Welcome to
And You And I

The protection of your communication contents is in your own responsibility. To rely on others means to take bad risks.

And You And I helps you to send and read encrypted mails with your iPhone, iPad, or iPod in a quick and straightforward way.

User´s guide ▶

Background information

▼

End-to-End Security for Mails

For a secure exchange of mails it is not sufficient to protect the transport to the next mail server with SSL, or to encrypt them on server side.

Only end-to-end encryption ensures that your sensitive data reach the desired recipients without being disclosed or read before.

The content of your mails is protected at any time and at any place only this way.

Keys for S/MIME in iOS

Apple iOS supports end-to-end encryption with the S/MIME format.

Apple iOS also offers to secure local files with "Data Protection", which disables file read access from a locked device.

And You And I generates keys and certificates that can be used for S/MIME.

It´s crucial how these keys are generated, stored, and handed over.

Protection of your Privacy

All keys are generated and managed on your device based on strong cryptography.

This is done without using or calling external services from the Internet.

You decide on your own which sensitive data is stored where and how long.

The mail encryption itself is completely done by the Mail App of iOS, once you assign the keys to your mail accounts.

Secure Implementation in And You And I

And You And I also uses strong cryptographic algorithms to protect your keys.

A condition for secure, non-guessable or predictable keys is very good random number data, best done by collecting a lot of digitalized live events from the analogue world outside.

The protection by passwords and their strength is also important: The longer the better, with sufficient complexity.

Random Seed and Passwords

Random bits are retrieved from your device´s gyroscope during each app launch, when you smoothly move it in your hands ("Random Seed").

All data is encrypted at any time, using an ID Password of your own choice.

The ID Password can be changed anytime, and must be longer than 15 characters.

All generated keys are encrypted again, using a unique strong random password.

Data Protection Permissions - Contacts

And You And I requires your personal mail address, first and last name, and your city, to put it into your certificate.

You are asked for the permision to read your contacts when the first key identity is created.

If you do not want to grant this permission, you can deny for the time being, and enter all personal data manually.

Data Protection Permissions - iCloud

And You And I allows to synchronize your strong encrypted keys and certificates with other iPhones, iPads, or iPods, using Apple iCloud.

If you do not want to use iCloud, you can disallow it in the system settings or in the app settings for the time being, and manage your data locally.

And You And I

Free S/MIME Certificates
for Apple iPhone and iPad

Available on the App Store

http://andyouandi.eu

Made somewhere in Hessen, Germany.

User´s guide ▶