










decode



**Deployments of pilots in
Amsterdam**



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 732546



Project no. 732546

DECODE

DEcentralised Citizens Owned Data Ecosystem

D5.5 Deployment of Pilots in Amsterdam

Version Number: V1.0

Lead beneficiary: Waag

Due Date: March 31, 2019

Author(s): Max Kortlander, Job Spierings, Tom Demeyer (Waag)

Editors and reviewers: Javier Rodriguez (IMI), Jaromil Roio, Andrea D'Intino(DYNE), Safia Akkus (AMS)

Dissemination level:		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Approved by: Francesca Bria (Chief Technology and Digital Innovation Officer, Barcelona City Hall)
Date: 31/03/2019

This report is currently awaiting approval from the EC and cannot be not considered to be a final version.

Table of Contents

Figures and Tables	3
Abbreviations	4
1. Introduction	5
2. Pilot 1: Gebiedonline	7
2.1 Technical description and results	8
2.1.1 Example Technical Journey	10
2.2 Educational Description and Results	12
2.2.1 Educational Description	12
2.2.2 Educational Results:	12
2.3 Pilot Roadmap	19
3. Pilot 2: Claim verification (18+)	20
3.1 Technical description and results	20
3.1.1 Approach	20
3.1.2 Goals of the pilot	21
3.1.3 Advantages observed	21
3.2 Current status and description of pilot	22
3.2.1 Onboarding Process	23
3.2.2 Attribute Based Disclosure	27
3.3 Results and User Engagement	32
3.4 Pilot Roadmap	34
4. Conclusions and Further Ways to Apply the Technology	35
Appendix 1: DECODE criteria for selection, principles, and architectural themes as described in D1.1	36

Figures and Tables

Figure 1: The Gebiedonline pilot consists of technical implementations to the Gebiedonline (GO) platform and educational outreach through the Digital Identity Lab. The Claim Verification (18+) pilot consists of a physical passport box and a mobile web app. 6

Figure 2: GO, Irma App, and Irma API interaction schema 10

Figure 3: An excerpt from *Digital Identity: A New Balance* 13

Figure 4: *You, Online* 14

Figure 5: Screenshot from the *Digital Identity Video Series* 14

Figure 6: Screenshot from the 'articles' page on the policylab.waag.org website, with previews of two articles seen here. 15

Figure 7: A screenshot from the toolbox at <https://policylab.waag.org/tools/>, with links and descriptions for three resources shown here. 16

Figure 8: Gebiedonline development kickoff 17

Figure 9: 'Wegingskader' presented by City of Amsterdam. 18

Figure 10: This screen will appear upon visiting decode.amsterdam 23

Figure 11: The passport box is a physical unit, pictured here. 24

Figure 12: A physical passport is placed into the Passport Box to be scanned. 25

Figure 13: A phone scans a DECODE onboarding code from the Passport Box. 26

Figure 14: Passport data, including the passport image, date of birth, nationality, and full name are loaded onto a user's phone at the end of the onboarding procedure. 27

Figure 15: The person requesting information from another party must first define their own identity as well as the question being posed. 28

Figure 16: The question posed by Safia has been translated into a QR code, which can now be read by another device. 29

Figure 17: Here, Stan can choose whether or not to share with Safia if he qualifies as 'Over 18'. 30

Figure 18 : The final step in attribute based disclosure is seen here, with confirmation that Stan is above 18.	31
Figure 19 : The Passport Box during a demo at the 'State of the Internet' event	32
Figure 20 : Roadmap: Digital Identity and Services 2019 - 2020 - 20xx.	33
Table 1 : Gebied online Pilot Events	17

Abbreviations

AMS	Amsterdam CITY COUNCIL
ABC	Attribute Based Credentials
IoT	Internet of Things
IRMA	I Reveal My Attributes (App for ABC by RU)
MVP	Minimum Viable Product
TW	ThoughtWorks
TH	Thingful
WP	Work Package
WS	Waag
RU	Radboud University
PET	Privacy Enhancing Technologies
BCNNow	Barcelona Now (tool described in detail in deliverable D5.3)
SCK	Smart Citizen Kit

1. Introduction

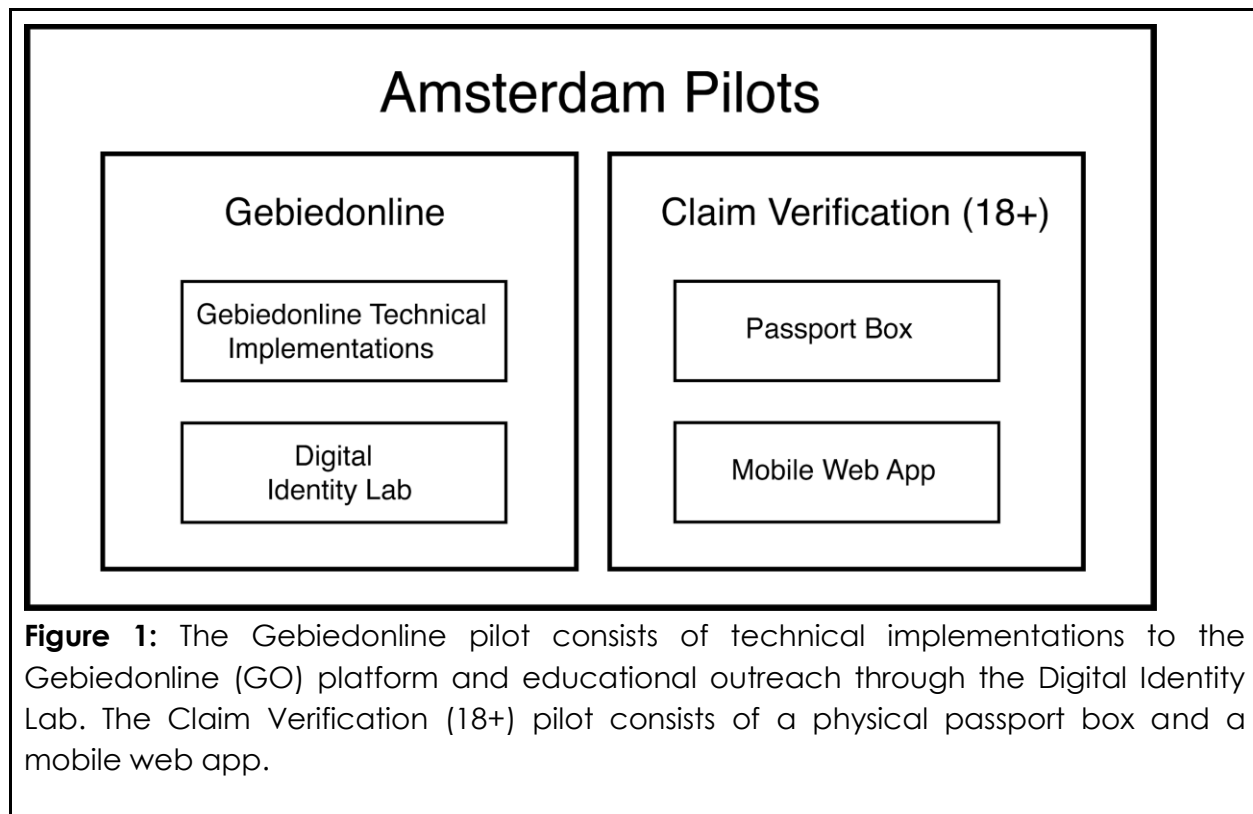
This report describes the work undertaken in the DECODE pilots in Amsterdam through January, 2019.

