihe „Sichere Email mit S/MIME“. Die gesamte Reihe besteht aus den 4 Dokumenten:

1. **Sichere Email mit S/MIME und Thunderbird (unter Windows, MAC und Linux)**
   Das 1. Dokument enthält die Theorie und erläutert, wie sichere S/MIME-Email mit dem Mail-Client „Thunderbird“ funktioniert.
2. **Sichere Email mit S/MIME und Outlook unter Windows**
   Das 2. Dokument zeigt, wie es unter Windows mit dem Mail-Client „Outlook“ geht (mit und ohne Virtual Smartcard).
3. **Sichere Email mit S/MIME unter Android**
   Das 3. Dokument zeigt, wie es unter Android mit dem Mail-Client „SMail“ geht.
4. **Sichere Email mit S/MIME unter iOS**
   Das 4. Dokument zeigt, wie es unter iOS mit dem Mail-Client „Mail“ geht.

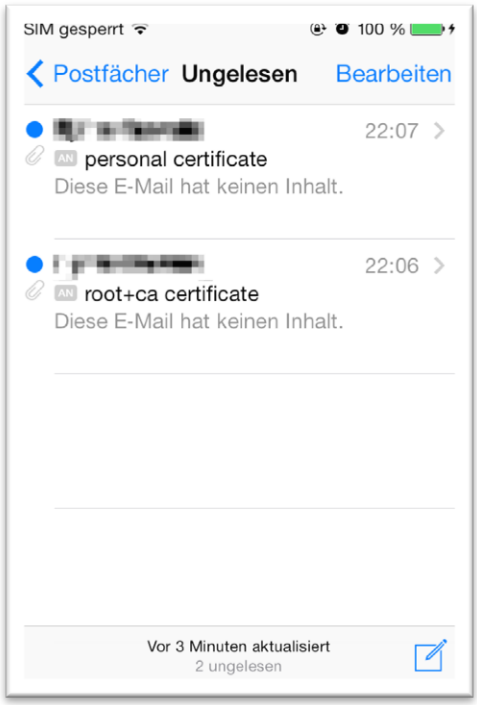
Schritt 1: Installieren der Zertifikate

Vor der Installation Ihres Zertifikats muss es auf das Apple-Gerät übertragen werden. Wir nehmen an, dass Sie – wie in Dokument 1 („Sichere Email mit S/MIME und Thunderbird“) beschrieben – auf Ihrem PC schon ein kostenloses Zertifikat beantragt und eine P12-Datei erstellt haben.

Erstellen Sie hierzu auf Ihrem Desktop-PC eine neue Email, und fügen Sie evtl. die Root- & CA-Zertifikate der Zertifizierungsstelle ein (Mit CA ist der Anbieter gemeint, der Ihr eigenes Zertifikat ausgestellt hat. In Windows kann man sich die Hierarchie mit anzeigen lassen und dort auch das CA-Zertifikat exportieren. Dieses muss man aber nur installieren, wenn es nicht bereits per Default auf dem Gerät installiert ist. Liste bereits installierter Root-Zertifikate: https://support.apple.com/en-us/HT204132).

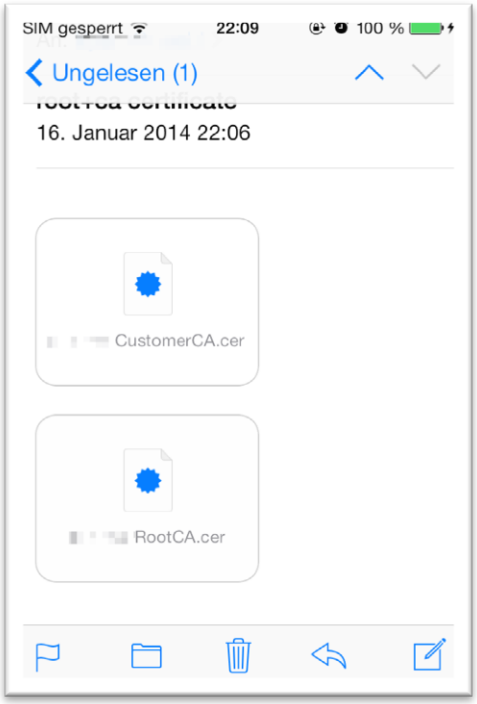
In einer zweiten Email hängen Sie bitte Ihre persönliche P12-Datei als Anhang an. Falls Sie jeweils ein eigenes S/MIME-Zertifikat zum Signieren / Verschlüsseln verwenden, fügen Sie bitte beide P12-Dateien hinzu (Das dürfte im Kontext von Endnutzern selten vorkommen, da öffentlichen CAs eigentlich nur „gemeinsame“ Zertifikate ausstellen, also Zertifikate sowohl zum Signieren als auch zum Verschlüsseln).

