Attribute based authentication and more using IRMA

Jean Popma

Interfacultary Hub for Security, Privacy and Data Governance

Privacy by Design Foundation

J.Popma@ru.nl 18-10-2019

Radboud University

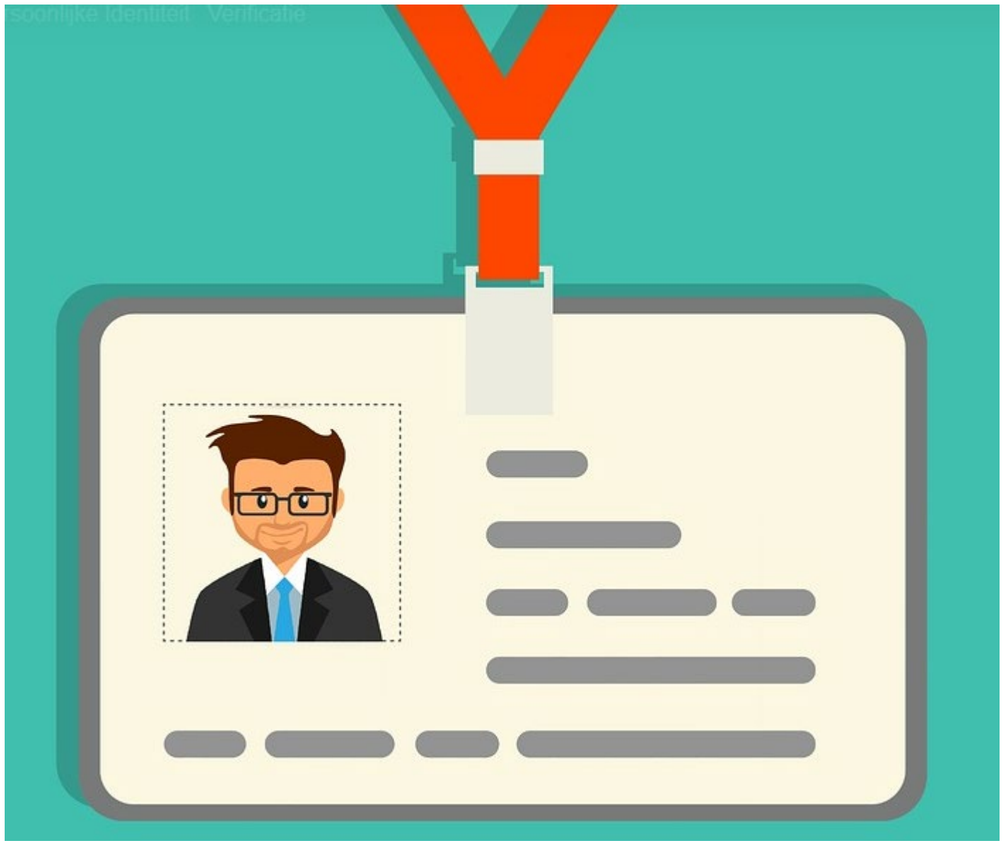
About myself

- Datacenter manager 1987-2000 at Radboud University
- Managing director of ICT-service centre from 2000 to 2013 at Radboud University
- Corporate Information Security Officer and acting Privacy Officer from 2013-2016 at Radboud University
- Chairman of CERT-RU 2001-2017
- SURF CyberSaveYourself steering committee 2012-2016 https://www.cybersaveyourself.nl/
- Member of the board of the Privacy by design Foundation (working on IRMA, https://privacybydesign.foundation)
- Currently Project Manager Applied Security Research working on PEP https://pep.cs.ru.nl/ at iHub, Radboud University

Radboud Interdisciplinary Hub for Security, Privacy and Data Governance

https://www.youtube.com/watch?v=yA4aRrbKsH0

What is identity?



Digital identity examples

Digital identity is widely used

- Online banking (authentication, signing)
- Buying alcoholic beverages: copy of ID? proof that age>18?
- Opening accounts (facebook's 'real name policy'?)
- Information request under GDPR
- Buying in a webshop
- Buying at Ebay, Marktplaats….
- Physical access (by card or device)
- Access to health-related information
- …….

Real world versus virtual world identities

NOISE TO SIGNAL
RobCottingham.ca/cartoon

1993 .....

"On the internet nobody knows you're a dog"
(Peter Steiner, New Yorker, 1993)

.... Is history

How the hell does Facebook know I'm a dog?

Attributes

Attributes are properties of people with some level of stability

- Examples: given name, family name, gender, age, date of birth, phone number, physical addres, e- mail address, social security number, profession, employer etc.
- Attributes are typically limited pieces of information, linked to a natural person.
- Attributes are clearly distinguished from ‘records’ and ‘dossiers’
- An attribute can be
  - (uniquely) identifying in a given context (student number, social security number, driver’s licence number etc.)
  - Non-identifying (gender, older than 18, registered doctor, postal code etc.)
- Attributes have a certain validity period (data of birth, gender, address, ‘younger than 18’)
- Attributes may differ in level of trust (social security number, facebook ID, bank credentials)

Identity & Attributes

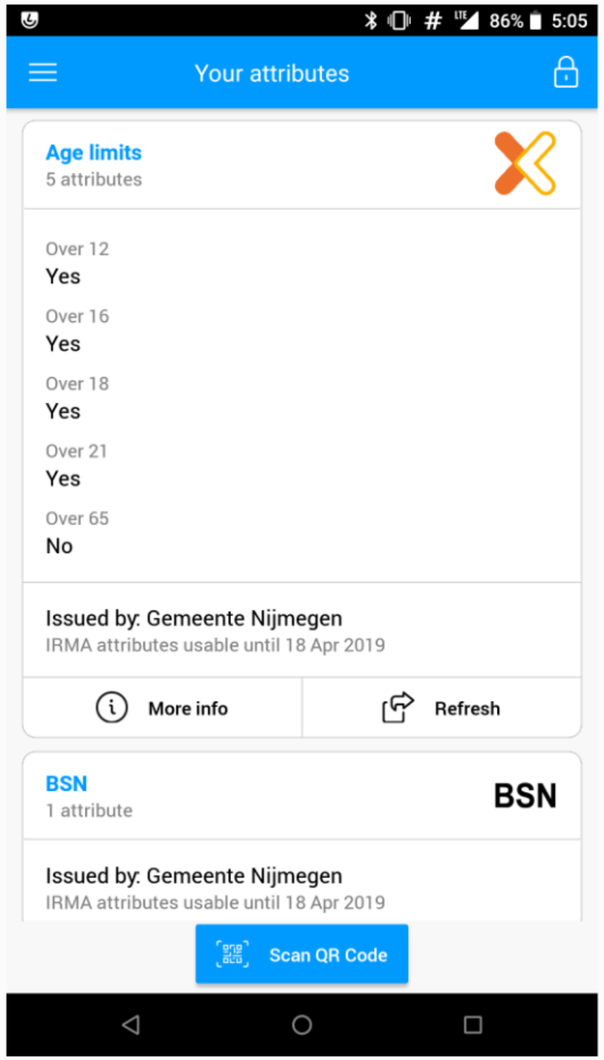
Definition:
The (complete) identity of a person is a set of all attributes that hold for that person – at a particular point in time.