The DECODE pilots are usable systems that promote the project's core values. The Amsterdam pilots take an **educational approach** towards citizens and public administrations, which is guided by the following:¹

- Pilot partners aim to **build technical solutions that demonstrate opportunities** and possibilities in the realm of digital identity.
- The solutions should be **useable by the general public** and **provide a clear path forward for further development**.
- Amsterdam pilot partners utilize this technology as a framework to **educate people about DECODE values** such as privacy by design, attribute-based credentials, digital identity, data ownership, and data commons.
- Finally, the direct, applied, real-world effects of these pilots should clearly **demonstrate the benefits of DECODE** values to users.

This has led to two (2) current pilots in Amsterdam: Gebiedonline and Claim Verification (18+). Both focus on implementation of Attribute-Based Credentials.

¹ These goals have developed from the DECODE criteria for selection, principles, and architectural themes described in D1.1. A summary of these can be found in Appendix 1.



DECODE is an inherently complex and ambitious project, which set out to invent, define, design and develop a full public stack solution, with communities and 14 partners all over Europe. This document discusses only those concepts that have been piloted in Amsterdam after having been identified as technically feasible and strongly committed to DECODE's ideals.

Amsterdam pilot partners are proud of the results their communities have achieved: in the Amsterdam pilots alone, technically viable proofs of concept have been developed, awareness has been raised on strategic levels of society, and a number of Dutch public administrations (including Amsterdam, Haarlem, Leiden, Almere, and Utrecht) have begun to take concrete steps towards implementing DECODE values into their data use.

Decode, personal data and digital identity

Generally, Decode has preferred to use "sharing personal data" over terms that include the sociologically complex term 'identity'. To be able to 'identify' oneself is only one possible use-case. However, within the public debate and communities in which the Amsterdam pilot partners are aiming for impact, the term digital identity is the defining concept and buzzword. To match with the narrative of this community, it has been helpful to adopt the term.

2. Pilot 1: Gebiedonline

Gebiedonline is a pre-existing digital platform that enables local people, groups and organisations to view events taking place in their neighbourhood, share news, exchange and borrow products and services, and meet people. It is a community owned and operated member-based cooperative. The Gebiedonline board and community have a clear view: they want their platform to be open source, inclusive and to **enable their users to have granular control over the data they share** with the platform and with other users in the community. Gebiedonline has been a partner in this pilot since having taken part in an open challenge organized by Waag in Spring 2017, which challenged communities to take part in DECODE.

Gebiedonline has strongly and successfully implemented the concept of a community-managed social network. It thus represents DECODE many criteria for pilot selection (giving people ownership of their personal data, decentralized IoT access, data shared for the public good). However, as noted in D1.1, Gebiedonline is still “missing features on security and is not sufficiently privacy aware.” (D1.1 p. 61). As such, the platform provides a great opportunity for a use case that **technically implements security and verification improvements**.

To these ends², **the pilot proposes to build and pilot a set of features to use and access the platform using Attribute Based Credentials**. With Gebiedonline, the Amsterdam pilot is developing two main **technical** use cases utilizing the IRMA platform:

1. **Integrating the IRMA API into an existing GO neighborhood/network**. This would allow members of a (to-be-selected) neighborhood/network to share personal attributes with others in their community without sharing non-essential personal data. For example, a user could prove his or her place of residency based on census records, without ever having to share their address with Gebiedonline.
2. **Logging in to GO with IRMA**, which provides a more secure login than is currently available on the site.

Discussing specific options for further and future use cases. Integration of the IRMA API paves the way for peer-to-peer (P2P) identification, which would allow, for example, two verified community members to approve that a third person does indeed live in their neighborhood.

During initial development for this pilot, it became clear that there was an additional value in the educational aspects of this process—discussing attribute-based credentials

² Specifically, ‘enabling their users to have granular control over the data they share’ and ‘technically implementing security and verification improvements’.

with people and exploring its potential applications and implications. Doing so with tangible examples on hand provided pilot partners with a unique and highly practical lens through which to approach concepts such as digital identity, data ownership and how these are examples of the way in which technology embeds or obstructs shared ethics and public values .

As such, the Gebiedonline technical use cases have provided the basis for further **educational outreach about digital identity** in this pilot, of which citizens and public administrations are target groups. In particular, this outreach aims to inform people about ethical and technical issues and risks regarding attributes, identification data ownership and management, as well as to provide opportunities to address these issues through the uptake of technology. During dedicated events, pilot partners, citizens, and local public administrators co-created concepts of digital identity together; this went beyond collecting input, and allowed those present to create a broad perspective on the topic. This conversation has proven to be especially fruitful when, using decode principles, architecture and technology, specific actionable alternatives can be offered to the audience. This task has been carried out through various publications, events, and consultations which are described further in section [2.2 Educational Description and Results](#).

2.1 Technical description and results

A multi-step approach to integrating ABC features on GO has been developed by Waag. The proposed implementations focus on privacy and added benefits for users. These implementations expand on functionality one step at a time. They utilize IRMA, a community tested identity platform that provides the technology to support sovereignty in personal data management.