Senden Sie beide Emails an den auf dem Apple-Gerät konfigurierten Email-Account.

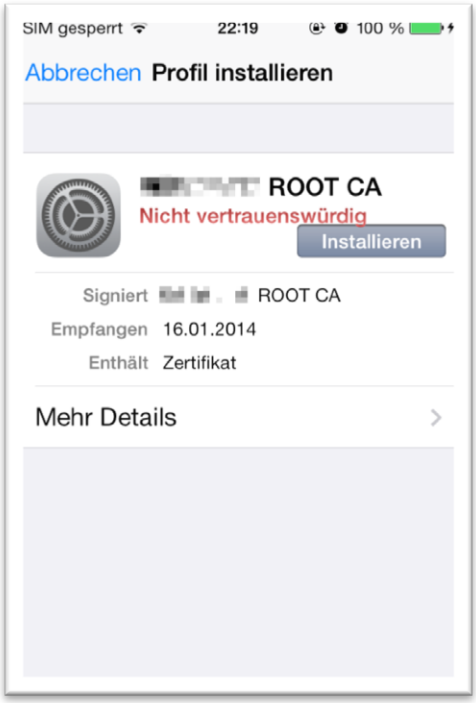


Die folgenden Schritte 1 bis 3 sind normalerweise nicht nötig (siehe S. 1 unter „Gegeben“), denn normalerweise ist das Zertifikat des Ausstellers, der Ihr persönliches S/MIME-Zertifikat unterschrieben hat, schon standardmäßig im Keystore enthalten.

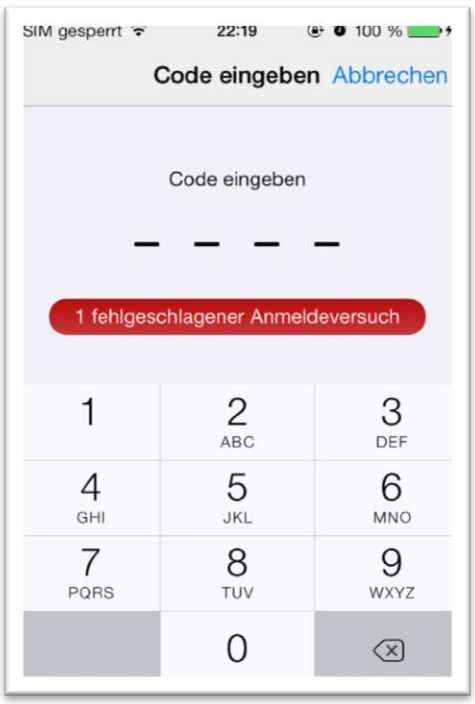
1. Öffnen Sie die Email auf dem Gerät zur Installation der Root- / CA-Zertifikate.

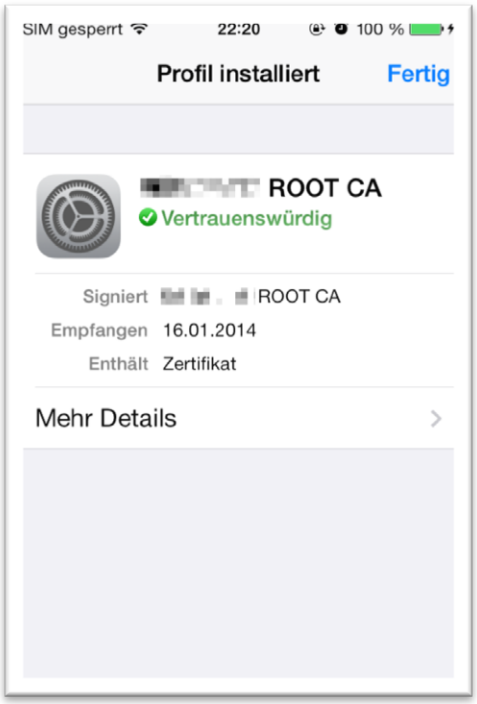


2. Klicken Sie auf das **Root-Zertifikat**. Über den Button „Installieren“ wird das Zertifikat auf dem Gerät installiert.