- Basic Ideas about attributes as part of an identity:
  - Authentication can be contextual (different attributes can be used in different contexts)
  - Only necessary information is shared (minimisation)
  - Authorisation can be done based on attributes. For example participation in closed discussion groups (age, gender restricted, student in a course, patients peer groups): a social security-number or copy of passport is not adequate.

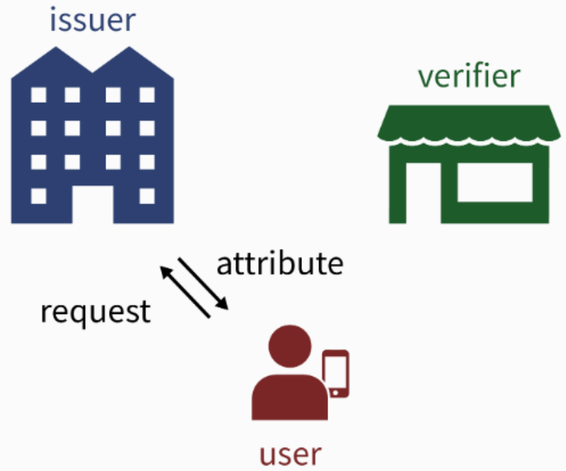
Digital identity

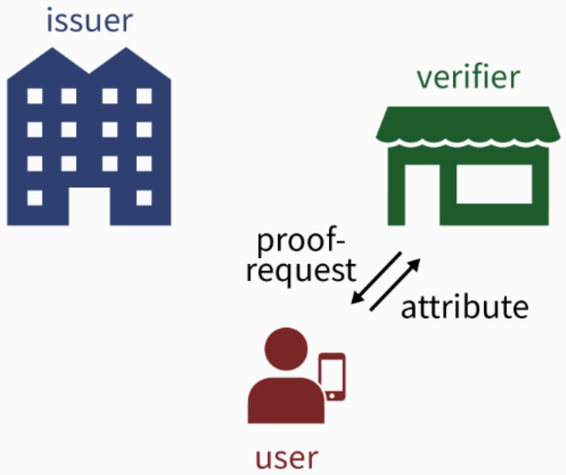
- Used for
  - Authentication (followed by authorisation)
  - Encryption
  - Signing
- Properties
  - Attribute based
  - Irrefutable
  - Verifiable
- Requirements
  - Lawful use
  - Minimisation

The IRMA attribute based identity platform

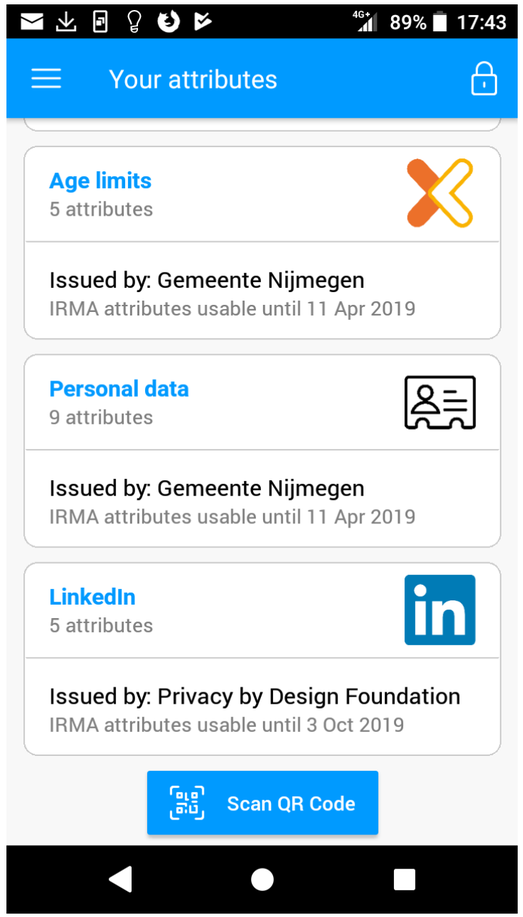


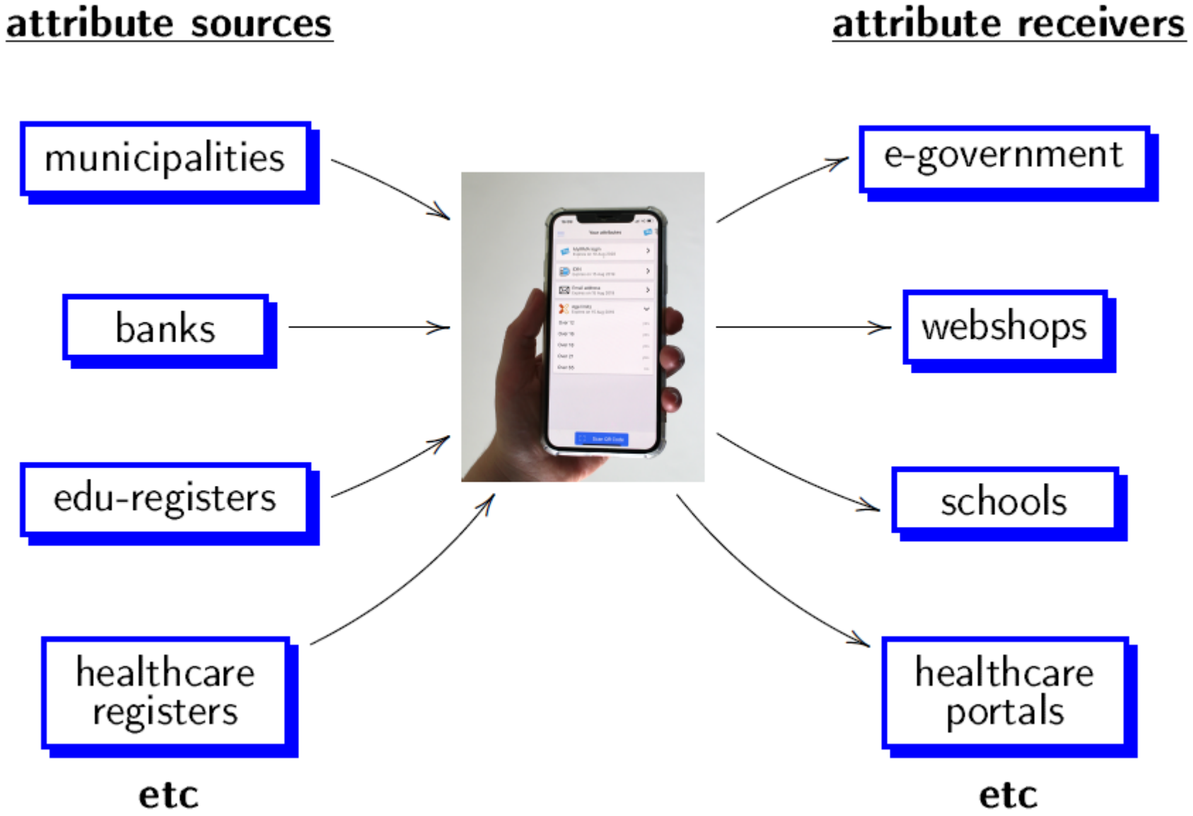
- User collects attributes
- Attributes are digitally signed by trusted issuer
- Identifying (name) or not (> 18)
- Multiple disclosures are unlinkable
- Decentral: attributes are stored only on phone
- IRMA PIN to unlock app & attributes
- Free and open source