All of the steps in this approach have already been verified as technically possible by both Waag and the Gebiedonline development team. Following the writing of this document, pilot partners will present their proposal to undertake this approach with one of the Gebiedonline networks. Following the assessment and the identification of an appropriate subnetwork/neighborhood with which to partner, some or all of the following technical steps may be realized:

- **Technical Step 1: Integrate IRMA API³** into a Gebiedonline network.
 - This **requires** integration of the IRMA API into an existing GO network.

³ <https://privacybydesign.foundation/irma-explanation/#topic> contains further information about IRMA and the IRMA API.

- It would **allow** users to provide attribute based credentials on the site. For example, someone could verify that they live in a particular neighborhood without sharing their address; this would allow for discussions or votes to be restricted to actual residents.
- This step would **add** a level of verification not currently available on the site. It does so in a way that minimizes the personal information that users are sharing.
- **Technically**, this will provide a proof of concept in which attribute based credentials are taken up in an existing system (in this case, a cooperative social network). Implementation and use of this step will also help to **educate** citizens, community leaders and public administrators (neighborhood level) about ABC, and to **demonstrate** ABC's benefits and feasibility to the tech community. This step will also provide qualitative, sociological insight into the user experience — what people find useful, valuable, difficult, etc. about integrating IRMA into their Gebiedonline use.
- Integration of the IRMA API would provide the first step in a potential **path of migration** towards the uptake of further use cases including but not limited to:
 - Peer-to-peer identification on the GO platform: For example if two people are both verified members of a neighborhood, they could 'vouch' for their neighbor, verifying that he or she also lives in the neighborhood. In this case, the neighbors themselves (instead of a city registry) are the trusted party with the power to issue credentials.
 - Login with IRMA which provides a more secure login than is currently available on the site.
 - Using Different Attributes in different neighborhoods. For example, a user could have separate profiles for the neighborhoods that he or she works in, with each profile containing separate information.
- **Technical Step 2: Issue a Gebiedonline-credential via IRMA.**
 - This **requires** defining attributes of one or more credentials and list these in with the IRMA-scheme manager.
 - It would **allow** GO users to re-use, anonymously and securely, any information from the GO platform in another context. For example, to proof membership of a specific community without sharing any personal details.

- This step would **add** a level of personal data sharing not currently available on the site. It does so in a way that minimizes the personal information that users are sharing.
- **Technically**, GO can issue attribute based credentials to their users. It would empower them to be part of a web of trust to their community.

2.1.1 Example Technical Journey

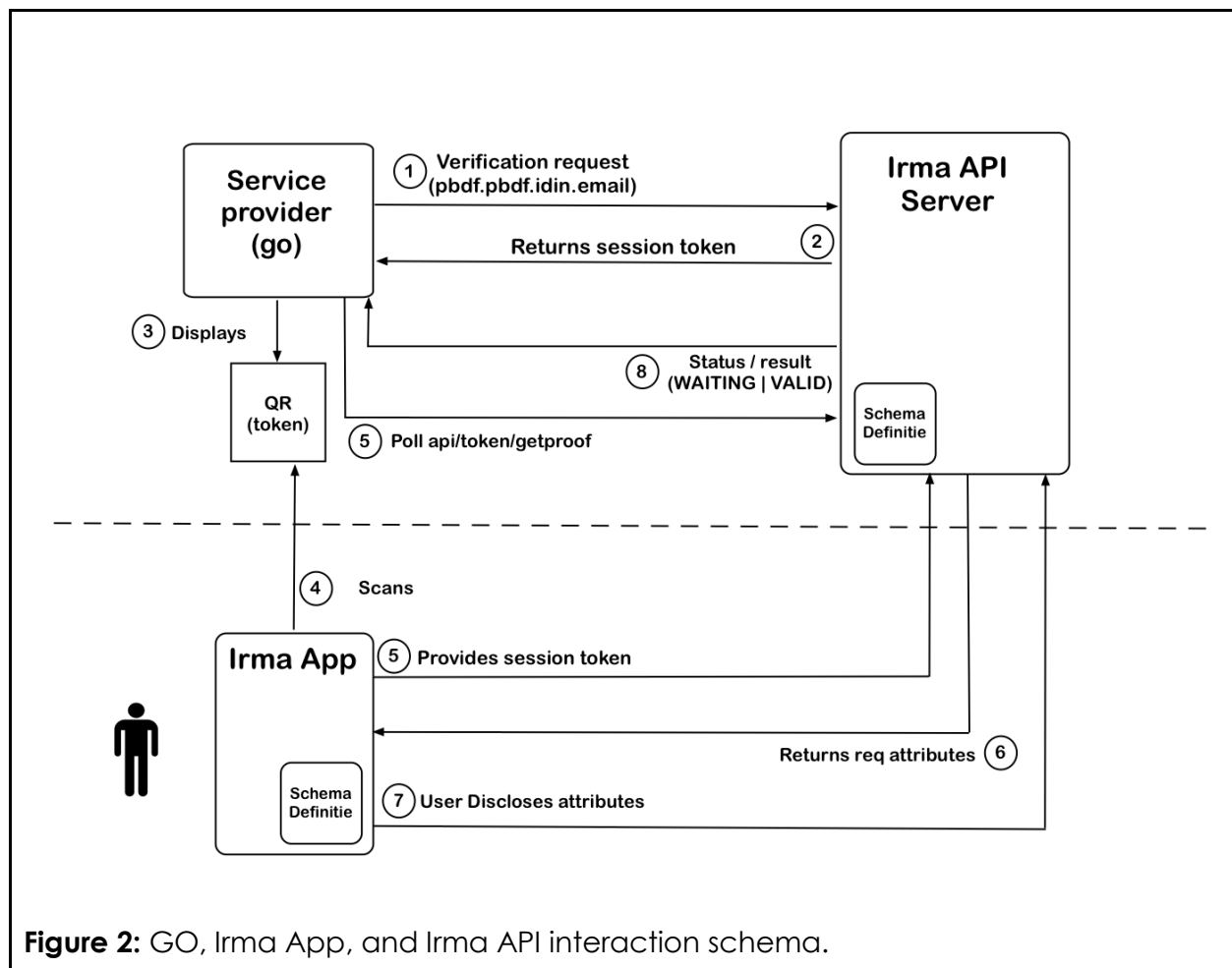


Figure 2: GO, Irma App, and Irma API interaction schema.

Figure 2 (above) depicts a single user journey whereby a new user wants to use an email address to register an account on Gebiedonline. Rather than develop their own system for verifying email addresses, GO can allow users to provide a verified email address through the IRMA app. (Note that while this specific example uses 'verified email', the process described below would be the same for using any IRMA-verified attribute on the GO website.)

