Sichere Email mit S/MIME unter Android[1]

1. Übersicht

Gegeben:

1) Smartphone mit Android-Betriebssystem, und ein Mail-Account.

2) Eine P12-Datei, in der das eigene S/MIME-Zertifikat und der eigene private Schlüssel vorliegen (Wie dies erzeugt wurde, wurde im ersten Dokument „Sichere Email mit S/MIME und Thunderbird“ beschrieben).

Unter Android liegen mehrere Mail-Clients vor. Wir haben zwei gewählt:

1) SMail ist kostenlos (aber Werbe-finanziert) und bietet die volle S/MIME-Funktionalität.
2) R2Mail2 bietet nicht nur die volle S/MIME-Funktionalität, sondern zusätzlich auch die volle PGP-Funktionalität. Weiterhin ist eine Anbindung an einen Exchange Server möglich. R2Mail2 ist kostenlos, zeigt aber in der kostenlosen Variante nur die letzten 10 Emails an. Die Kaufversion kostet einmalig 4,80€.

Alternativen hatten in der freien Version teilweise Beschränkungen: K9 kann nur PGP, kein S/MIME. Djigizo ist ein noch schlecht zu bedienender Aufsatz auf den Android Standard-Mail-Client Gmail. Touchdown gibt es in einer 30-Tage Testversion, kostet danach stolze 14,67€. (Stand März 2014)

[1] Dies ist das 3. Dokument in der Reihe "Sichere Email mit S/MIME" (© 2016).

Vorgehensweise:

In drei Schritten sichere Email einrichten:

1. Den entsprechenden Mail-Client für Android (SMail oder R2Mail2) aus dem Google Play Store installieren und dabei gleich einen Mail-Account anlegen
   (→ geht nahezu vollautomatisch).

2. Installieren des Zertifikats im Mail-Client.

3. Erster Kommunikationsteilnehmer sendet eine signierte Mail, der zweite kann schon verschlüsselt antworten.

Inhaltsverzeichnis

SICHERE EMAIL MIT S/MIME UND SMAIL ODER R2MAIL2 UNTER ANDROID

Begriffserklärungen:

S/MIME	Protokoll für sichere Email
SMail und R2Mail2	Zwei Mail-Clients unter Android
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: 1.1.2
- Autoren: Michael Schober, Dennis Walter (NOVOSEC AG), André Heller (Trivadis GmbH) 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 Emailkommunizieren wollen).

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

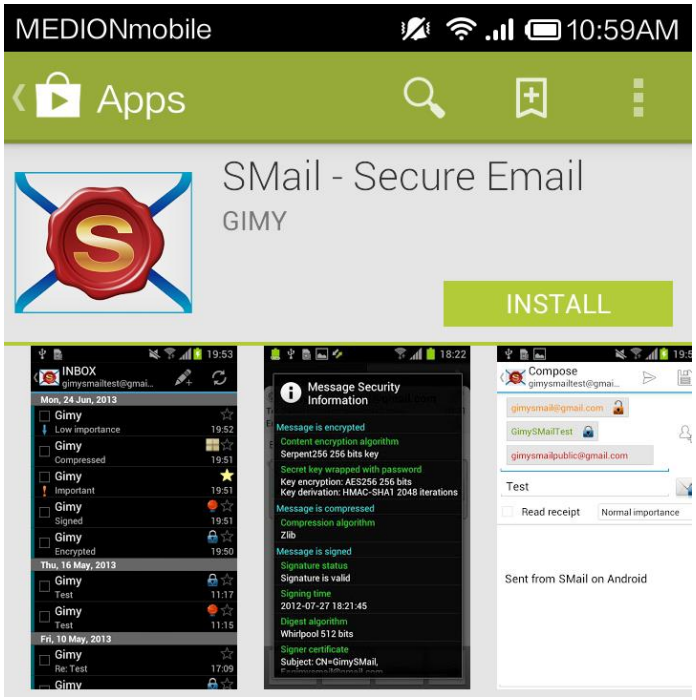
1. **Sichere Email mit S/MIME und Thunderbird (unter Windows, MAC und Linux)**
   Das 1. Dokument enthält die Theorie und erläutert, wie sichere S/MIME-Email mit dem Mail-Client „Thunderbird“ funktioniert.
2. **Sichere Email mit S/MIME und Outlook unter Windows**
   Das 2. Dokument zeigt, wie es unter 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 den Mail-Clients „SMail“ und „R2Mail2“ geht.
4. **Sichere Email mit S/MIME unter iOS**
   Das 4. Dokument zeigt, wie es unter iOS mit dem Mail-Client „Mail“ geht.

2. SMail für Android

Schritt 1: SMail installieren und Email-Account einrichten

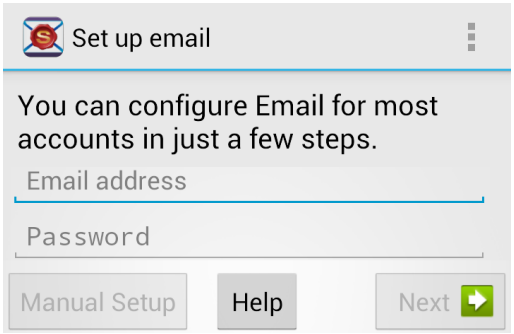
→ Dies geht nahezu vollautomatisch.

1. Installieren Sie SMail aus dem Google Play Store.

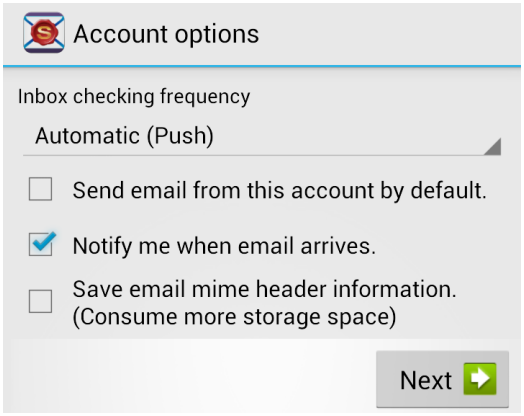


2. Starten Sie die App mit diesem Icon.

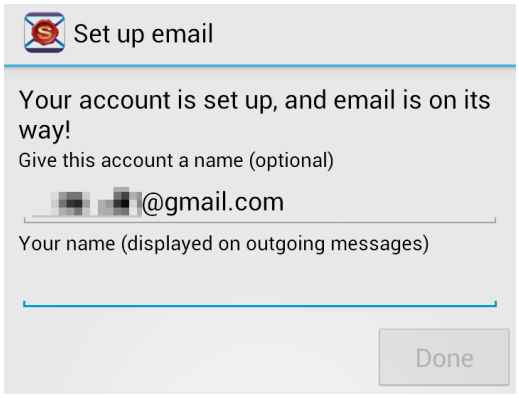
3. Geben Sie Ihre vorhandene Email-Adresse und das zugehörige Passwort ein und drücken Sie „Next“. Sollte ihr Account nicht automatisch hinzugefügt werden können, müssen Sie das „Manual Setup“ durchführen.



4. Stellen Sie die Account-Optionen ein und drücken Sie „Next“.



5. Geben Sie Ihren Namen ein und drücken Sie auf „Done“.

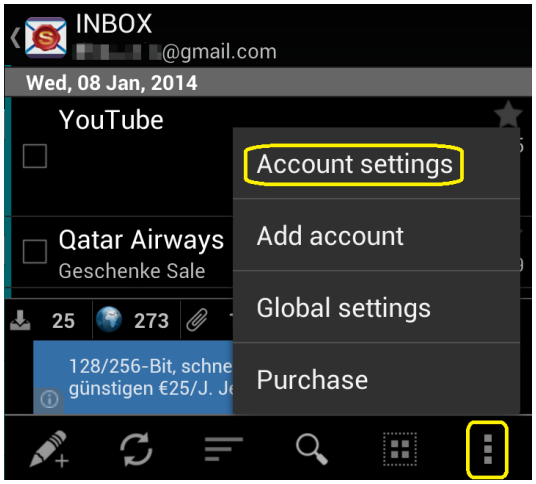


6. Ihr Email-Account ist nun eingerichtet.

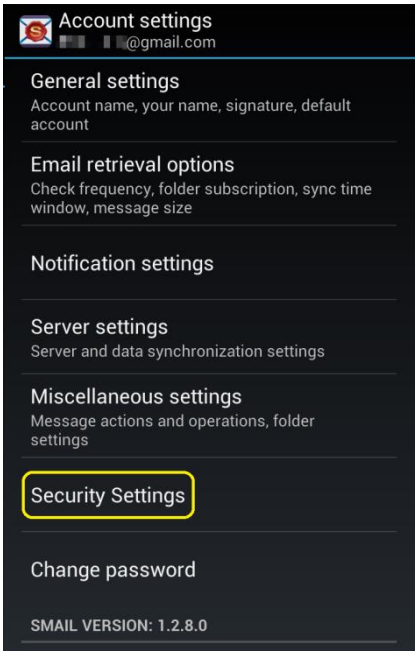
Schritt 2: Installieren der Zertifikate in SMail

SMail enthält einen eigenen Zertifikatsmanager, der die CA-Zertifikate abspeichert. Außerdem hat SMail einen Keystore (lokaler Software-Container), der den privaten Schlüssel und die User-Zertifikate enthält.