The IRMA attribute based identity platform

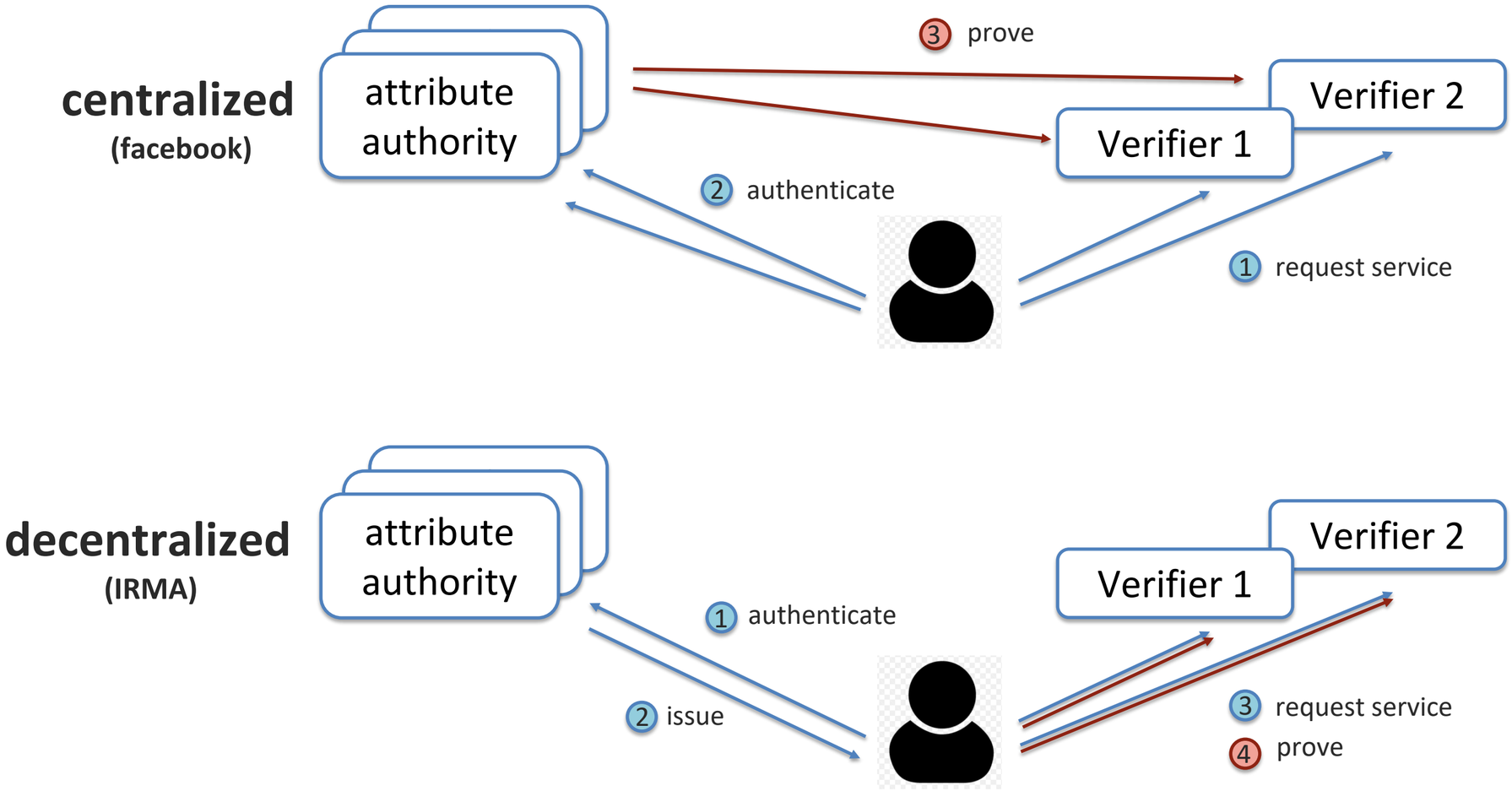




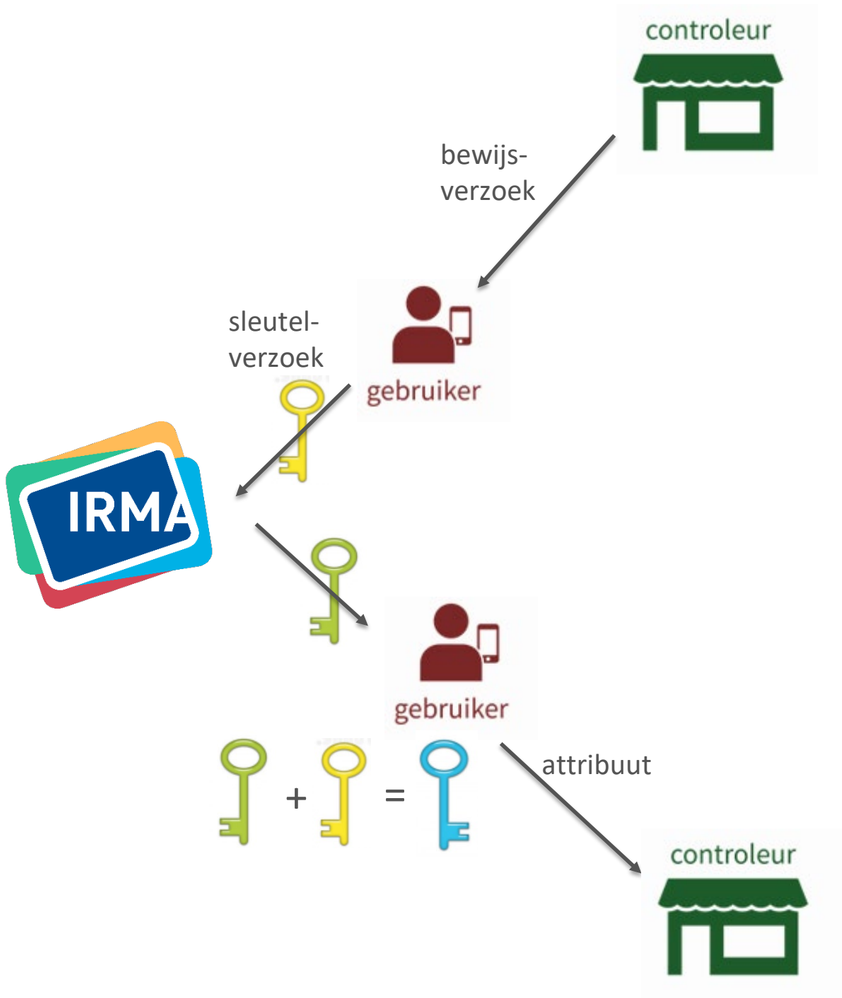
Attributes currently available

- 20 attributes from central citizen registration (Basisregister persoonsgegevens, BRP), including the social security number (BSN), and name/address/date of birth
- 8 attributes from IDIN (bank) including address, name, address, date of birth)
- 8 attributes from SURFnet (employee/student status at any university or applied science university)
- 1 attribute Phonenumber
- 1 attribute verified e-mail address
- BIG (registered and authorized health care professionals)
- AGB (administrative ID for health-care profesionals)
- (…)

Centralized versus Decentralized



IRMA Split Key

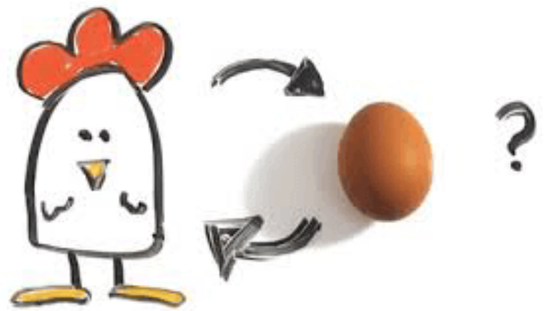


Digital signatures

- Use of public/private key technology
- A digital signature contains attributes about yourself, signed with a private key.
- Verifiable attributes themselves (I am a doctor, I am an employee of...., My name is …. Etc) can be part of the signature.
- Authenticity can be verified by anyone using your public key.
- Signature becomes void if signed document/content is changed after signing

From Chicken to Egg (or vice versa?)

Radboud University: Academic phase, research and initial development 2008-2016



2014

- Antonio de la Piedra, Jaap-Henk Hoepman, and Pim Vuller
  Implementation of Attribute Based Credentials on Smart Card
  International Conference on Cryptology and Network Secu
  Gritzalis, Aggelos Kiayias, and Ioannis Askoxylakis (Eds.), Sp
  p.270-289. Paper
- Pim Vullers, *Efficient Implementations of Attribute-based Cred*
  Thesis, Radboud University, 2014. pdf.
- Merel Koning, Paulan Korenhof, Gergely Alpár and Jaap-Her
  Cs: an analysis of attribute-based credentials in the light of data p
  ty. Version of Internet, Law and Politics 2014 conference, an
  2014 symposium.

2019

Brouwer prijs 2018

KONINKLIJKE
HOLLANDSCHE MAATSCHAPPIJ
DER WETENSCHAPPEN