This journey may occur after 1) GO has implemented their own IRMA API server and 2) the user has a verified (email address) attribute on the IRMA app on their mobile device, which they have already downloaded.

It is also important to note that Gebiedonline as a service provider only needs to account for those steps which take place above the dotted line.

The steps can be briefly described as follows:

1. GO tells the IRMA API that a question is being asked (in this case, there is an email verification request).
2. The IRMA API sends a QR code back to GO, which is needed to answer this question.
3. That QR code is displayed on the IRMA website.
4. The user opens the IRMA app on his or her phone and scans the QR code. This QR code contains the information that the IRMA app needs to communicate with the IRMA API server, as well as a special ID to mark this particular session.
5. (above the dotted line) The GO website essentially asks the IRMA API: 'Do we have validation yet?' If the IRMA API responds 'No', the GO website will continue to ask, 'How about now?' This continues until step 7 below. Meanwhile...

(below the dotted line) The IRMA app presents the token to the API server, specifying the particular request.

6. The IRMA API returns the request for attributes to the IRMA app. Essentially, the API asks the app: 'GO is requesting [in this case] your email address — do you want to share it?'
7. Confirmation or rejection is sent from the IRMA app to the API server ('yes I want to share this information' or 'no I do not want to share this information'). The actual e-mail address is transferred from the app to the server.
8. IRMA says to GO 'this is a valid email address' and provides GO with the user's verified email address.

2.2 Educational Description and Results

2.2.1 Educational Description

Many of the lessons learned through our development and discussions of the technical aspect of the pilot have expanded into an educational strategy which is focused on strategic and sustainable adoption of the DECODE technology, vision and concepts.

The strategy is aimed at three target groups: policy makers, developers, and citizens/city makers. These communities correspond with three impact levels: strategic, technical and practical.

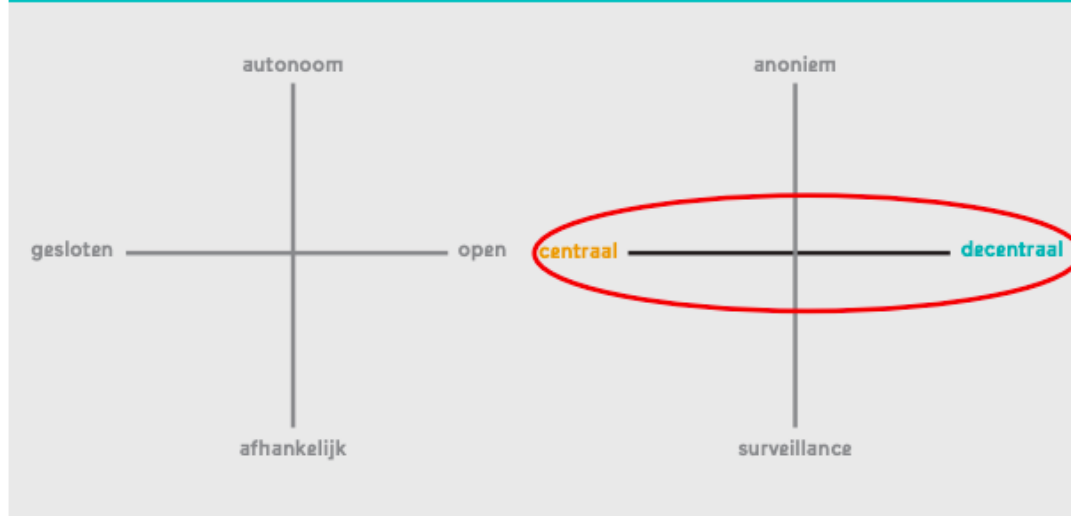
1. Policy makers: we see that important decisions on how we organize our online identity are taken by policy makers. Therefore, they are an important strategic target group for the DECODE project.
2. Developers: to be able to have larger adaptation in civic tech, social enterprises and other organizations aware of the DECODE agenda and concerns, developers need to have
3. Citizens: public awareness on the need for more online data sovereignty and control has taken a massive flight the past two years. Presenting alternatives that actually technically solve this need is a great way of presenting the DECODE (and alike) solutions.

2.2.2 Educational Results:

The 'Digital Identity Lab' was created to house the various educational outputs stemming from Waag's efforts to educate citizens and policymakers about digital identity in DECODE. Written and visual materials that have been created in the lab can be found online at <https://digitaleidentiteit.waag.org/>. An English version of the site, containing many of the resources which are relevant for an international audiences, can be found at <https://policylab.waag.org/>. Specific materials on the site include:

- **Wegingskader (Policy Framework) – Digital Identity: A New Balance** (Dutch: <https://digitaleidentiteit.waag.org/artikel/wegingskader/>): This document covers values, norms and technology for digital identity. It serves as a policy framework for Dutch public administrations, organizations, and companies that want to deepen their understanding of new forms of digital identity and personal data sharing.

3. Spreid verantwoordelijkheid & risico



Centraal

- Eén dienst voor alle gevallen
- Data Lake
- 'ID-provider' is essentiële stap
- Broker/centrale hub

Decentraal

- Meerdere aanbieders
- Federatieve opzet
- Gebruiker is essentiële stap
- Gescheiden verstrekken en gebruiken
- Data verspreid / bij bron

Figure 3: An excerpt from *Digital Identity: A New Balance*. This figure is entitled 'Spread responsibility and risk' and provides an overview of the differences between a centralised and a decentralised database.

Central: One service for all cases; Data lake; ID provider is essential step; broker/central hub.

Decentral: Multiple providers; federative design; user is essential step; separate distribution and use; data distributed / at source

- **You, Online** (Dutch [<https://digitaleidentiteit.waag.org/jij-online/>] and English [<https://policylab.waag.org/you-online/>]) is an interactive article which uses input provided by the reader to 'explore identity in the digital age'. The article draws from videos, case studies, analogies, and thought experiments to introduce readers to the topic. It is written in a fun, playful style and was designed to be accessible to a wide audience.

Yo, let us know the following and you can continue!

My local mall/market is called...

Sometimes, I go there to buy a(n)...

Send it, I guess.

Figure 4: *You, Online* requests information from the user, which reappears in the article's text to demonstrate a lesson on digital identity. (None of the information collected is stored in any way).