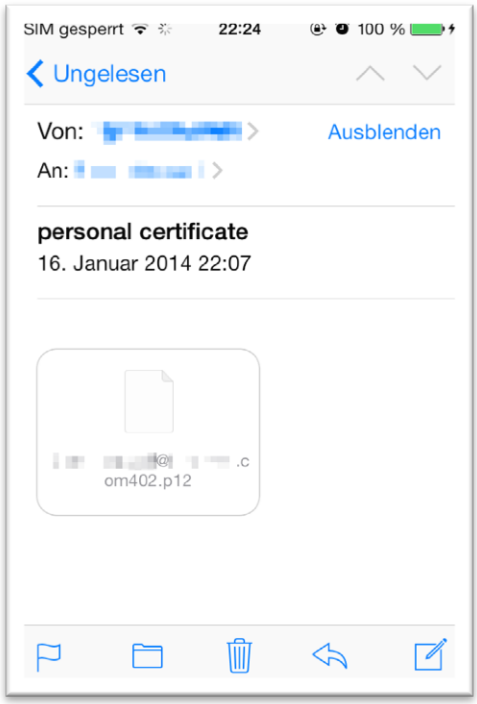


3. Falls Sie auf Ihrem Gerät einen Passcode konfiguriert haben, werden Sie während der Installation aufgefordert, diesen zur Autorisierung einzugeben. Anschließend wird das Zertifikat als vertrauenswürdig angezeigt. Führen Sie die gleichen Schritte für das **CA-Zertifikat** durch.

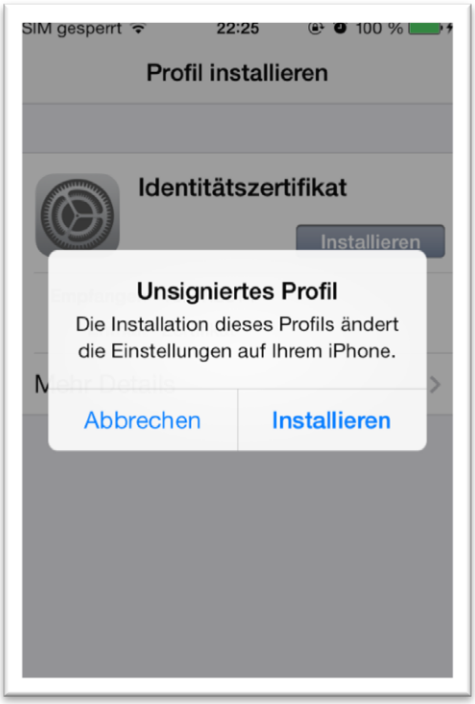




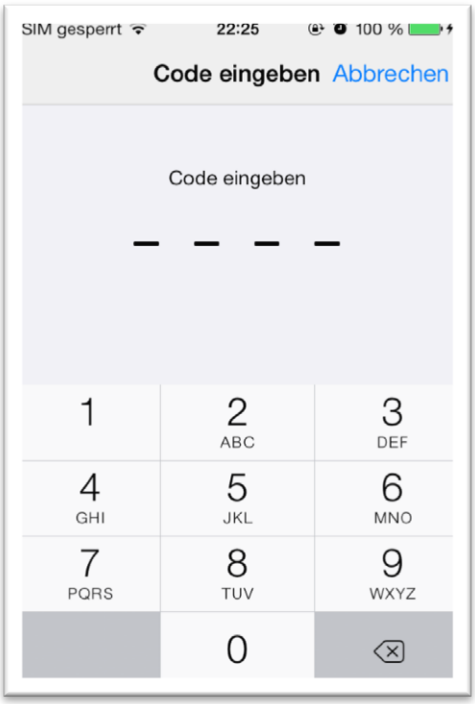
4. Öffnen Sie anschließend die Email mit Ihrem persönlichen S/MIME-Zertifikat.



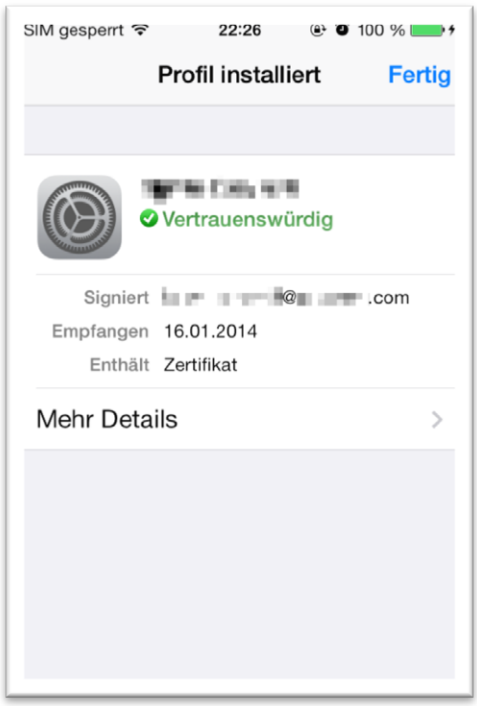
5. Klicken Sie auf dem Button „Installieren“, um den Importvorgang zu starten.



6. Geben Sie Ihren Passcode zur Bestätigung ein. Anschließend werden Sie aufgefordert, das Passwort Ihrer persönlichen Schlüsseldatei (P12-Datei) einzugeben.
Nach Drücken auf „Weiter“ sind Ihr Zertifikat und der private Schlüssel importiert.



