

Latest IRMA developments

Surfnet, Utrecht

Sietse Ringers

3 november 2017

Overview

- * Redesigned IRMA app for iOS
- * Newly available attributes
 - * Mobile phone numbers
 - * IBAN numbers (soon)
- * IRMA attribute-based signatures plans

IRMA on iOS

- * Platform-independent (mostly)
 - * Android-version will eventually replace current Android app
- * Redesigned, more friendly graphical interface
 - * Future version will include Dutch translations
- * Consists of two parts:
 - * IRMA engine written in Go
 - * Graphical interface in React Native
- * Thanks to Maarten Everts and Tomas Harreveld!

Mobile phone number attribute

- * Via: <https://privacybydesign.foundation/issuance/>
 - * choose mobile phone number issuance
- * Provide your (Dutch) mobile phone number
 - * a text (SMS) message is sent to this number — free of charge
 - * it contains both a code and a link
 - * either of them generates a QR-code for issuing the number
- * Service is experimental, via foundation's own sms server

- * Thanks to student-employee Ayke van Laethem!

Planned: IBAN attribute

- * Foundation has subscribed to iDeal for online payments
- * Procedure for obtaining IBAN attribute:
 1. transfer €1 to foundation's bank account via iDeal
 2. foundation receives confirmation message ("F-bericht") with name of bank account holder and IBAN number
 3. The foundation then issues these data as attributes
- * Combined iDeal + iDIN issuance
 - * after the "free-of-charge" iDIN pilot period is over
 - * the foundation basically passes on the bank's charges

IRMA attribute-based signatures

- * IRMA attributes cryptographically attached to a message
- * Examples:
 - * attach your “I am a teacher” attribute to student grades
 - * Attach your IBAN attribute to “I transfer €10,- to S. Ringers”
- * A subproject has started to make a signature ecosystem
 - * work done jointly with Alliander

IRMA attribute-based signatures

- * Cross-platform desktop application for making “IRMA signature requests”
- * Workflow:
 - * You choose:
 - * a text, to be signed — flat text at first
 - * a list of attributes to be included
 - * the request is sent, as email attachment, to the signer
 - * clicking on the attachment opens the IRMA app for signing
 - * the requester gets a copy, and the signer retains one
- * Long term strategy: authentication for free, signing via subscription

Audience feedback/input

- * Suggestions for additional IRMA attributes?
 - * New verification/deployment options?
 - * current pilots in preparation in education and health care
 - * Volunteers for signature contribution/evaluation?
 - * Any other feedback . . .
-
- * Stay informed: https://twitter.com/IRMA_privacy