- Digital Identity Video Series** (Dutch subtitles English subtitles) (<https://digitaleidentiteit.waag.org/artikel/video-serie/>; <https://policylab.waag.org/article/video-series/>) - Waag interviewed local citizens about their thoughts on identity in the digital age. The citizens share their opinions and experiences with online banking, social media, interacting with the government online, and more. This video series is integrated into the aforementioned article *You, Online*.



- A **series of articles and blogs** (Dutch [https://digitaleidentiteit.waag.org/artikelen/]; English [https://policylab.waag.org/articles/]) address a variety of topics related to digital identity: how to understand the topic, which tools and resources can help to manage digital identity, explorations into the effects of our digital identities on ourselves and our families, and more.

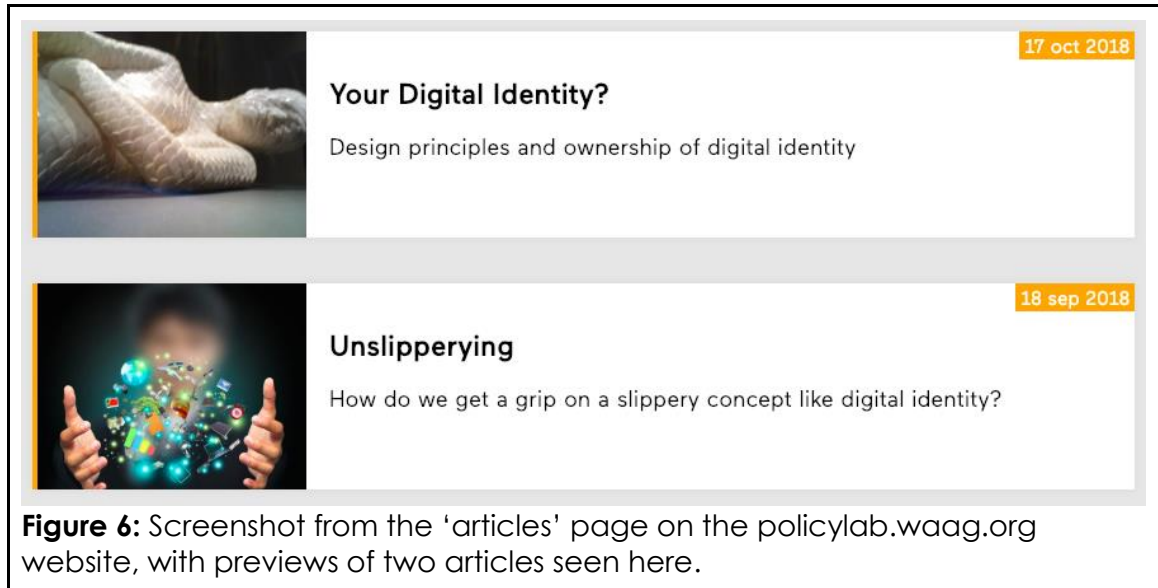
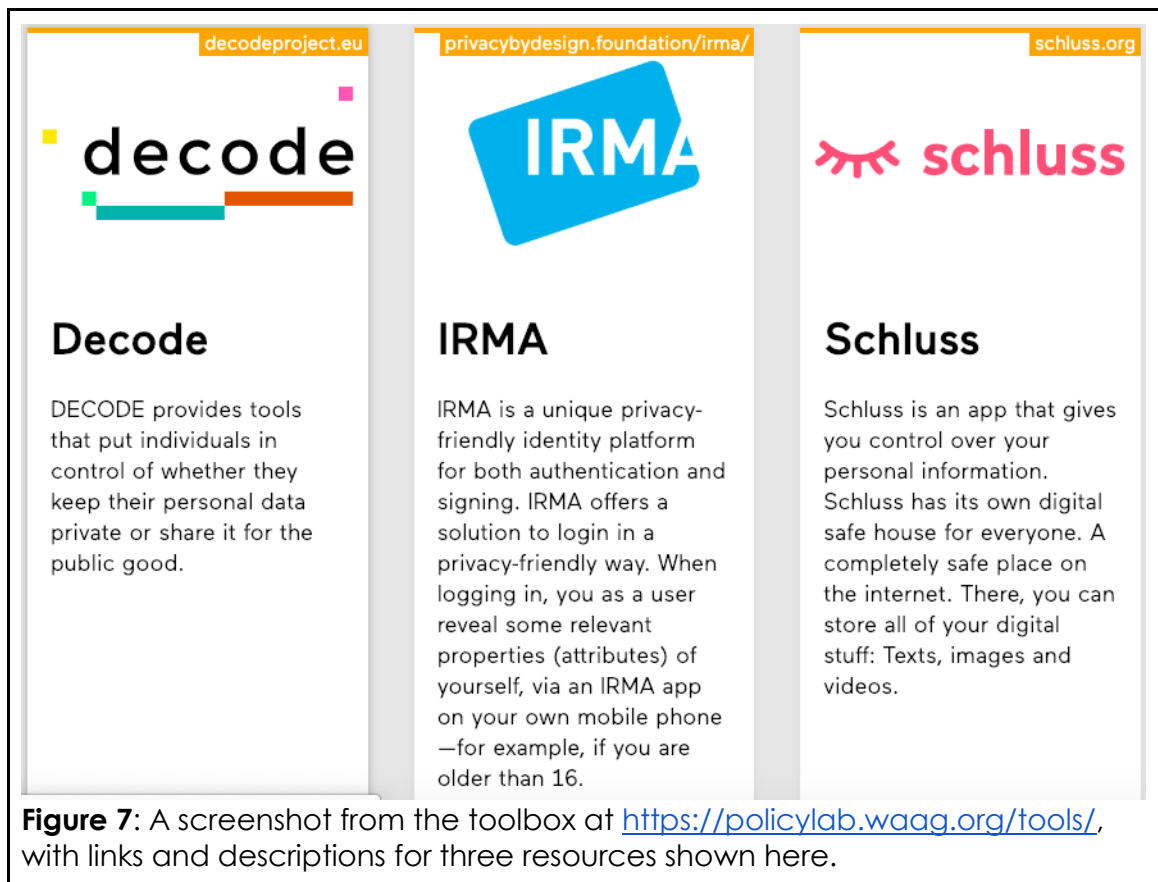


Figure 6: Screenshot from the 'articles' page on the policylab.waag.org website, with previews of two articles seen here.