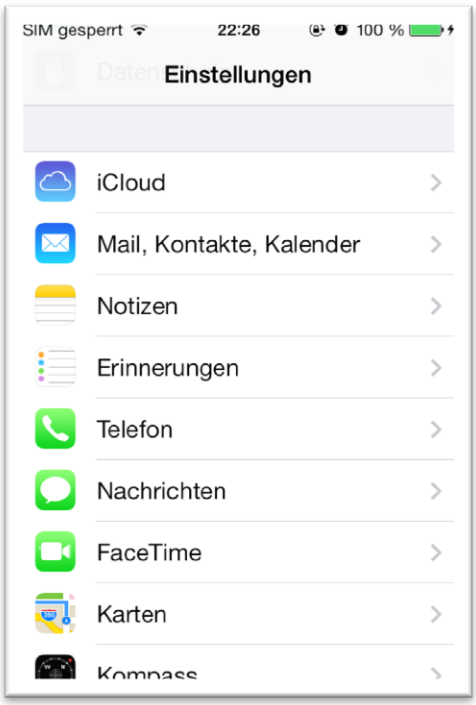
7. Ihr persönliches Zertifikat ist importiert und vertrauenswürdig. Durch Klicken von „Fertig“ beenden Sie den Import-Assistenten.

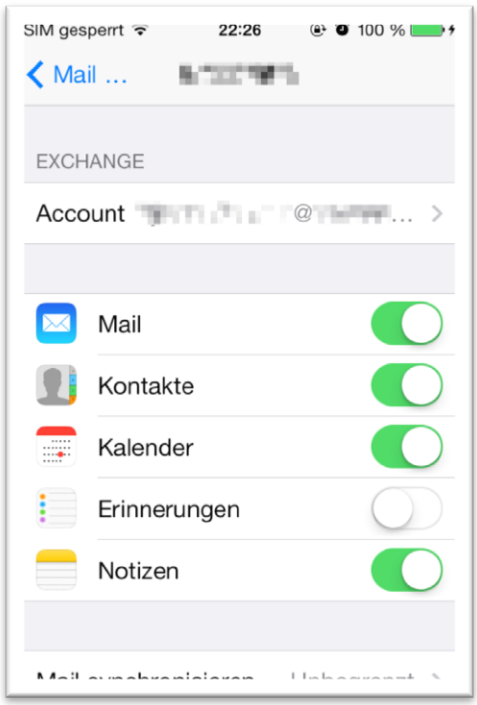


Schritt 2: Email-Account für S/MIME konfigurieren

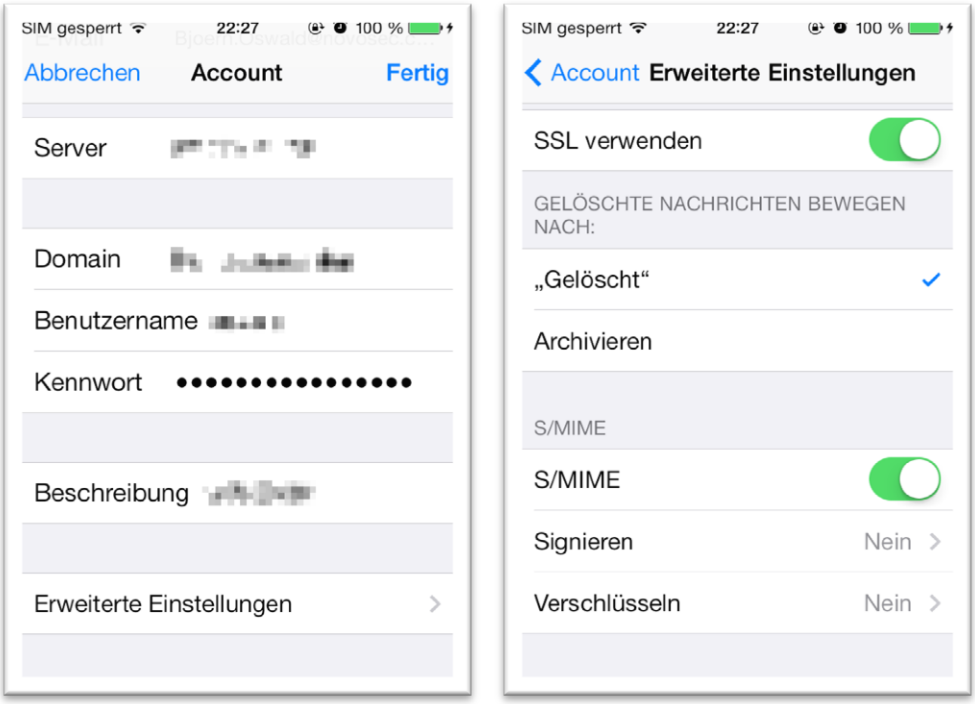
Nachdem alle Zertifikate erfolgreich importiert wurden und das Gerät diesen vertraut, muss S/MIME für den zu verwendenden Email-Account im Mailprogramm „Mail“ eingerichtet werden. S/MIME wird unter iOS global aktiviert. Das bedeutet, dass Mail anschließend jede ausgehende Email signiert. Bei Aktivierung der Verschlüsselung wird ebenfalls immer versucht zu verschlüsseln. Voraussetzung hierzu ist, dass ein S/MIME-Zertifikat für alle Empfänger gespeichert ist. Andernfalls wird von Mail ein Hinweis angezeigt, dass für den Empfänger nicht verschlüsselt werden kann.