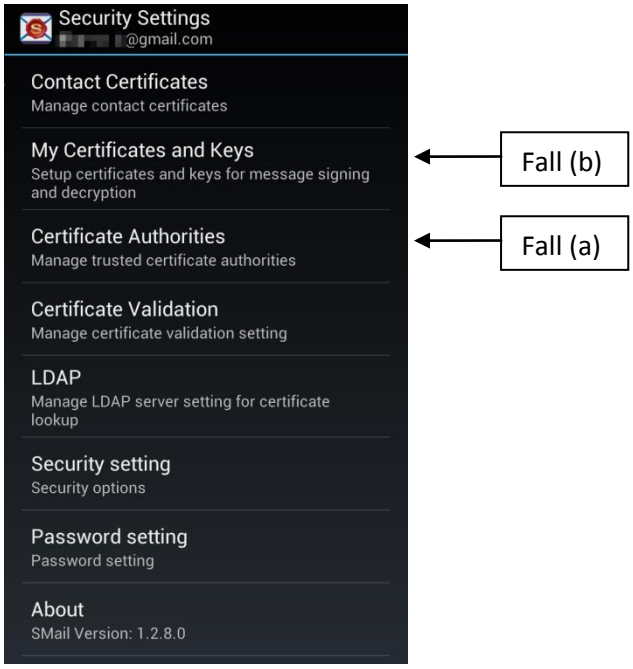
1. Importieren Sie alle benötigten Certificate-Authority-Zertifikate und Ihr eigenes Zertifikat. Drücken Sie dazu unten rechts auf die drei Punkte. Dann drücken Sie auf „Account settings“.



2. Drücken Sie auf „Security Settings“.

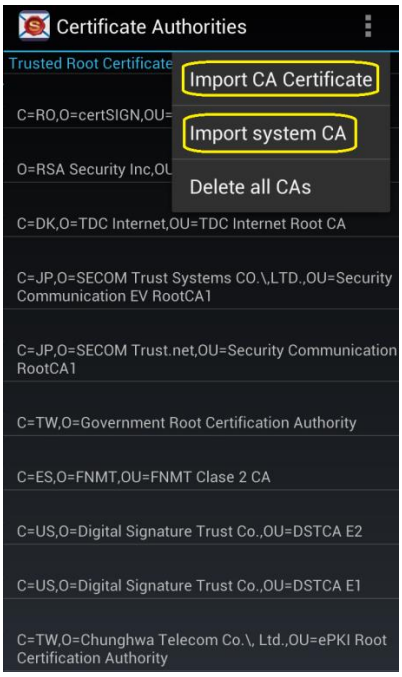


3. In diesem Menü müssen 2 Arten von Zertifikaten hinzugefügt werden. Die Reihenfolge hierbei ist egal.

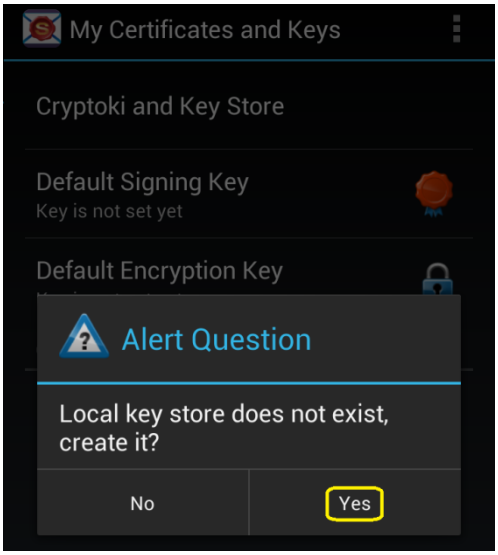


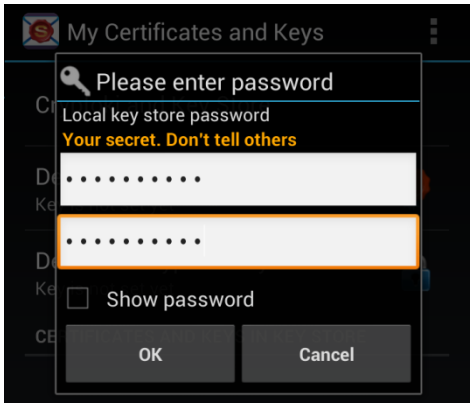
   a. Import des/der CA- Zertifikate: Drücken Sie auf „Certificate Authorities“. Anschließend drücken Sie oben rechts auf die drei Punkte und wählen „Import system CA“. Dieser Menüpunkt fügt alle auf Ihrem System vorhandenen CAs in den SMail-Zertifikatsmanager ein.

Sollen Sie nur ein bestimmtes CA-Zertifikat benötigen oder ist Ihre CA keine „system CA“, drücken Sie auf „Import CA Certificate und wählen Ihr CA-Zertifikat aus. Überprüfen Sie anschließend, ob Ihre CA in der Liste vorhanden ist.

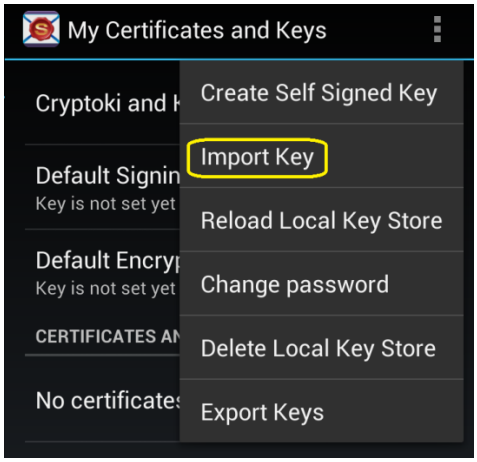


b. Import des User-Zertifikats: Drücken Sie auf „My Certificates and Keys“. Falls kein lokaler Keystore vorhanden ist, werden Sie gefragt, ob Sie einen anlegen möchten. Wählen Sie „Yes“ und vergeben Sie ein Passwort.

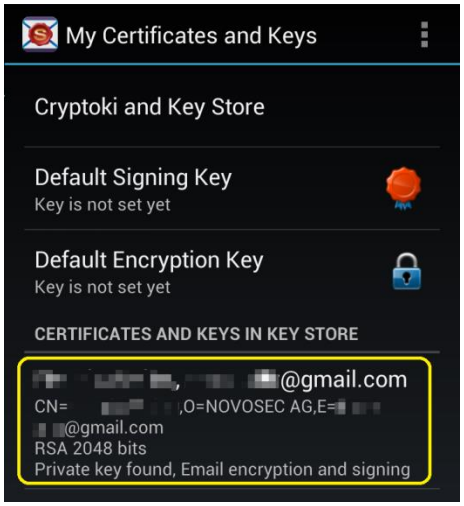


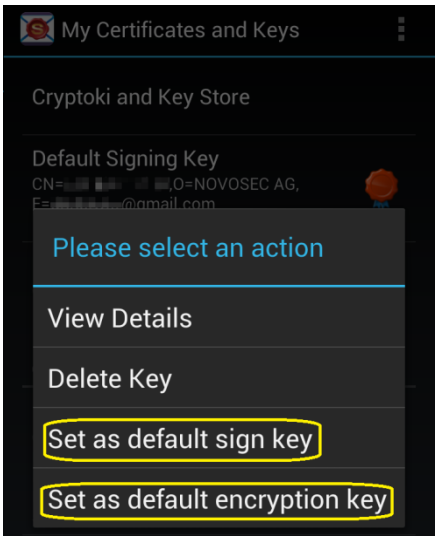


Drücken Sie oben rechts auf die drei Punkte und anschließend auf „Import Key“. Wählen Sie Ihre Schlüsseldatei und geben Sie das bei der Schlüsselerstellung oder bei der P12-Erstellung verwendete Passwort ein. Der Import erfolgt vom lokalen Dateisystem des Mobiles. Ihre eigene P12-Datei übertragen Sie am besten per USB vom Desktop-PC auf das Gerät.

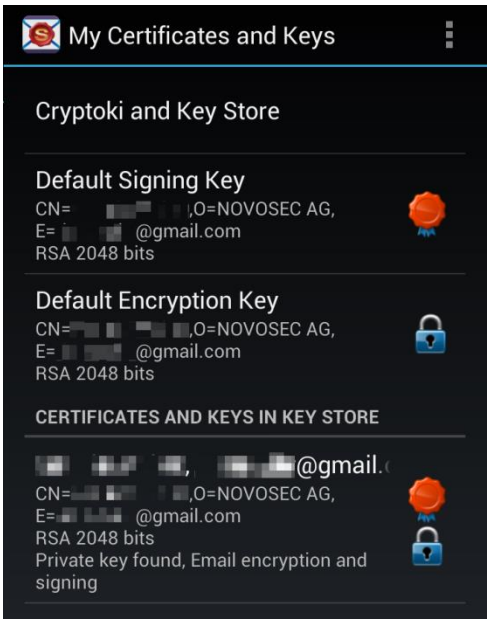


Sie können nun sehen, ob Ihr Zertifikat korrekt importiert wurde. Drücken Sie auf das Zertifikat und wählen Sie „Set as default sign key“ und „Set as default encryption key“.