- A **toolbox** with links and descriptions of various tools, initiatives, and organizations related to digital identity, ABC, data ownership, personal data management, and online privacy. This includes project and project partner pages (such as DECODE and IRMA) as well as links to other resources from outside of the project.



In addition to the efforts described above which are able to be housed online, some of the Digital Identity Lab's work has taken place through meetings and workshops, which are described in **Table 1** below. This includes:

- A series of consultations with public administrations, at multiple levels, within the Netherlands.
- A series of educational and awareness-raising workshops with citizens, public administrations, and tech professionals.

The following **meetings and events** took place to develop, test, and educate about digital identity, the Gebiedonline pilot and its implications:

July 2018: development kick-off Gebiedonline pilot: User Journeys, architecture, interaction schemas (TW, AMS, Waag and Crossmarx).



Figure 8: Gebiedonline Development Kickoff

September 2018: (retirement active TW development) research, dev. environment, localhost testing of IRMA as an open source tool for ABC (by Radboud Un. <https://privacybydesign.foundation/irma-en/>).

Oct. – Dec. 2018: Policy Lab Digital Identity: three pilots with ABC with Dutch Municipalities:

- * eDemocracy (Groningen, Emmen, Almelo) (October)
- * Mortgage application (Utrecht, Eindhoven) (November)
- * Driving Licence as an attribute (Haarlem, Leiden, Bloemendaal) (November)

The digital identity lab has provided an opportunity to share best practices in data ownership and digital privacy with citizens, developers, and public administrations.

February 2019: Presentation: ABC as state of the art tech for sharing personal data. Introduction to IRMA implementation at Crossmarx. Mapping Gebiedonline architecture with IRMA infrastructure.

Series of Meetups

- Designing Personal Data Ownership (27-9-2018) <https://waag.org/nl/event/designing-personal-data-ownership>
- Digital Identity Lab Meetup (8-11 -2018) <https://waag.org/nl/event/meetup-digitale-identiteitslab-logius>
- DSI Talks: Data from the people, for the people (8-11-18) <https://waag.org/nl/event/dsi-talks-data-people-people>
- Principles in Technology (13-10-18) <https://digitaleidentiteit.waag.org/event/principes-in-technologie-hoe-maak-je-ze-concreet/>

Table 1: Gebied online Pilot Events

In addition to the aforementioned actions carried out under the Digital Identity Lab, the outreach undertaken in this pilot has also led to concrete actions by the following partners:

- Based on outcomes of these sprints, the development team of IRMA has bumped up/added two features to their roadmap:
 - Include pass photo as an attribute
 - Develop a 'column', which allows the transfer of credentials from a passport/id-card/driving license to an IRMA attribute. Transfer can happen with both NFC and QR-codes (to include all mobile devices) and allows for higher levels of security in the eIDAS regulation.
 - In 2019 this will lead to the possibility of using non-identifying credentials
- At least three additional cities are actively piloting or even implementing open source ABC: Haarlem, Leiden, Almere.
- The use case "p2p verification" from the GO community has led to this feature being on the research backlog of the Coconut protocol, researching how to implement cryptographic peer-to-peer verification.



Figure 9: 'Wegingskader' presented by City of Amsterdam. Multiple Dutch municipalities, including the capital of Amsterdam, are adopting lessons from the Digital Identity Lab. (Translation): **what is wrong?**: unsafe (fraud), uncertainty among users, black box technology, centralization and surveillance, market power of technology giants, data central business models, administrative and legal vacuum; **what is needed:** values (Tada), autonomy, self-government, privacy by design, integrity about data use, decentralization, direction, concrete steps.

2.3 Pilot Roadmap

The following plan of action will guide the technical implementation of the GO pilot over the coming months. This is a tentative plan of action: Each step's execution is dependent on the successful completion of the step which comes before (for example, implementation and beta testing may not begin until/unless community onboarding has successfully taken place).

March 2019: Community onboarding

- During March, we plan to agree with GO on a specific community engagement, development, and monitoring roadmap. This includes finding a network/neighborhood on GO to work with, getting their agreement on which steps to develop and when, and agree upon a method to monitor and evaluate the use and implementation of those steps.

April 2019: Implementation and beta testing

- In this stage, the technical implementation will take place and be tested amongst the team and a group of beta test users.

May 2019: Community pilot

- The new features will be used on the GO platform by members of the neighborhood network. Pilot partners will monitor the uptake of these additional features to receive both qualitative and quantitative feedback.

June 2019: Present results

- Results and lessons learned from the first community pilot will be analysed, documented, and shared.

3. Pilot 2: Claim verification (18+)

Digital identity is a sprawling, abstract subject that can be made more tangible. Rather than focus on complex organizational problems, pilot partners wanted to make a manageable user experience case study on how digital identity could look in a concrete form. More specifically, with this pilot, partners wanted:

- to develop something of use to the citizens of Amsterdam;
- a clear user experience, a full understanding of the entire customer journey from A to B;
- to give citizens access to their personal data as stored in the municipal database, and allow them to share these data in a different context, on- or offline;
- a pilot that could be approached iteratively, where initial steps could both have a clear impact and also leave room for further development and applications;
- to demonstrate that these aims are possible and can happen, to inspire further trust and belief in this approach towards citizen identity.

With the Passport Box, pilot participants will be able to prove that they are over a certain age⁴ (for example, over 18)—without having to share their full identity, date of birth, or social security number—through the use of attribute based credentials. The pilot is hands-on research towards answering practical questions like ‘how would this actually work?’; ‘what user interaction is needed?’; and ‘do citizens find this useful?’

3.1 Technical description and results

3.1.1 Approach

A modular approach to implement the core features of DECODE's software stack has been developed by Dyne with particular emphasis on data encryption. It is based on the Zenroom VM which also features

- advanced zero knowledge proof functionalities (Coconut crypto scheme)
- natural language execution for cryptographic transformations
- data manipulation (Zencode interpreted since version 0.8.1)
- modular bindings to Python and NodeJS

⁴ Alongside age, gender and name were also incorporated into this pilot as verifiable attributes.

The proposed implementations focus on privacy and added benefits for users, but also on developer experience to facilitate the integration in bigger applications which can be developed ad-hoc for pilots.