De Koninklijk Hollands Maatschappij der Wetenschappen (KHMW) rijkt jaarlijks de Brouwer prijs uit voor wetenschap en samenleving. Deze prijs wordt in 2018 toegekend aan de stichting Privacy by Design. De jury waardeert dat de stichting met IRMA mensen weer grip op de bescherming van persoonsgegevens verschaft en daarmee, bij alle technologische ontwikkelingen, vertrouwen in de samenleving geeft. De jury, heeft naast de maatschappelijke urgentie van het initiatief, vooral het criterium van de wetenschappelijke onderbouwing zwaar laten wegen. Aan de prijs is een geldbedrag van honderdduizend Euro verbonden.

IRMA wint Internet Innovatie Award 2019

De stichting Privacy by Design heeft de Internet Innovatie Award 2019 van de Internet Society gewonnen voor het identiteitsplatform IRMA.

12th International Workshop on Sec
LNCS 9871, 2016, p.106-121. Paper
Gergely Alpár Lejla Batina, Lynn Bat
Guellier, Iynkaran Natgunanathan. *M*
thentication - Position Paper. 1st ACM
Internet of Things (MAL-IoT 2016),
Sietse Ringers, *Quantization using J*
dential Schemes, PhD Thesis, Groni

)15

Brinda Hampiholi, Gergely Alpár,
cal Attribute-Based Signatures. In: *I*
Proceedings of the Fifth Internat
Cryptography Engineering (SPA
p.310-328. Paper.
Antonio de la Piedra. 2015. *Efficie*
Cs. In Revised Selected Papers of the 7th International Conference on Trusted
Volume 9565 (INTRUST 2015), Moti Yung, Jianbiao Zhang, and Zhen Yang (Eds.), Springer LNCS 9565, 2015, p.183-199. Paper
Gergely Alpár, *Attribute-Based Identity Management*, PhD Thesis, Radboud University,

Nederlandse Privacy Award 2018

De stichting Privacy First heeft in january 2018 de *Nederlandse Privacy Award* toegekend aan het identiteitsplatform IRMA. De jury prijst de privacy by design-opzet, het grote innovatieve vermogen, en de potentiële maatschappelijke impact van IRMA. Deze prijs is een eervolle erkenning van IRMA's sterke focus op privacybescherming. Er is geen geldbedrag aan verbonden, maar wel een kunstwerk, zoals op afgebeeld op het bijgaande plaatje.

iHub

privacy by design

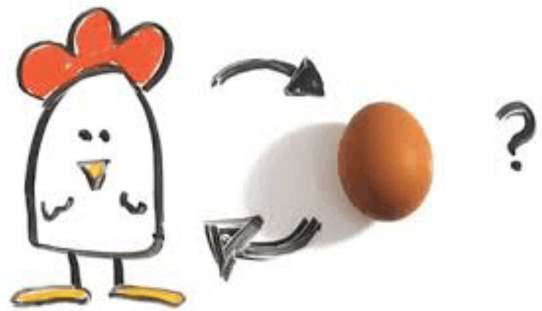
Radboud University

From Chicken to Egg (or vice versa?)