Ihr Zertifikat wird nun als Standard-Zertifikat für die Signatur und die Verschlüsselung verwendet.



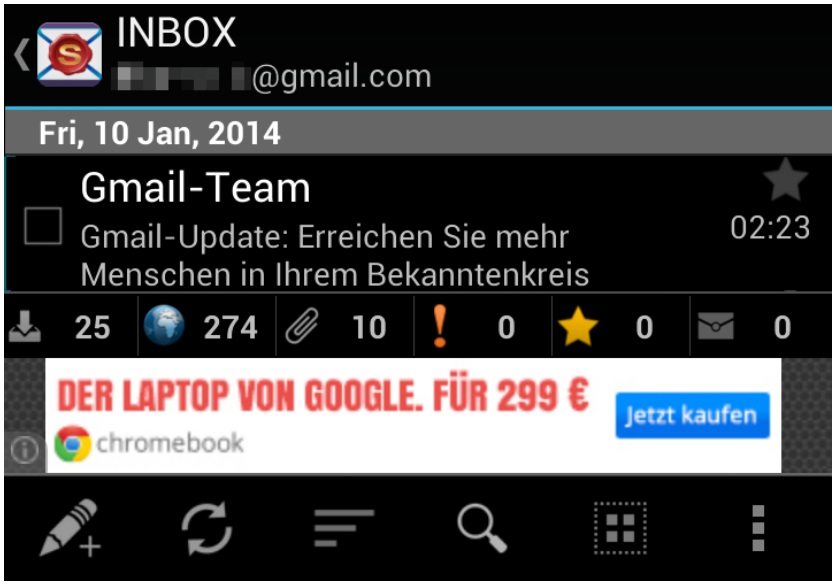
4. Sie können jetzt signierte Emails versenden.

Schritt 3: Senden und Empfangen verschlüsselter E-Mails

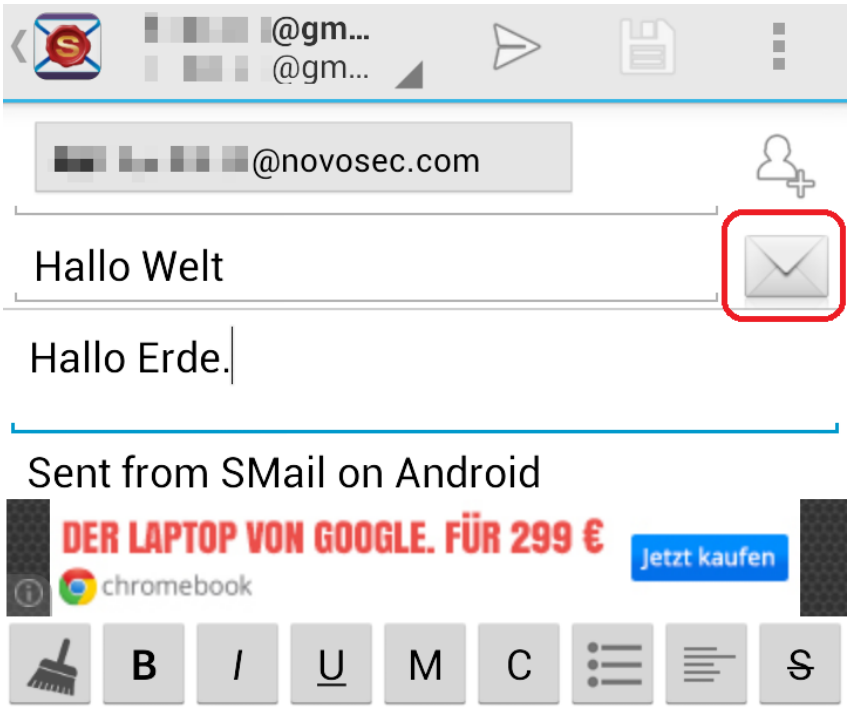
Der erste Kommunikationsteilnehmer sendet eine signierte Mail, der zweite kann sofort verschlüsselt antworten.

a) Schreiben einer signierten Email

Gehen Sie in die Inbox und drücken Sie unten links auf den Stift mit dem Pluszeichen.

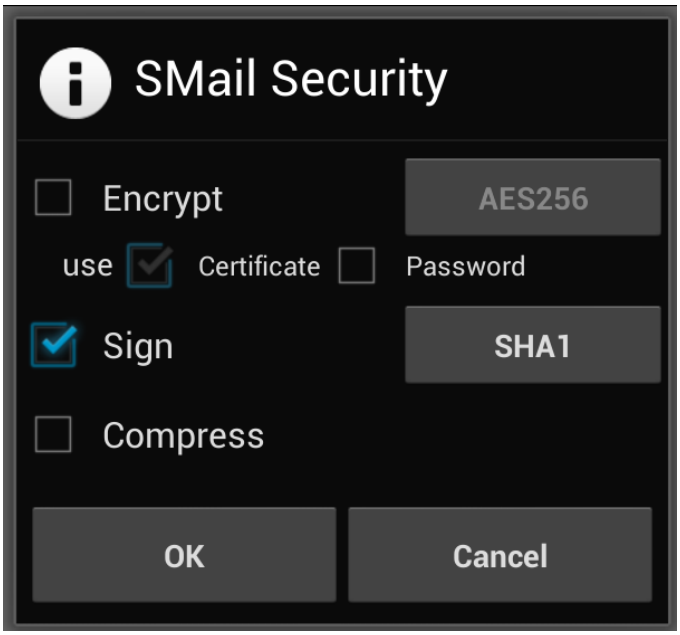


Schreiben Sie eine Nachricht und drücken Sie auf den weißen Briefumschlag.

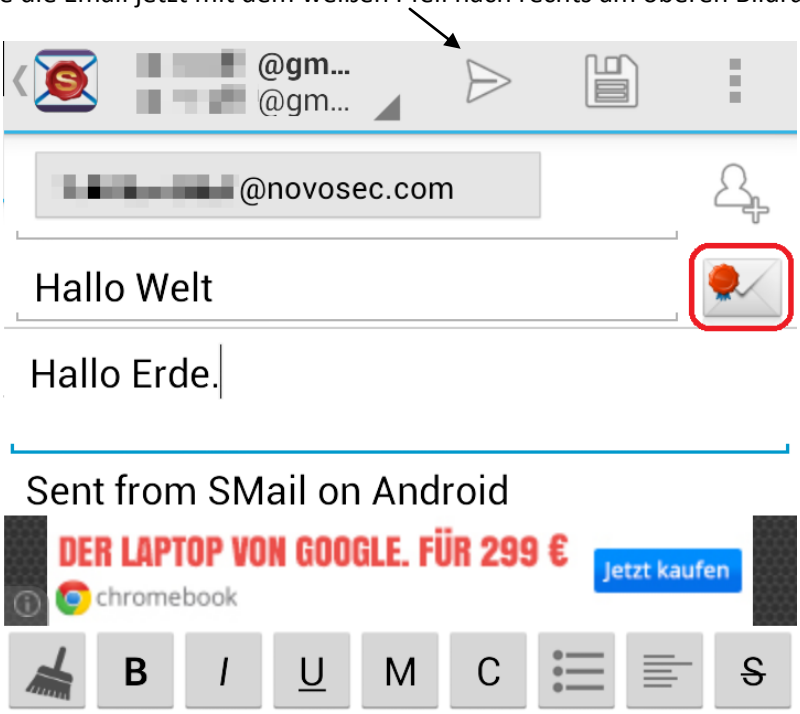


Sie können auswählen, ob Sie die Email nur signieren oder auch verschlüsseln möchten. Da Sie bisher keine weiteren Zertifikate von Dritten besitzen, setzen Sie einen Haken bei „Sign“ und drücken auf „OK“.

Rechts könnten Sie den voreingestellten Algorithmus ändern, mit dem die Signatur erzeugt wird.



Nun sehen Sie ein Siegel an dem weißen Briefumschlag. Dieses Siegel zeigt an, dass die Email signiert wird. Versenden Sie die Email jetzt mit dem weißen Pfeil nach rechts am oberen Bildrand.

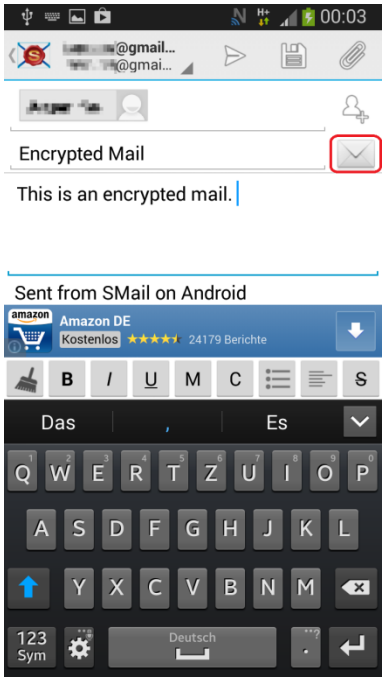


Nach Erhalt Ihrer signierten Email, ist Ihr Kommunikationspartner im Besitz Ihres öffentlichen Schlüssels und kann Ihnen somit verschlüsselte Emails zusenden. Sobald Sie eine signierte Email Ihres Kommunikationspartners erhalten haben, können Sie auch verschlüsselt antworten.