The main pilot implementation realized in cooperation with the UX and development team of Amsterdam municipality includes:

- Hardware and software to scan a passport's digital contents via NFC
- Zenroom integration to encrypt and manipulate the data extracted
- 3D printed prototype of casing and totem for the passport reader

3.1.2 Goals of the pilot

The pilot provides a station to verify the personal data contained inside a passport (name, nationality, birthdate, photo) so that an operator can decide to release a credential when a condition bound to such data verifies. Zenroom can then be used to provide a portable credential associated to the issuer and the specific attribute issued. The credential released can also be a zero-knowledge proof attribute whose use can be publicly verified without leaving a trace that is directly connected to the subject holding the attribute.

In practice this realised an easy to setup station to make the 18+ pilot possible: releasing proofs that people are older than 18 years old and for instance is possible for them to use the credential issued to buy alcohol at a supermarket or in a club, without having to disclose their full identity.

3.1.3 Advantages observed

The advantages observed in the realisation of the pilots can be summarised as follows, representing advancements over IRMA in this implementation:

- easy to setup station integrating with existing national passport protocol
- possible to run the credential issuance also offline
- possible to enable additional credential issuers
- verified ease of development integration and ad-hoc white-label development

In particular the last point referring to developer experience where scientists and engineers from the city have reported, it was very easy to integrate Zenroom seamlessly into the pilot application software and hardware setup, thanks to Python and Javascript bindings and the presence of a documented API and Lua programmable language. The implementation also led to improvements to Zenroom's codebase (leading to the 0.8.1 release) with some prominent bug fixes and a few features added. The experience has prompted Dyne.org developers to emphasize on the provision of Zenroom language bindings (also distributed officially via pip and npm packaging) as this seems to constitute a clear edge for DECODE technology to be easily adopted, whereas other implementations including IRMA are less modular and do not facilitate

white-label implementations. This lead also to the completion of modular components that can run natively on mobiles (iOS and Android) and work ongoing for Cortex chips, builds that are now included in a nightly snapshot release of all targets through our continuous integration infrastructure on <https://sdk.dyne.org:4443/view/zenroom/>.

The Amsterdam pilot has made a basic use of Zenroom's capability for symmetric encryption protected with a memorisable PIN using AES-GCM and PBKDF2 protections, as the implementation of the Coconut credential system was still ongoing. Completion of the Coconut credential system now offers an opportunity to revisit the pilot and provide it the same Zero Knowledge Proof and Homomorphic Encryption features later used with the DECIDIM pilot in Barcelona, at the cost of very little intervention on the software since such an upgrade would just entail the modification of Lua code embedded with Zencode (natural language). Other possible enhancements at the reach of DECODE's pilots also include the translation of Zencode to Dutch, providing a localisation that wouldn't only facilitate the developers, but especially the pilot participants in the moment in which Zencode smart-contracts can be shown to the screen.

3.2 Current status and description of pilot

Claim Verification 18+ is a prototype, consisting of a web-app available at <https://decode.amsterdam> and a passport scanner. The application utilizes the DECODE technology 'Zenroom' (<https://zenroom.dyne.org>) for encryption. The passport scanner is a physical box that can scan a passport's RFID-chip, and translate the passport's data into a QR code. Individual attributes of that data can then be verified (such as 'I live in x city, or I am above x years of age) without sharing any personal data that is not needed in a given situation.

For example, if a person wants to buy alcohol in the Netherlands, they would normally need to show an ID card which contains their name, photograph, specific address, and date of birth. With a system of attribute based credentials (such as this pilot), a person can provide the same level of proof that they 'qualify' for a particular transaction or service without sharing more information than is absolutely needed.

The Passport Box and mobile web app currently verify age, gender, and full name. It could be further developed to verify other attributes, and/or applied to different contexts. Currently, two distinct stages are supported in this pilot: onboarding and attribute based disclosure.

3.2.1 Onboarding Process

The Onboarding process takes place one time per user, and must be completed before the application can be used. It requires users to be in the presence of a physical Passport Box⁵, and is the moment in which a user's passport information is transferred onto his or her phone.