1. Öffnen Sie die App „Einstellungen“ und wählen Sie unter „Mail, Kontakte, Kalender“ Ihren Email-Account aus.

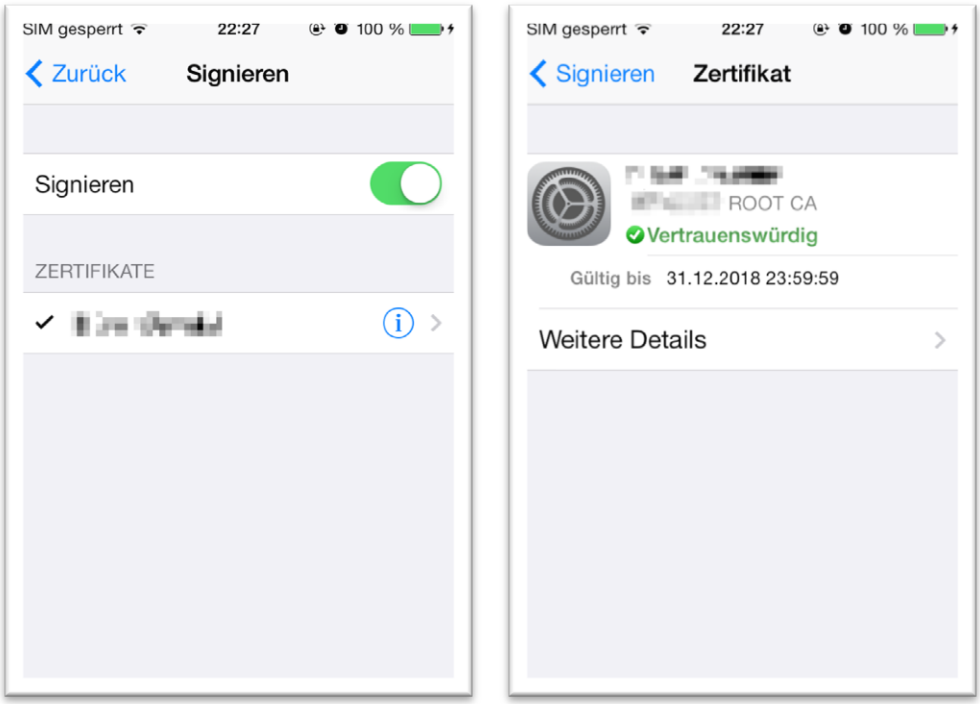


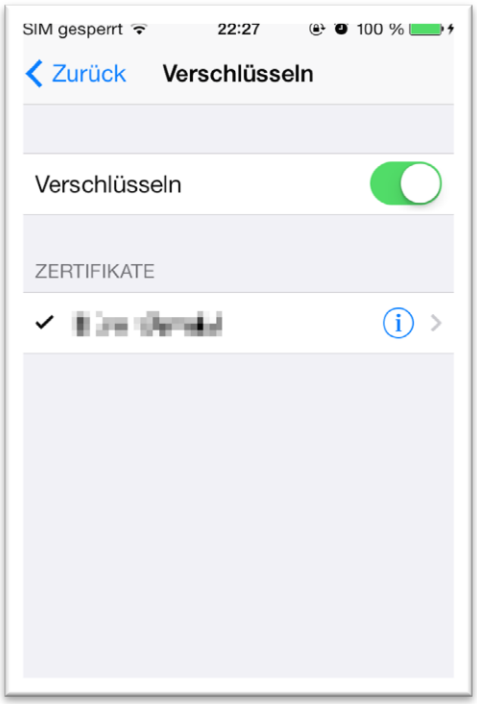


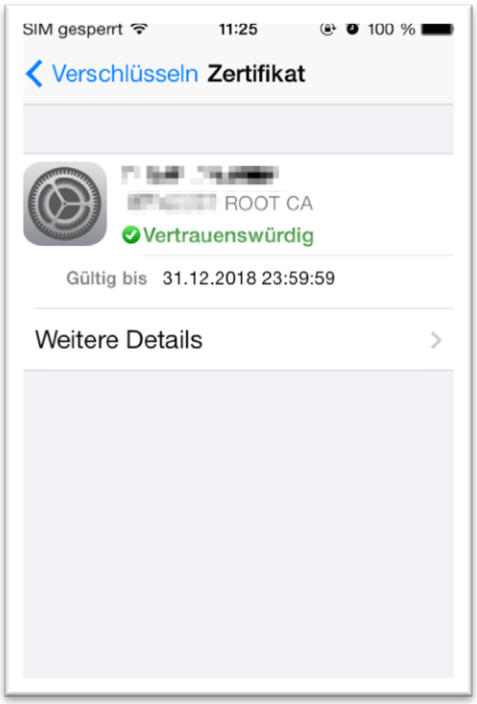
2. Öffnen Sie „Erweiterte Einstellungen“ in den Account-Einstellungen und aktivieren Sie S/MIME. Die Funktonen „Signieren“ und „Verschlüsseln“ können beide / einzeln aktiviert werden.



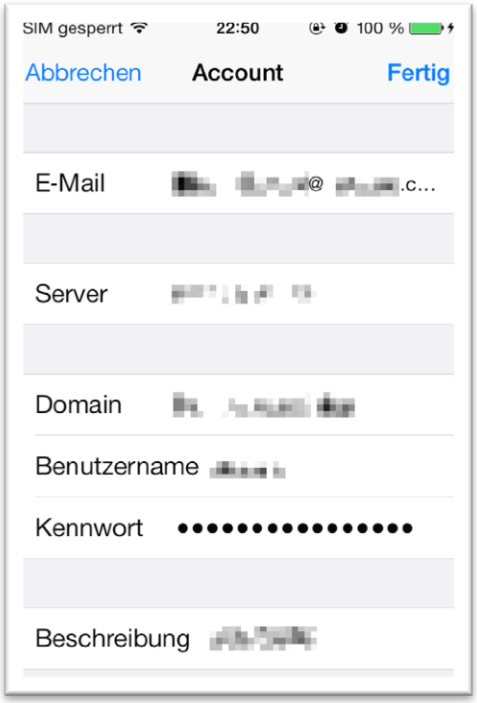
3. Verknüpfen Sie Ihr persönliches S/MIME-Zertifikat mit den Funktionen „Signieren“ und „Verschlüsseln.