Anmerkung 1: Das Zertifikat aus einer empfangenen signierten Email wird automatisch unter Ihren Kontakten abgespeichert.

b) Schreiben einer verschlüsselten Email

Schreiben Sie dazu eine Nachricht und berühren Sie – wie beim Signieren – den weißen Briefumschlag:

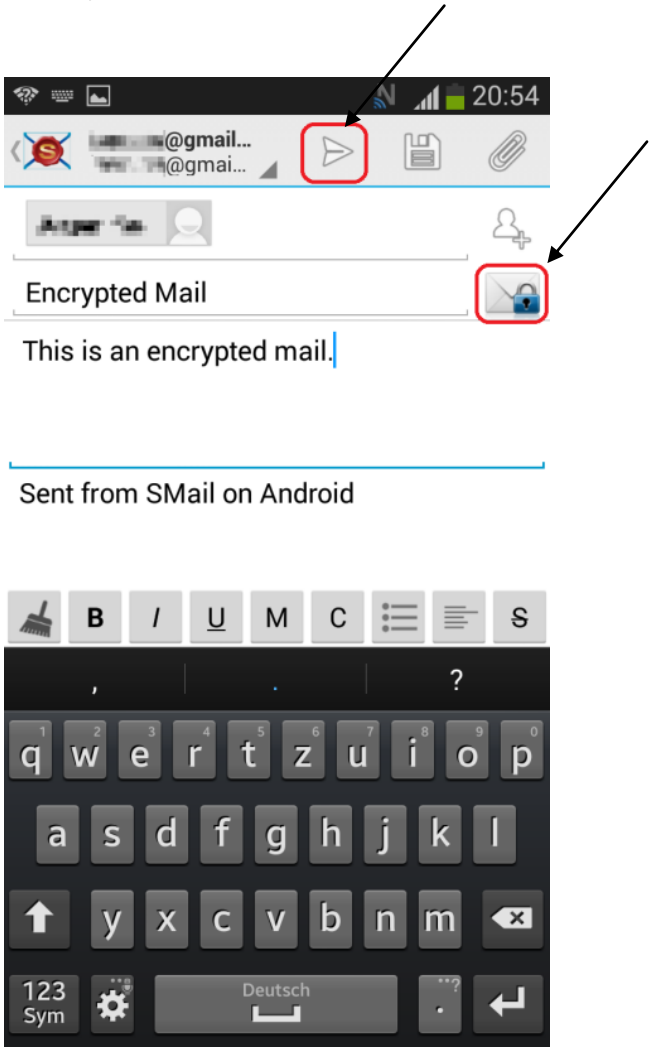


Bitte wählen Sie nun „Encrypt“ und „use Certificate“, indem Sie die entsprechenden Häkchen setzen.

Wie auch bei der Signatur, können Sie rechts durch Antippen auswählen, mit welchem Algorithmus verschlüsselt werden soll (im Beispiel ist dies AES256).

Nun können Sie ein Vorhängeschloss am weißen Briefumschlag erkennen. Dies zeigt an, dass die Email verschlüsselt gesendet wird.

Versenden der verschlüsselten Email, indem Sie auf den weißen Pfeil nach rechts in der oberen Leiste klicken.



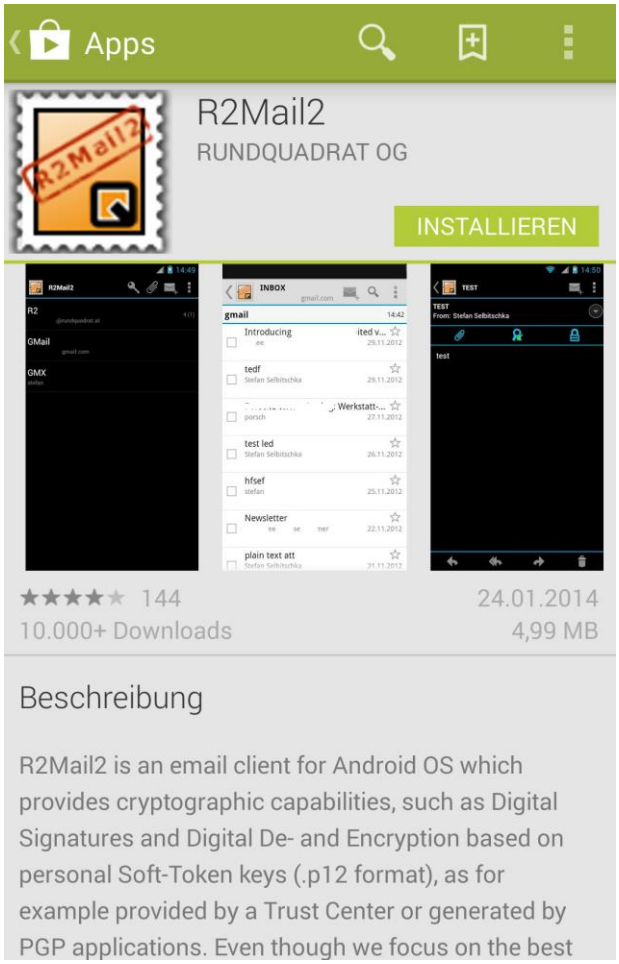
Anmerkung 2: Verschlüsselte Emails werden automatisch signiert.

3. R2Mail2 für Android

Schritt 1: R2Mail2 installieren und Email-Account einrichten

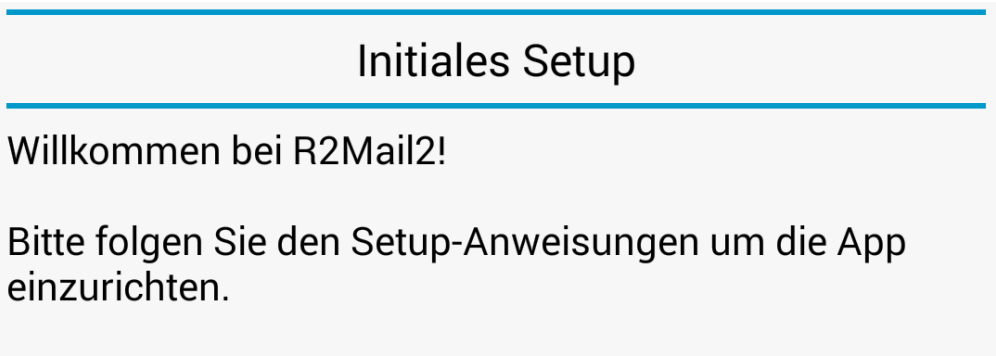
→ Dies geht nahezu vollautomatisch.

Installiere R2Mail2 aus dem Google Play Store.

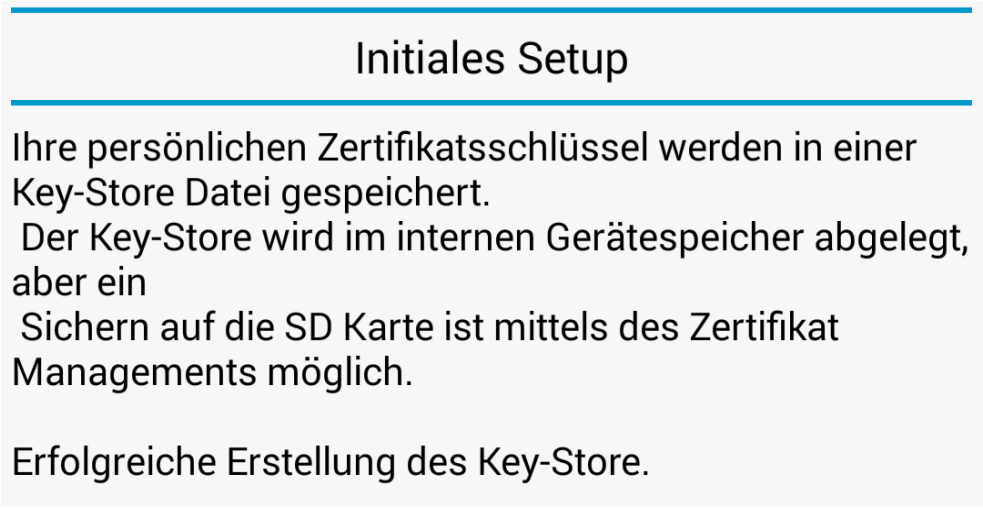


Starten der App mit diesem Icon:

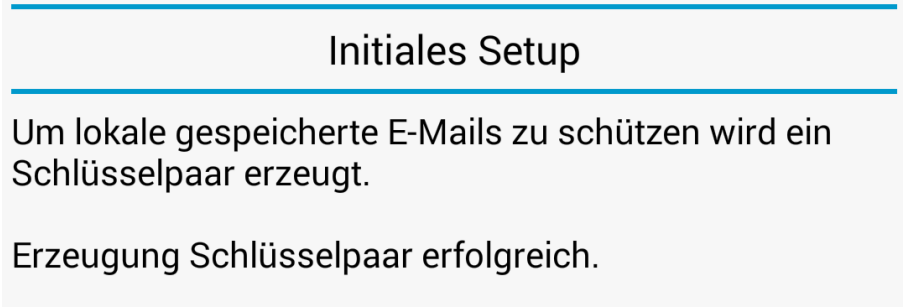
Folge den Anweisungen des initialen Setups in der App. Die Einrichtung ist vollautomatisch. Dazu bitte immer auf „Weiter“ gehen.