Radboud University: Academic phase, research and initial development 2008-2016

Privacy by Design Foundation: Widening, pilot projects 2016-2020

- Municipalities (> 20 cities will start to use IRMA)
- Health care
- Edu sector



Identity in healthcare: lots of actors, lots of islands

Patients

- Identity must be known to professionals & administration, but not elsewhere (as a patient)
- need strong (mfa) authentication for online access of records
- may need anonymous access, f.i. For discussion groups.
- need a way to mandate others to act on their behalf

Participants in health research projects

- Identity must be known during the data collection phase
- but not during the analysis phase (context switch)
- Requires pseudonymisation and (controlled) possibility for de-pseudonymisation

Professionals

- identity must be known to patients (authorisation and accountability)
- with roles and corresponding authorisations

Organisations

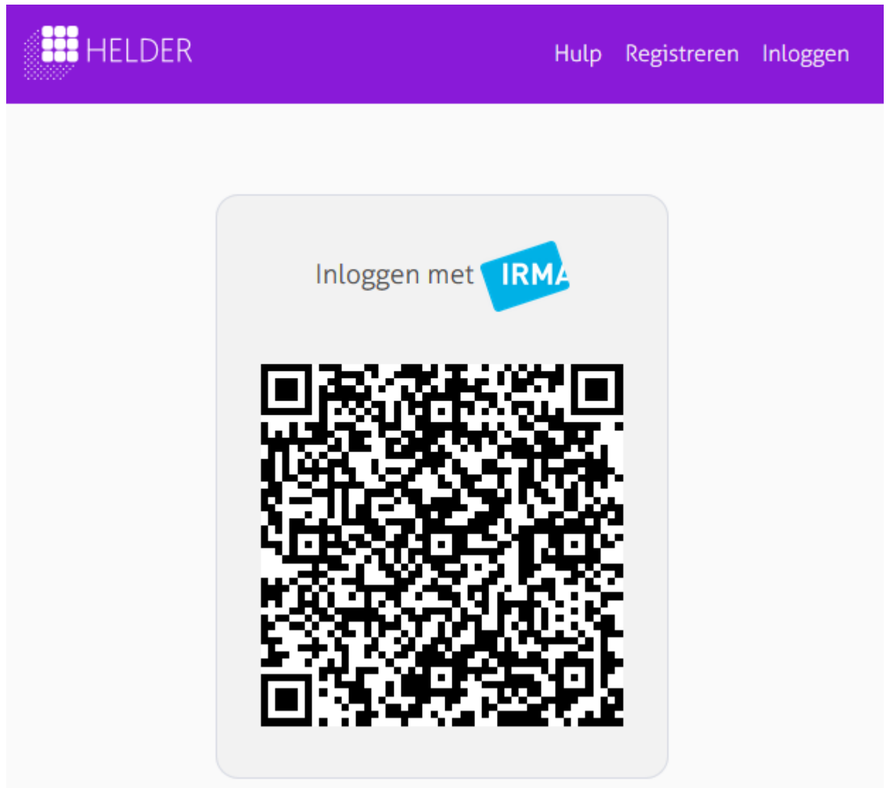
- Need to comply with legal and regulatory requirements. Most of them are not able to do that.

What is happening in the health-sector?

Lots of solutions/variations but none are satisfactory:

- Patients need to acquire many different technical solutions and skills to use them (passwords, OTP, multifactor authentication etc.)
- DigiD is a payed service : € 0,14 / transaction
  - iDIN (identity service of the banking sector) is even more expensive
  - Large organisations can afford this, but individual professionals cannot.
- Attributes for contextual authentication are lacking: therefore no possibility for authentication based on role, purpose etc.
- (Role-based) Digital signatures are not supported – or very expensive.

Nedap: Helder



Hallo huisarts!

De afgelopen jaren zijn de meeste thuiszorgschriftjes van de keukentafels weggedigitaliseerd. Dit heeft veel voordelen opgeleverd voor de zorg, maar het heeft de samenwerking tussen zorg en huisarts wel lastiger gemaakt.

Dat hebben we opgelost: vanaf nu kun je inloggen op Helder en jezelf toegang verschaffen tot een groeiend aantal thuiszorgdossiers van jouw patiënten.

Online samenwerken met de thuiszorg was nog nooit zo makkelijk!

Wat is het?

Helder is een webapplicatie die je ook als mobiele app kunt installeren. Daardoor is Helder zowel handig op de praktijk als onderweg of bij de patiënt thuis.

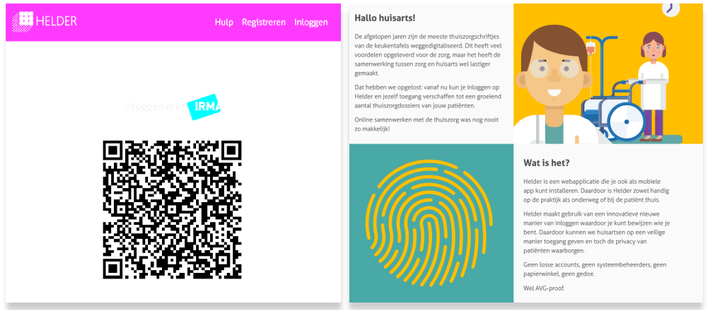
Helder maakt gebruik van een innovatieve nieuwe manier van inloggen waardoor je kunt bewijzen wie je bent. Daardoor kunnen we huisartsen op een veilige manier toegang geven en toch de privacy van patiënten waarborgen.

Geen losse accounts, geen systeembeheerders, geen papierwinkel, geen gedoe.