4. Navigieren Sie zurück bis in die Account-Einstellungen und beenden Sie die Konfiguration durch Klicken auf „Fertig“. Andernfalls werden die Änderungen nicht übernommen und S/MIME ist in Mail nicht aktiviert.



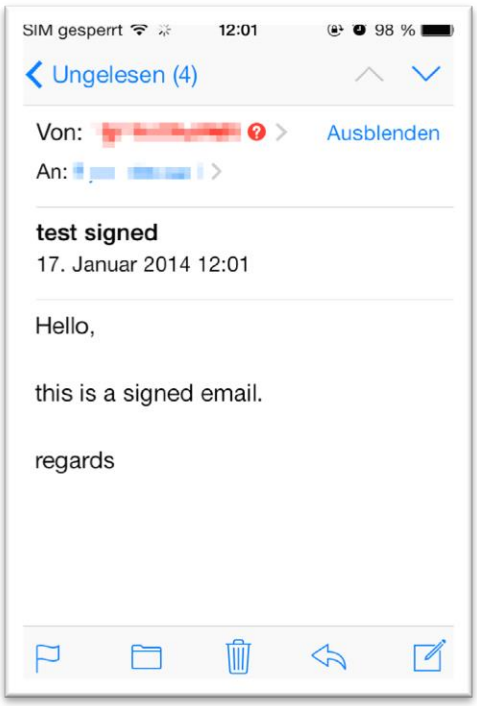
Schritt 3: Senden und Empfangen verschlüsselter Emails

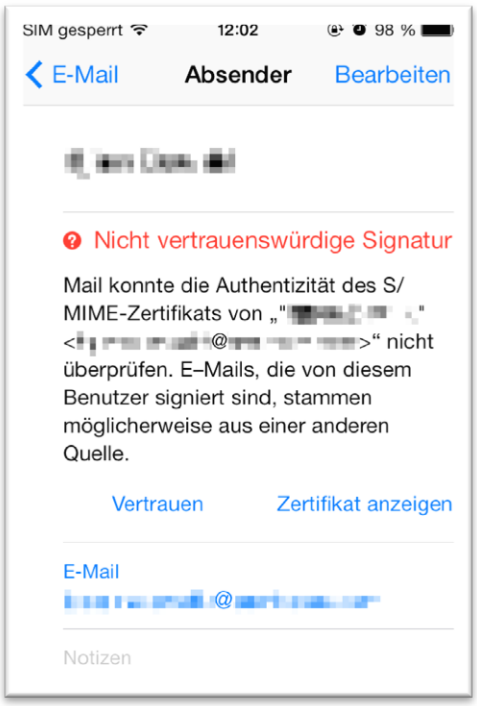
Wurden die Zertifikate importiert und ist S/MIME konfiguriert, werden bei Aktivierung von „Signieren“ alle versendeten Emails automatisch signiert. Die Verschlüsselung wird automatisch verwendet, wenn für alle Empfänger der Mail ein vertrauenswürdiges S/MIME-Zertifikat vorliegt.