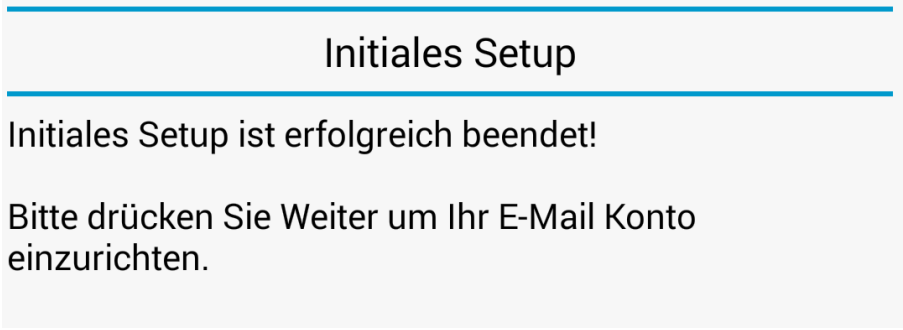


Hier werden die Zertifikate aus dem Android Key-Store automatisch in R2Mail2 importiert. Das ist notwendig, um später die Zertifikatsketten für alle S/MIME-Zertifikate nachvollziehen zu können.

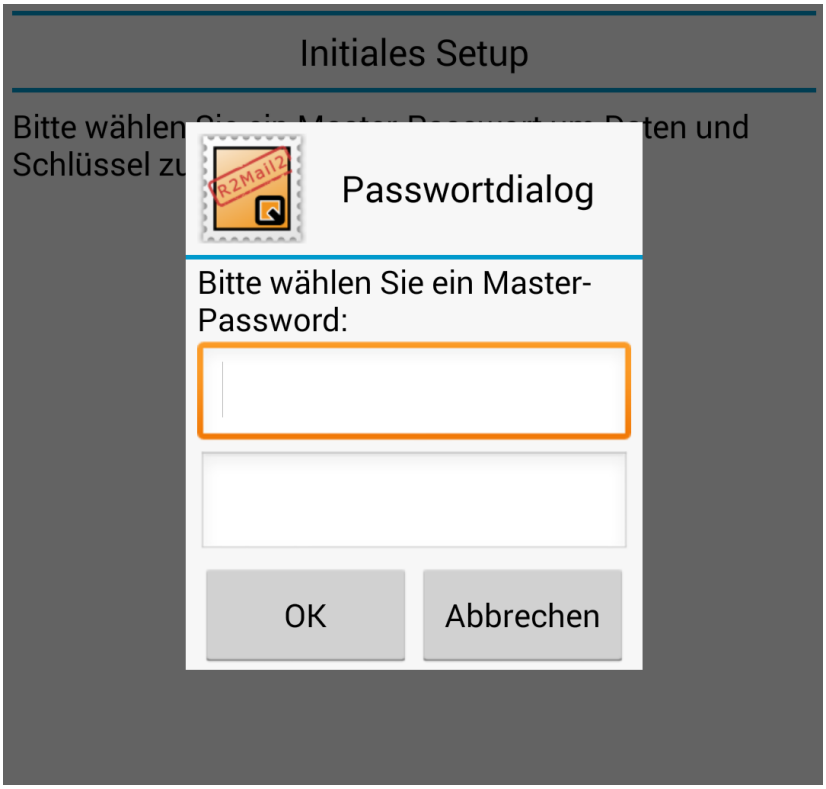


Nun wird der persönliche (eigens von R2Mail2 angelegte) Keystore erzeugt, in dem R2Mail2 später alle von R2Mail2 benutzten Zertifikate und Schlüssel verschlüsselt abspeichert werden.



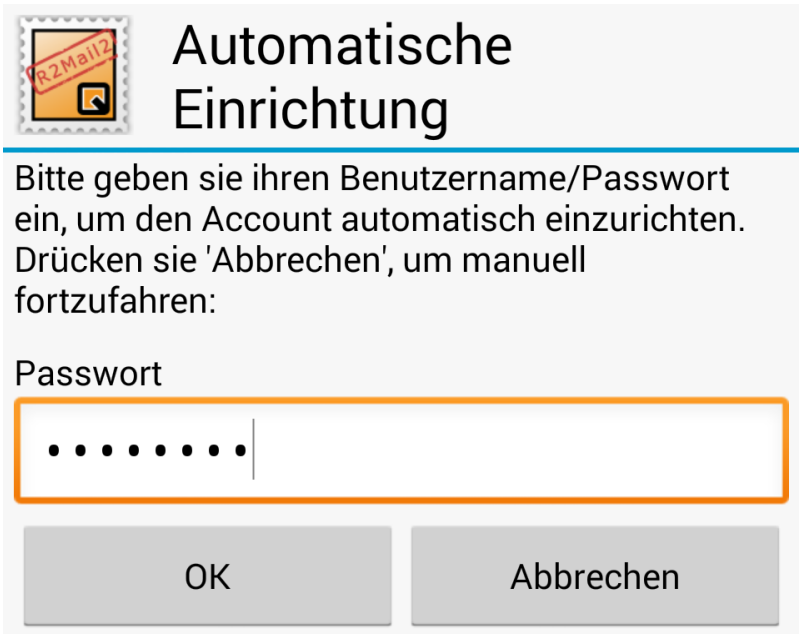


Hier muss nun ein Master-Passwort festlegelegt werden, mit dem die Zertifikate und auch die Nachrichten und Anhänge verschlüsselt werden (es zwei unterschiedliche Stores: einen für Nachrichten und Anhänge und einen für Zertifikate und Keys. Beide werden mit diesem einen Passwort entsperrt).

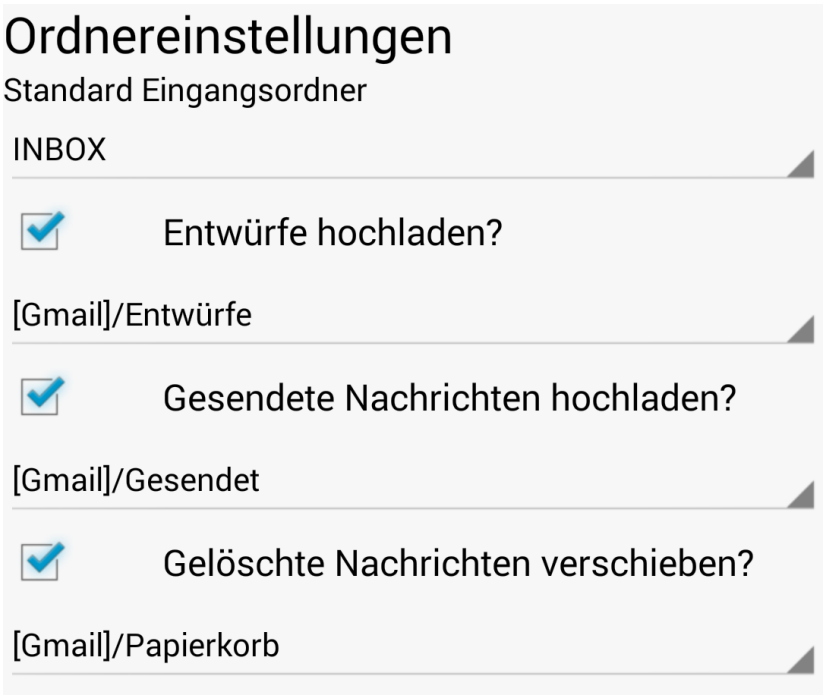


Direkt im Anschluss kann der Email-Account eingerichtet werden.