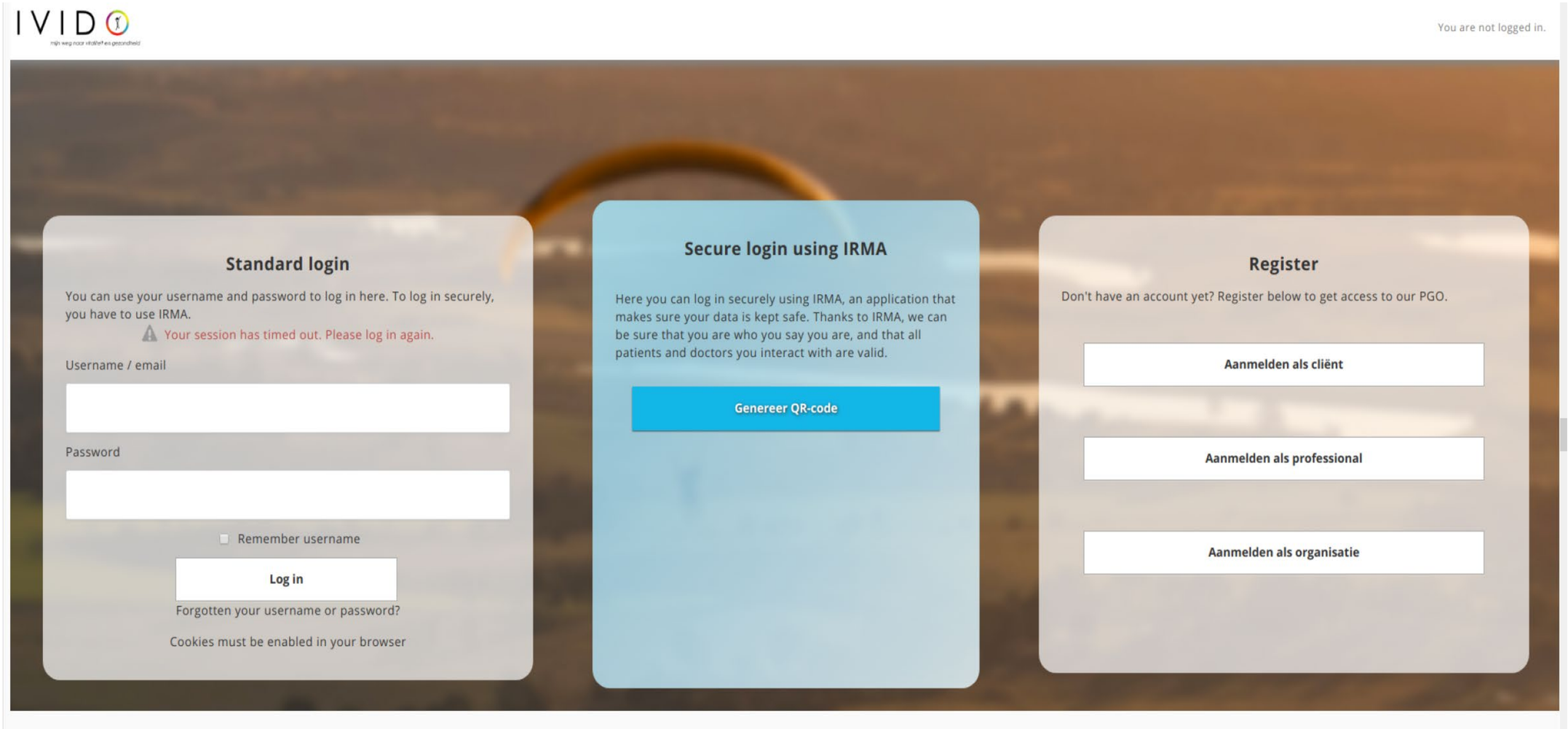
Wel AVG-proof.

Nedap: Helder

- Dossier homecare accessible by GP (huisarts)
- soon:
  - GP can add to dossier
  - Medication overview
  - Contact details of next of kin (mantelzorgers)
  - Signed care-requests from GP to home-care
  - ....



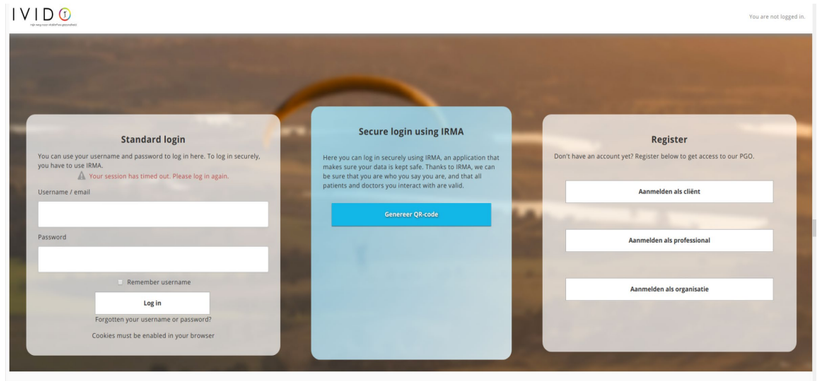
IVIDO PGO


IVIDO
You are not logged in.
Standard login
You can use your username and password to log in here. To log in securely, you have to use IRMA.
Your session has timed out. Please log in again.
Username / email
Password
Remember username
Log in
Forgotten your username or password?
Cookies must be enabled in your browser
Secure login using IRMA
Here you can log in securely using IRMA, an application that makes sure your data is kept safe. Thanks to IRMA, we can be sure that you are who you say you are, and that all patients and doctors you interact with are valid.
Genereer QR-code
Register
Don't have an account yet? Register below to get access to our PGO.
Aanmelden als cliënt
Aanmelden als professional
Aanmelden als organisatie

IVIDO PGO

- A Personal Health Environment (‘PGO’) is a communication tool and data repository for patients and professionals
- It can link to and receive data from many different sources (portals)
- A PHE is patient centered , as opposed to any portal
- The patient is in control, and is able to grant access

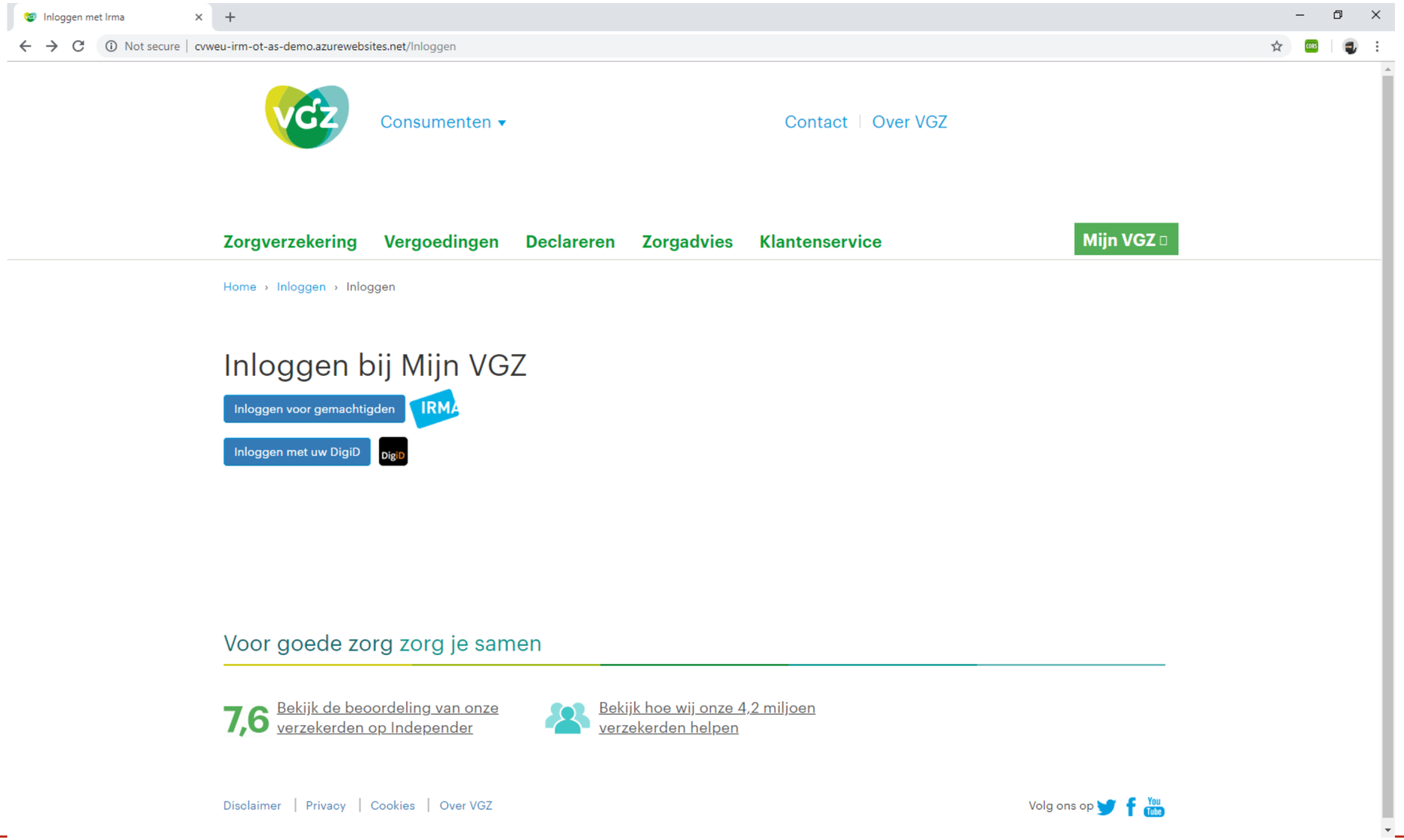
  to professionals.