Bevor eine verschlüsselte Email versendet werden kann, muss das S/MIME-Zertifikat – z.B. aus einer signierten Email des Kommunikationspartners – installiert werden.

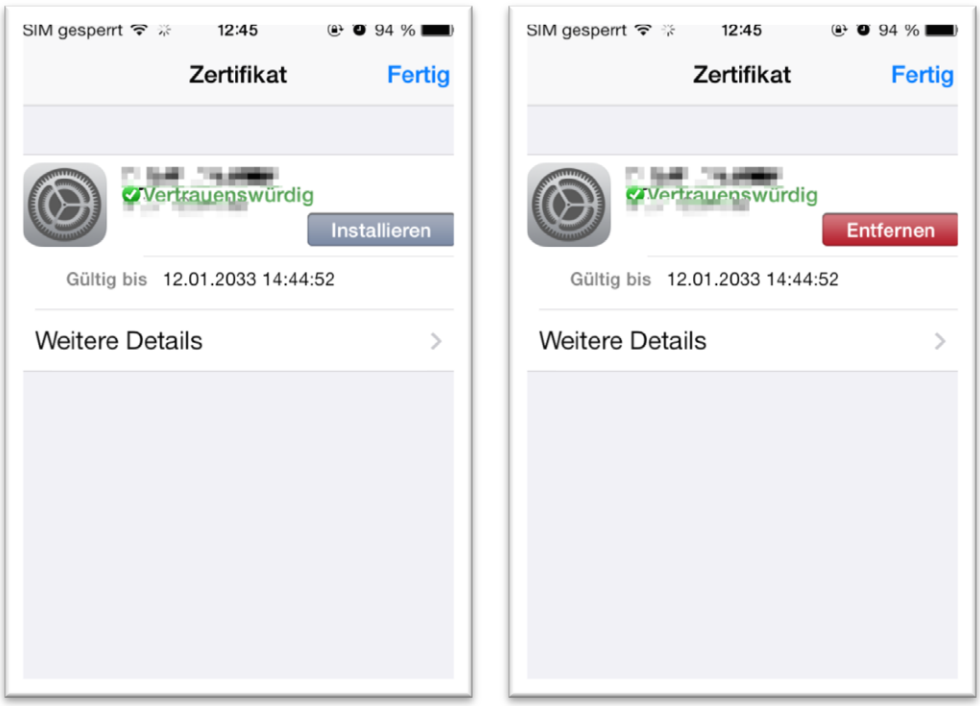
Zusätzlich hierzu wird bei Verwendung eines Microsoft Exchange-Accounts nach Empfänger-Zertifikaten in der globalen Adressliste (GAL) gesucht.

1. Zum Installieren des S/MIME-Zertifikats aus einer empfangenen signierten Email klicken Sie auf den Absender der Nachricht und im folgenden Fenster auf „Zertifikat anzeigen“.