Passwort eingeben für das Email-Konto

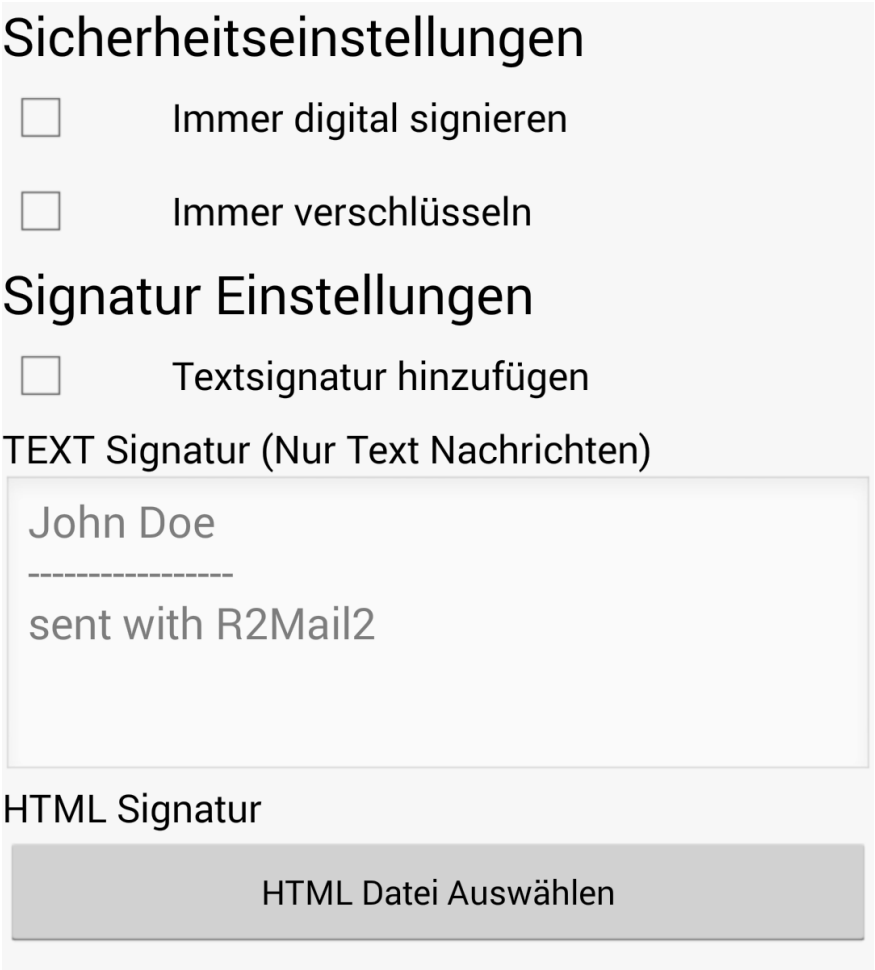


Bei der Einrichtung eines IMAP-Kontos kann ausgewählt werden, ob die Nachrichten automatisch zum Email-Anbieter hoch geladen werden. Wenn die Haken nicht gesetzt werden, bleiben die Entwürfe, gesendete und gelöschte Emails nur auf dem Gerät gespeichert.

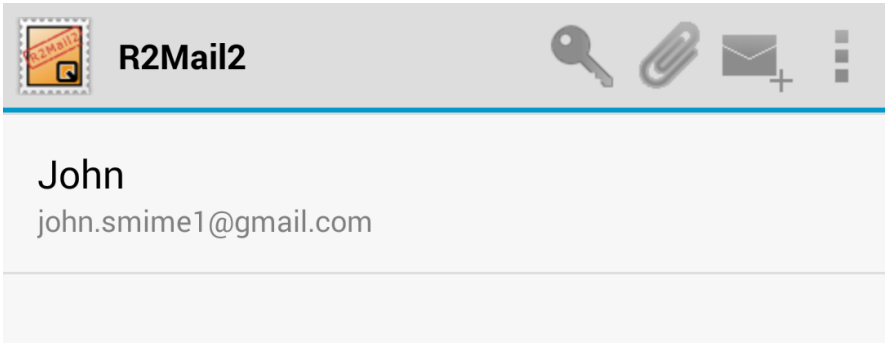


Am Ende der Einrichtung kann ausgewählt werden, ob Emails generell digital signiert werden oder ob jede Email digital signiert **und** verschlüsselt wird.

Hinweis: Ist „Immer verschlüsseln“ ausgewählt, muss zwingend der öffentliche Schlüssel aller jeweiligen Empfänger vorhanden sein, sonst kann die Email nur unverschlüsselt versendet werden.

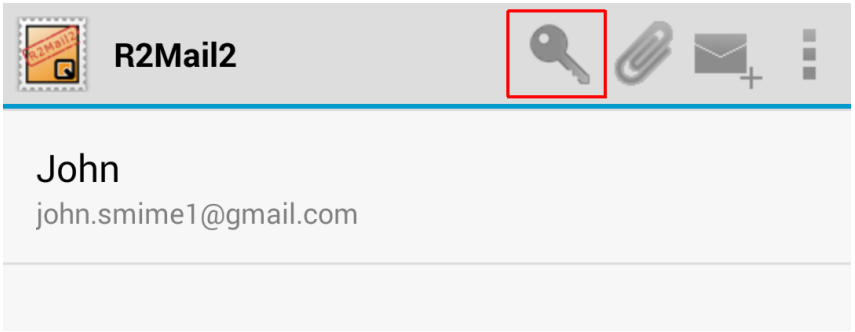


Danach ist der Email-Account fertig eingerichtet.

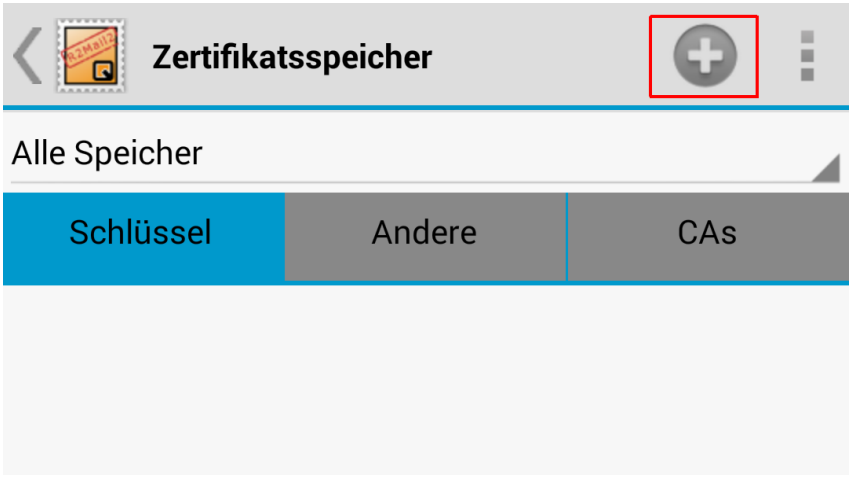


Schritt 2: Installieren der Zertifikate in R2Mail2

In der Hauptansicht auf den Schlüssel tippen:

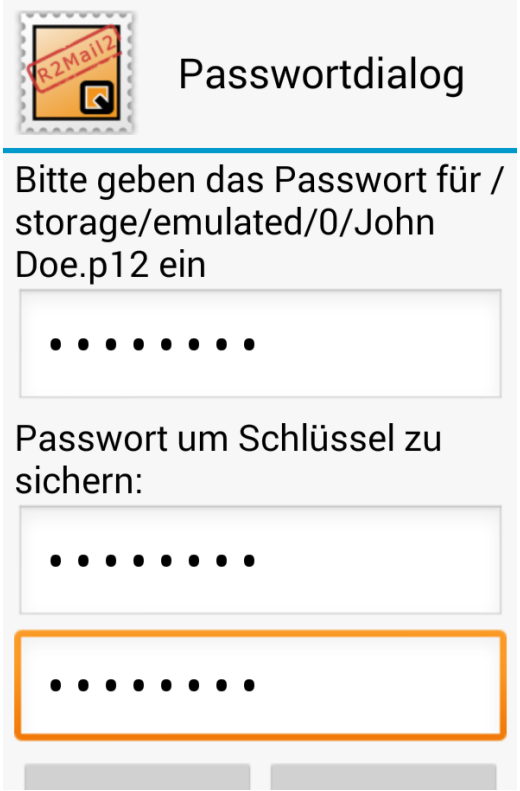


Im nächsten Fenster sind noch alle Felder leer. Hier einfach auf das Plus-Symbol tippen. Danach kann die P12-Datei ausgewählt und importiert werden.

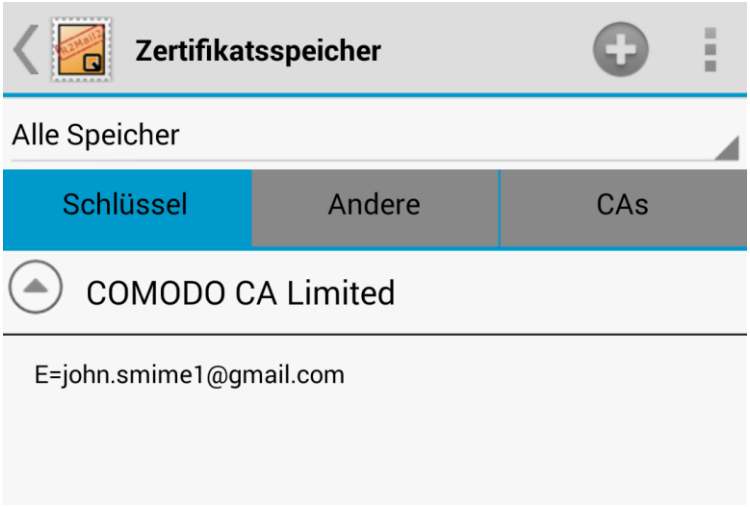


Beim Import muss das Passwort angegeben werden, das beim Export der P12-Datei aus Firefox oder Thunderbird gesetzt wurde.

Gleichzeitig muss ein Passwort gesetzt werden, um den privaten Schlüssel in R2Mail2 zu schützen. Dies kann entweder ein neues oder das gleiche sein, mit dem auch die P12-Datei geschützt war.



Nach einem erfolgreichen Import wird das Zertifikat unter „Schlüssel“ angezeigt.

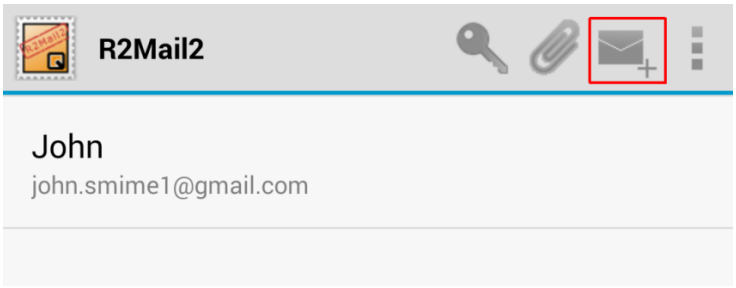


Schritt 3: Senden und Empfangen verschlüsselter Emails

Der erste Kommunikationsteilnehmer sendet eine signierte Email, der zweite kann sofort verschlüsselt antworten.