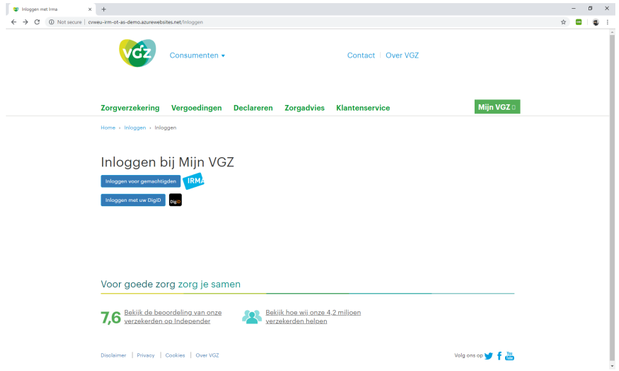
PHE/PGO the identity schizophrenia

- Use of Social Security number (‘BSN’) is **not allowed** for giving a patient access to her PHE/PGO
- Use of Social Security Number is **required** for giving a patient access to a health portal
- Result: at least two independent authentications and authentication means necessary.
- Irma can do both, which reduces the burden to a great extent.

VGZ: Mandate


Inloggen met Irma
Not secure | cvweu-irm-ot-as-demo.azurewebsites.net/Inloggen
VGZ
Consumenten
Contact | Over VGZ
Zorgverzekering
Vergoedingen
Declareren
Zorgadvies
Klantenservice
Mijn VGZ
Home › Inloggen › Inloggen
Inloggen bij Mijn VGZ
Inloggen voor gemachtigden
IRMA
Inloggen met uw DigiD
DigiD
Voor goede zorg zorg je samen
7,6
Bekijk de beoordeling van onze verzekerden op Independer
Bekijk hoe wij onze 4,2 miljoen verzekerden helpen
Disclaimer | Privacy | Cookies | Over VGZ
Volg ons op

VGZ : mandate



- Current practice: people give their (DIGID) cedentials to someone else
  - This means a mandate to everything
  - Might be ok with a close family member, but not with a professional or volunteer
- Idea: provide a specific attribute for a certain mandate
  - With this attribute a specific mandate is given to someone. In case of VGZ: to attend all affairs regarding the health insurance.
  - Mandate can be revoked at any time
- Status: Prototype is working

Persoonsgegevens opladen in IRMA-app

Nijmegen doet mee aan een proef met het toegankelijker maken van uw digitale gegevens. En u meer controle te geven over uw digitale identiteit. Hiervoor gebruikt u de app IRMA. Als u de IRMA-app geïnstalleerd heeft, kunt u ons vragen uw persoonsgegevens uit de Basisregistratie Personen (BRP) door te geven aan IRMA.

REGELEN

DigiD

Wat u moet weten

Gegevens uit de BRP

Amsterdam geautoriseerd een gegevensmanager

Basisidentiteit

BRP

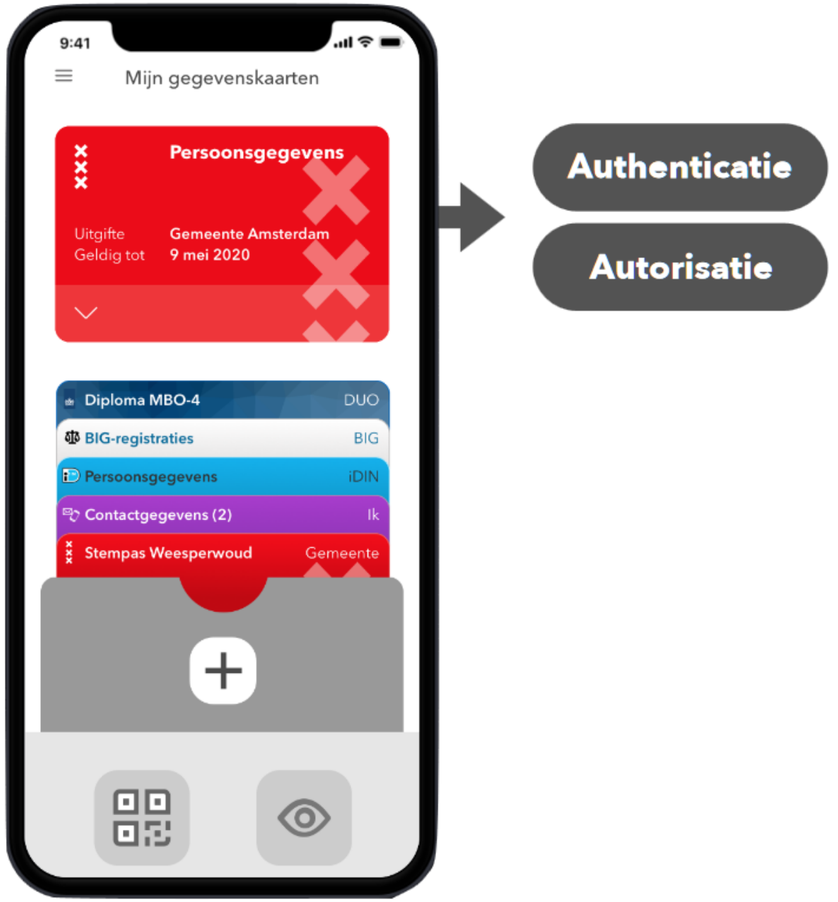
- Voornaam
- Achternaam
- Geslacht
- BSN nummer
- Nationaliteit
- Inschrijving
- Verblijfplaats

DI-Pasfoto

+

Je zet je eigen gegevens uit het basisregister versleuteld op je mobieltje en gebruikt die daarna als 'losse' kaarten die je per situatie kunt gebruiken voor authenticatie of autorisatie.