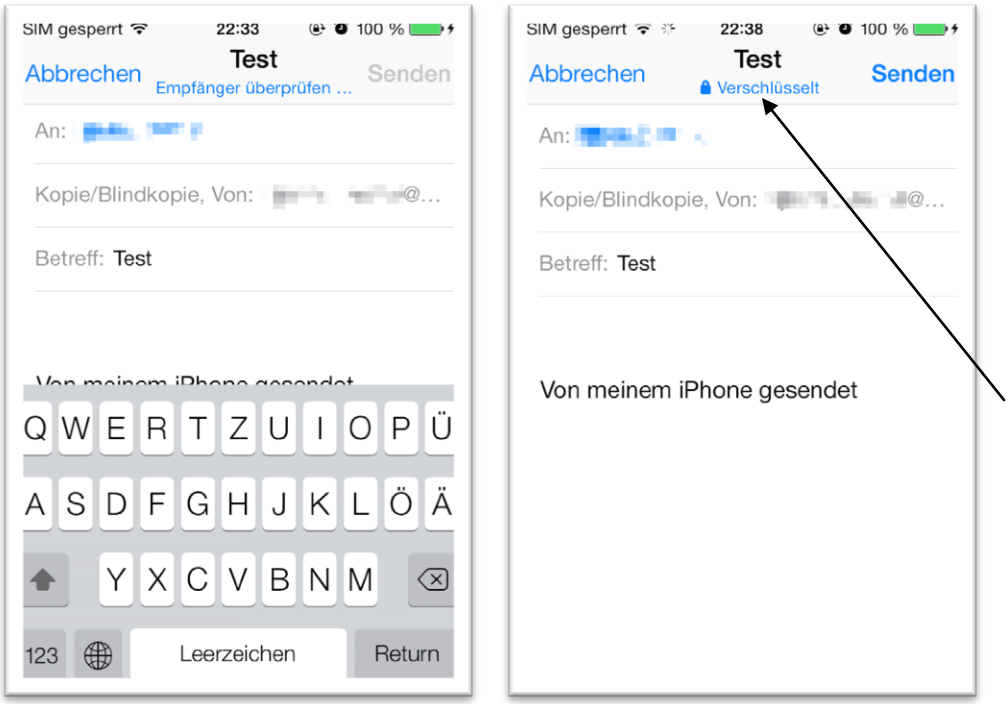




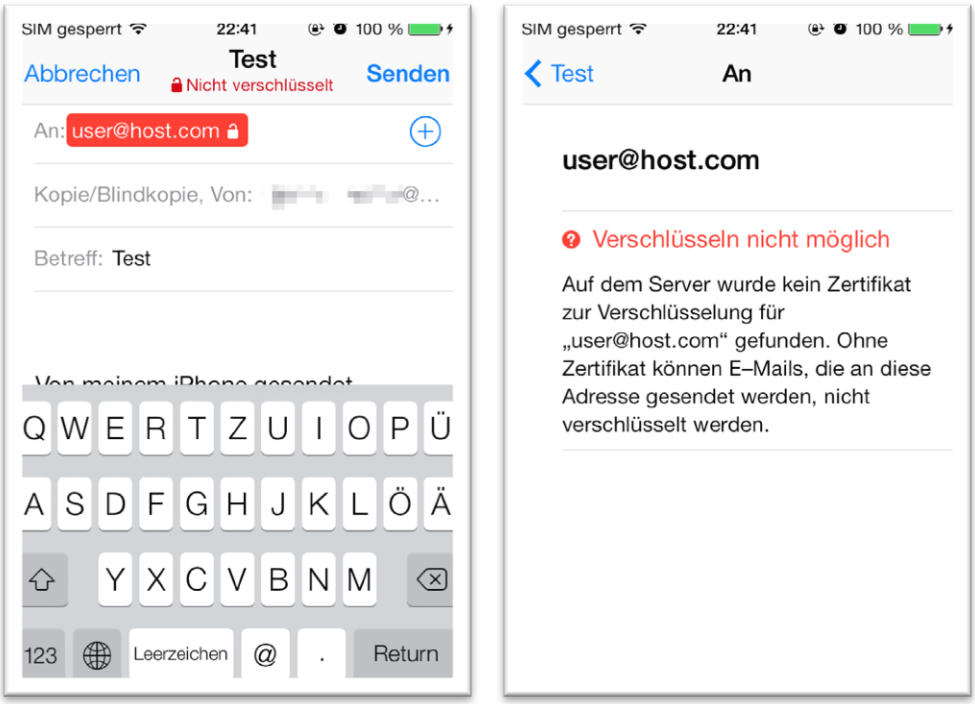
2. Klicken Sie auf „Installieren“, damit in Zukunft Emails für diesen Empfänger verschlüsselt gesendet werden können.



3. Beim Versenden von Emails wird automatisch geprüft, ob für den Empfänger ein Zertifikat vorliegt und damit verschlüsselt werden kann. Dies wird über ein Schloss-Symbol und den Text „verschlüsselt“ angezeigt. Die Email wird automatisch signiert – dies wird nicht extra angezeigt.



4. Ein rot eingefärbter Empfänger zeigt an, dass nicht verschlüsselt, sondern nur signiert wird.



5. Empfangene S/MIME-verschlüsselte Emails werden automatisch durch Mail entschlüsselt. Dass die Email verschlüsselt ist, wird über ein Schloss neben dem Absender angezeigt. Das Häkchen vor dem Schloss gibt an, dass die Email durch den Absender digital signiert wurde und die Signatur gültig ist.

Anhang: Weitere Infos

Übersicht Anhang:

A) Was sollte man als Laie wissen? Seite 16

A) Nutzung eines Mac

Auf dem Mac nutzt man meist 'Apple Mail' als Email-Client.

Dafür hilft keine der 4 Anleitungen. Deshalb hier ein Link, der anderen Apple-Nutzern half:

http://www.apfeltalk.de/community/threads/anleitung-e-mail-verschluesseln-auf-mac-und-ios.460823

Diese Anleitungsseite enthält 11 Seiten Nutzerkommentare!