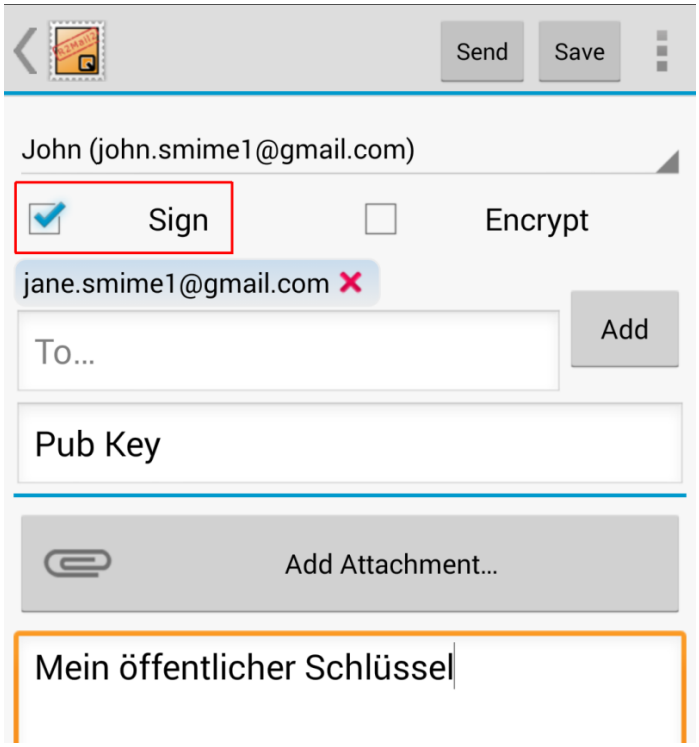
a) Schreiben einer signierten Email

Im Hauptfenster auf das Email-Symbol mit dem Plus-Zeichen tippen:



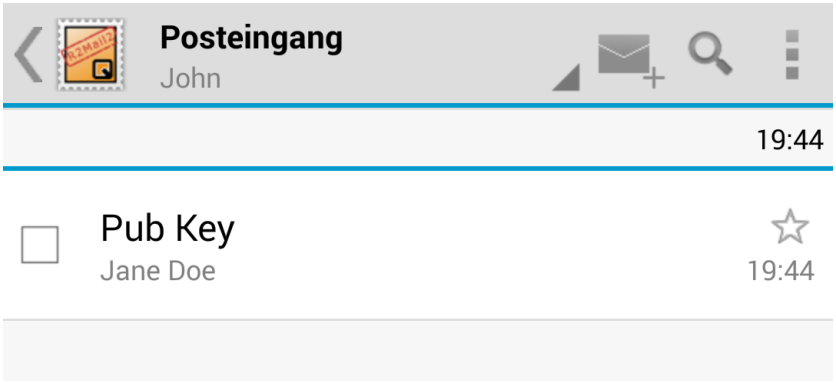
Ein Haken muss bei „Signieren“ gesetzt werden.
Es kann ausgewählt werden, ob die Email nur signiert oder auch verschlüsselt werden soll. Da bisher keine weiteren Zertifikate von Dritten vorhanden sind, ist nur signieren möglich.

Nach Erhalt der signierten Email ist der Kommunikationspartner im Besitz des öffentlichen Schlüssels und kann mir somit verschlüsselte Emails zusenden.



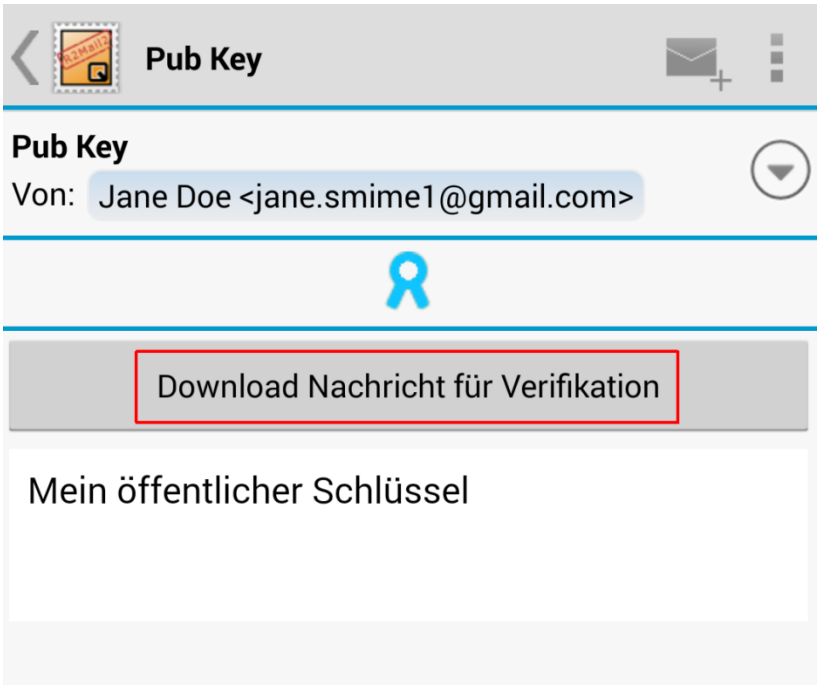
b) Empfangen einer signierten Email

Wenn ein Kommunikationspartner eine Email schreibt und diese digital signiert, dann kann der öffentliche Schlüssel direkt in meinem persönlichen Speicher abgespeichert werden.



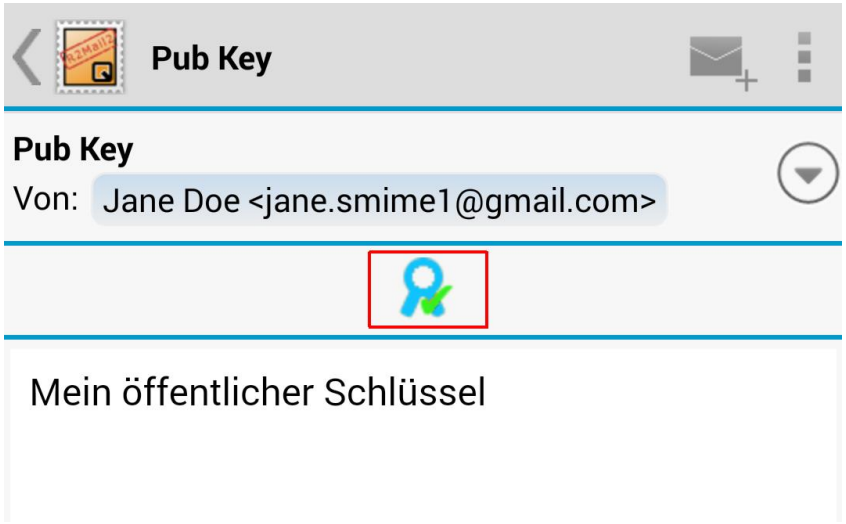
Wenn die Email geöffnet wird, kann man an dem blauen Symbol erkennen, dass die Email digital signiert ist. Wenn auf „Download Nachricht für Verifikation“ getippt wird, wird der öffentliche Schlüssel anhand des Zertifikats verifiziert. Hier werden die Gültigkeit und die Zertifikatskette überprüft.

Hinweis: Es kann in den Optionen eingestellt werden, dass Emails automatisch herunter geladen werden. Dann entfällt der Punkt „Download Nachricht für Verifikation“. Die Signatur wird dann nach dem Download automatisch verifiziert.

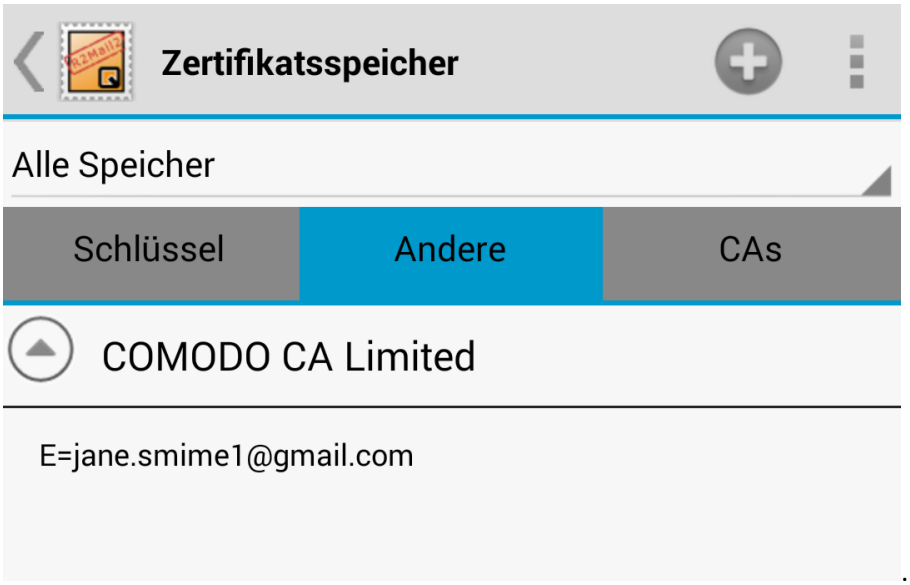


Ist alles korrekt, wird ein grüner Haken angezeigt.