Gegevenskaarten



Authenticatie

Autorisatie

Lokale Digitale Democratie met Consul

Gemeente Groningen

Log in

Log in via:

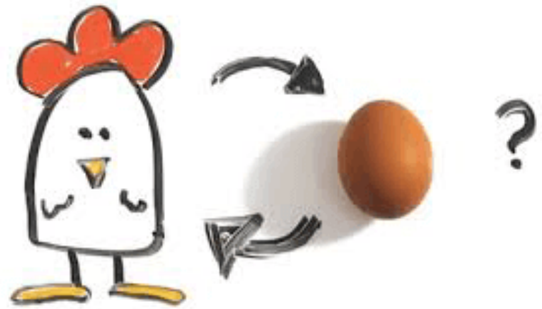
IRMA

From Chicken to Egg (or vice versa?)

Radboud University: Academic phase, research and initial development 2008-2016

Privacy by Design Foundation: Widening, pilot projects 2016-2020

- Municipalities (> 20 cities will start to use IRMA)
- Health care (Helder, Ivido, VGZ)
- Edu sector



- PBD/SIDN : professionalising and use as a community infrastructure 2019-
  - Durable and long term business plan
  - Uptime and quality guarantees
  - Support organisation

Legal aspects

- DPIA has been concluded and published:

  https://privacybydesign.foundation/pdf/DPIA-IRMA-dec-2018.pdf

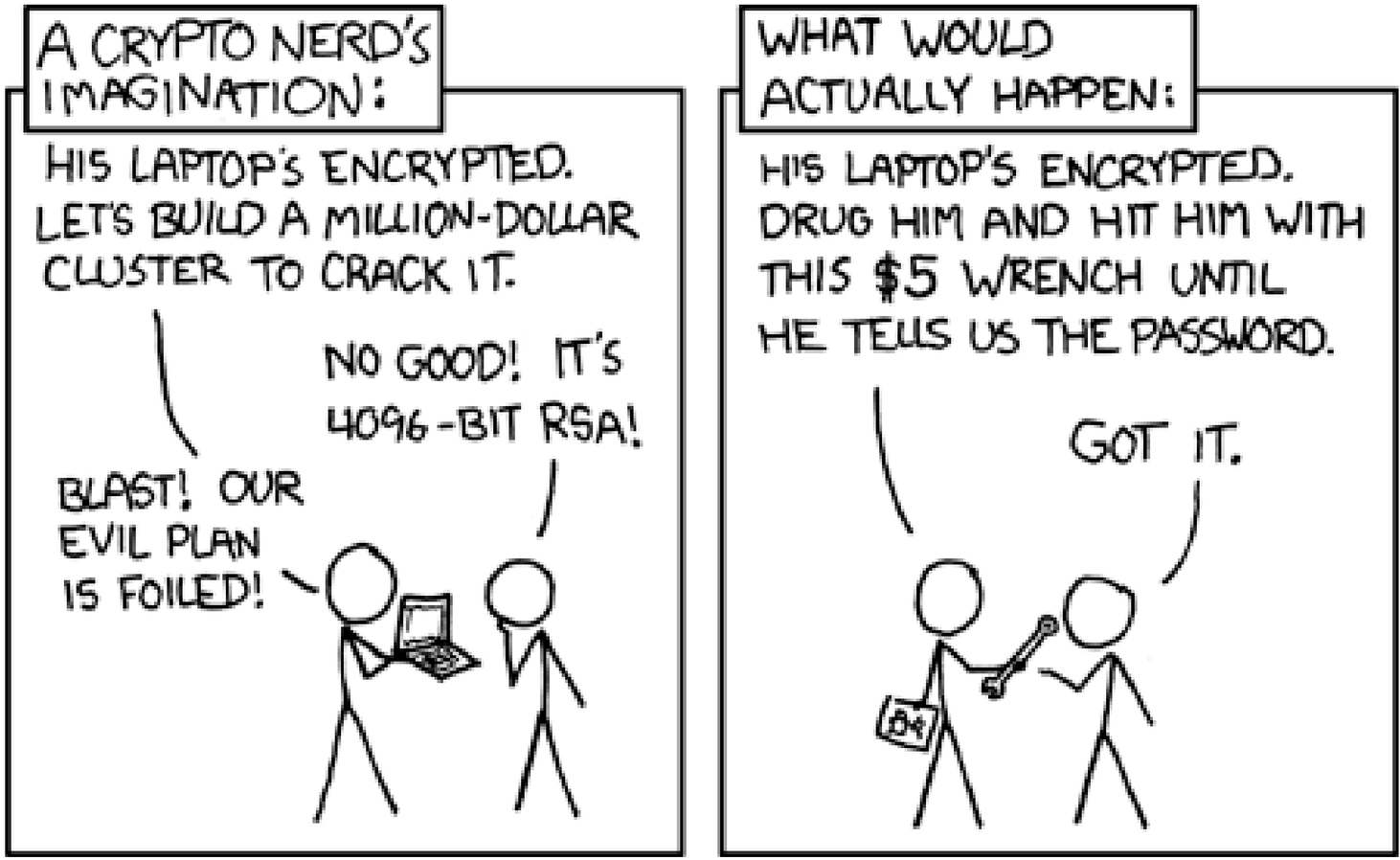
- Municipalities made a legal evaluation of IRMA
  - No obstacles for IRMA use with regard to GDPR
  - IRMA complies with legal requirements regarding electronic identification (eIDAS, proposed WDO)
  - Home office (BZK) has not put forward any obstacles to the further development and implementation of IRMA

Current developments (work in progress)

- Revocation of attributes
- Authenticated phonecalls
- Remote vetting for 2FA
- Interface redesign

IRMA On the horizon

- Raising confidence levels and acceptance
- Attribute based encryption/signing
- Source validation of news
- Pseudonomous job application
- Beyond borders….
- ……



More information & demo's : https://www.privacybydesign.foundation