Um das Zertifikat anzuzeigen und importieren zu können, auf das blaue Symbol mit dem grünen Haken tippen:



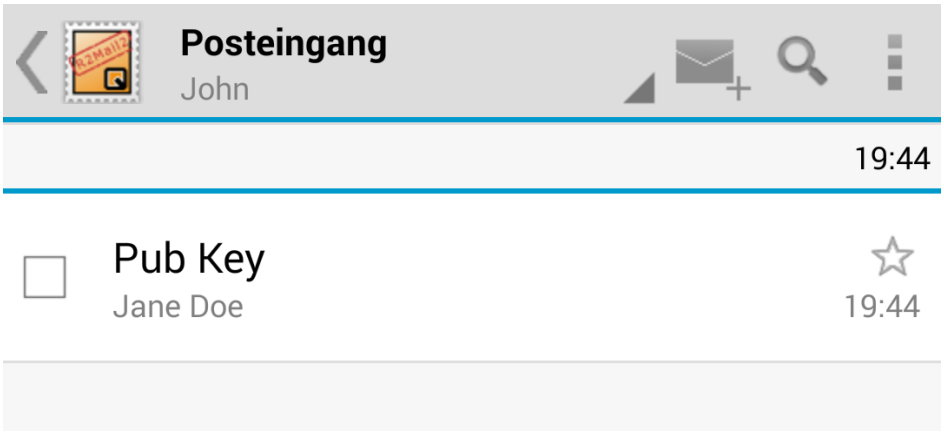
Hier werden nun alle wichtigen Informationen des Zertifikats angezeigt.
Über „Importiere Zertifikat in persönlichen Speicher“ wird der öffentliche Schlüssel abgespeichert und im Zertifikatsspeicher unter dem Reiter „Andere“ angezeigt.



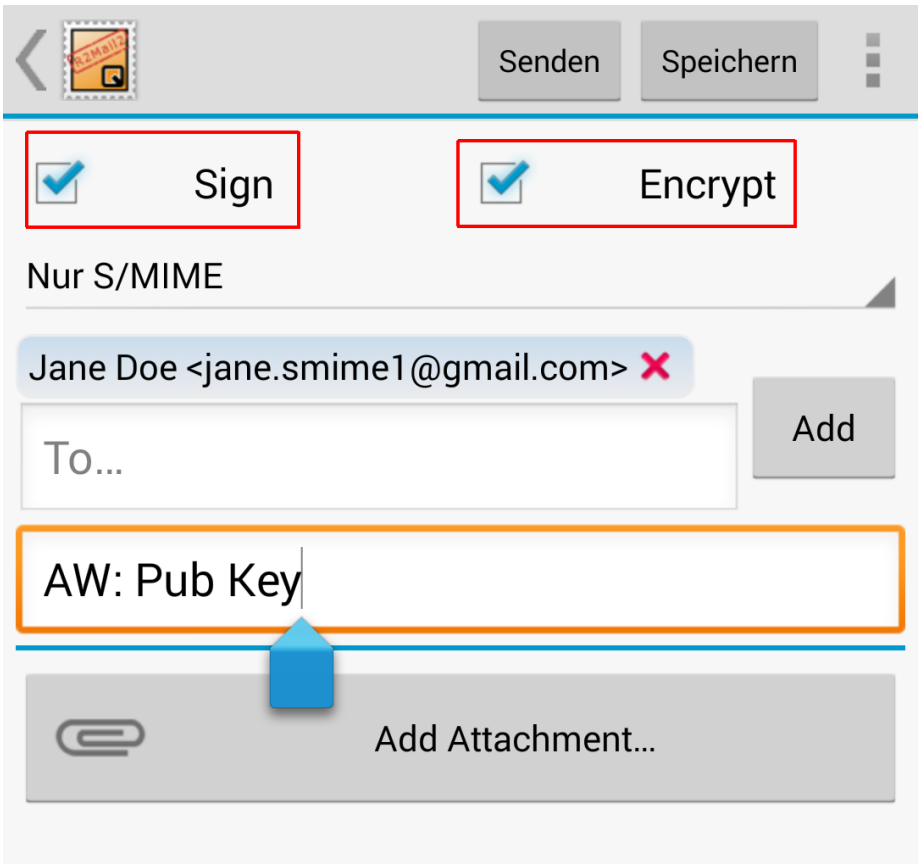
Nun können Emails an den Kommunikationspartner verschlüsselt werden.

c) Schreiben einer verschlüsselten Email

Im Posteingang die signierte Email des Kommunikationspartners öffnen:

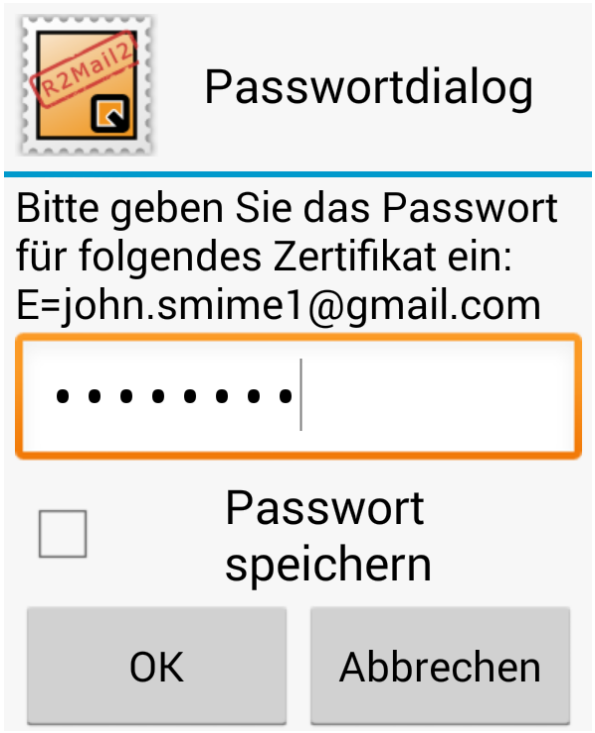


Im nächsten Schritt „Signieren“ und „Verschlüsseln“ auswählen:



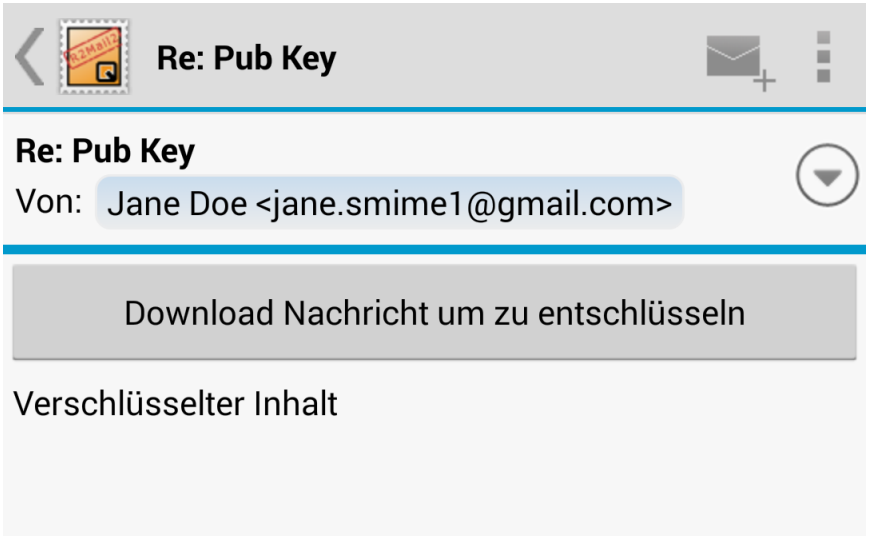
Vor dem Versenden muss das Passwort eingegeben werden, mit dem der private Schlüssel in R2Mail2 abgesichert ist. Man kann hier auch „Passwort speichern“ anhaken. Dann wird man in Zukunft nicht mehr danach gefragt.

Hinweis: Da R2Mail2 noch mit einem Master-Passwort gesichert ist, das je nach Einstellung bei jedem Aufruf des Programms eingegeben werden muss, kann diese Option ausgewählt werden.
Danach erfolgt die Signierung und Entschlüsselung ohne Passworteingabe.



d) Empfangen einer verschlüsselten Email

Wenn eine verschlüsselte Email empfangen und geöffnet wird, dann muss zuerst der Inhalt der Email herunter geladen werden. Dies geschieht je nach Einstellung automatisch (siehe S.28).



Dabei wird automatisch die Signatur (wenn vorhanden) verifiziert und die Email entschlüsselt.
Sollte im vorigen Schritt schon „Passwort speichern“ ausgewählt worden sein, entfällt dieser Dialog.

Die verifizierte und entschlüsselte Email liegt nun vor:
Links das blaue Symbol mit grünem Haken, das anzeigt, dass die Signatur erfolgreich verifiziert werden konnte, und rechts das blaue Schloss-Symbol, das anzeigt, dass die Email verschlüsselt empfangen wurde.