Step 1: Go to decode.amsterdam on your mobile device

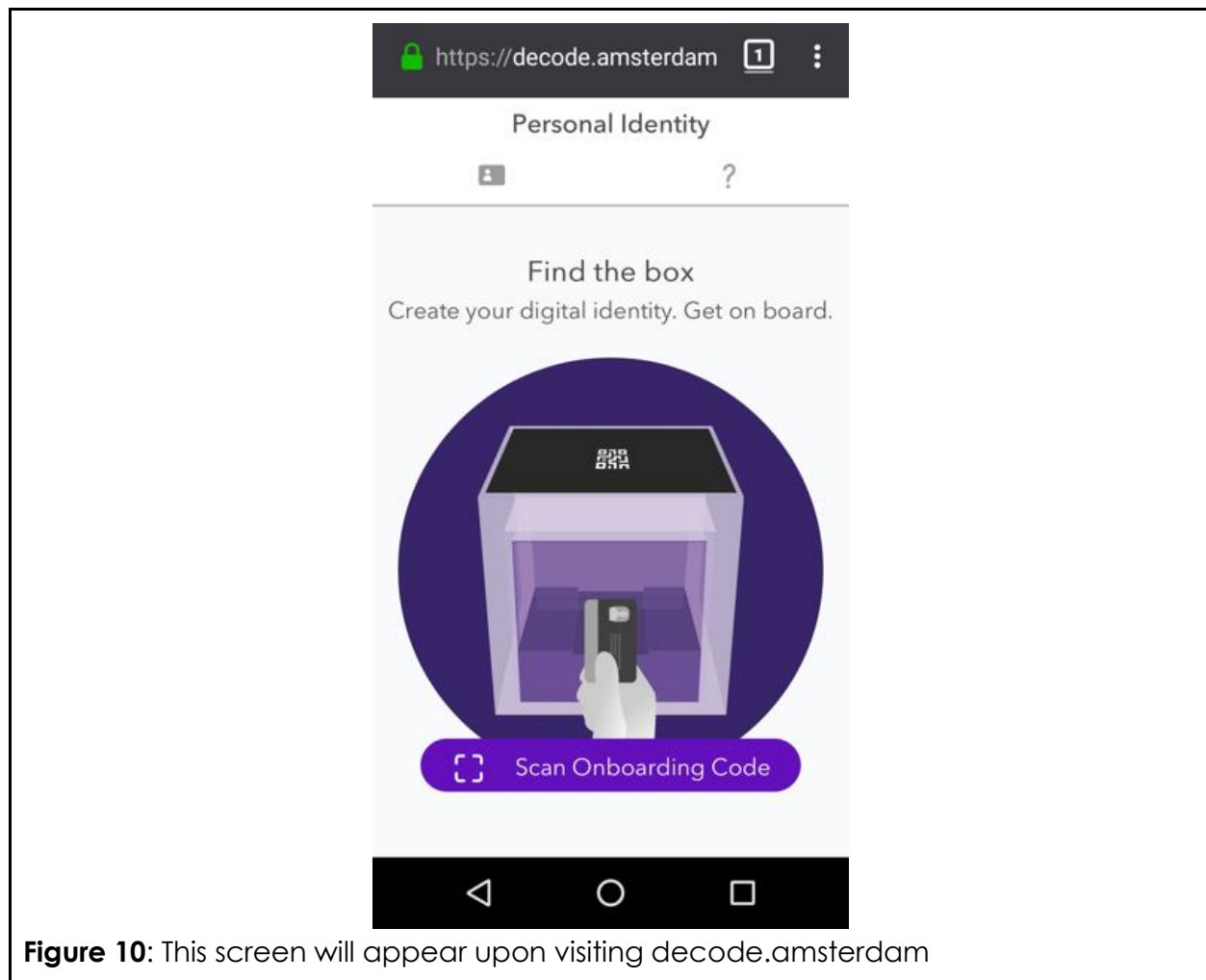


Figure 10: This screen will appear upon visiting decode.amsterdam

⁵ The current prototype is housed at the City of Amsterdam offices, and is sometimes available for use during public piloting events.

Step 2: Find the passport box



Figure 11: The passport box is a physical unit, pictured here.

Step 3: Place your passport into the box.



Figure 12: A physical passport is placed into the Passport Box to be scanned.

Step 4: The passport box will read your passport and generate a QR code.

Step 5: Scan the onboarding QR code from the passport box with your phone.



Figure 13: A phone scans a DECODE onboarding code from the Passport Box.

Step 6: You will now have a copy of the data from your passport on your phone.

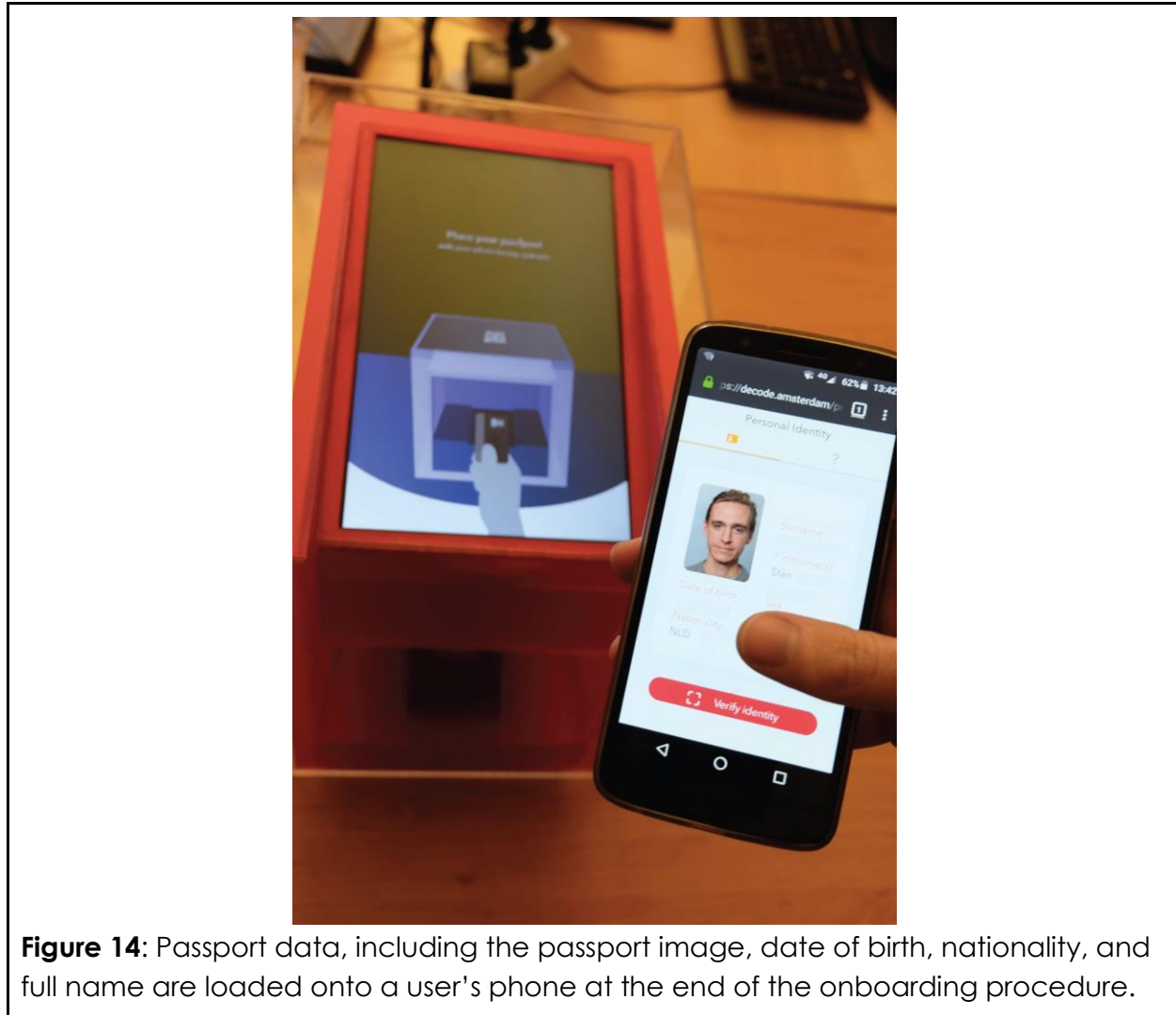


Figure 14: Passport data, including the passport image, date of birth, nationality, and full name are loaded onto a user's phone at the end of the onboarding procedure.

3.2.2 Attribute Based Disclosure

In this hypothetical scenario, Safia is a bartender who seeks verification that Stan, the patron, is over 18 years old. Stan will prove that he is over 18 years old without sharing extra data about himself, including his exact birthday.

Step 1: Safia, the bartender, first must

- define her own identity
- select which question to ask (in this case: Age)
- set the parameters for the question (in this case: Over 18?)

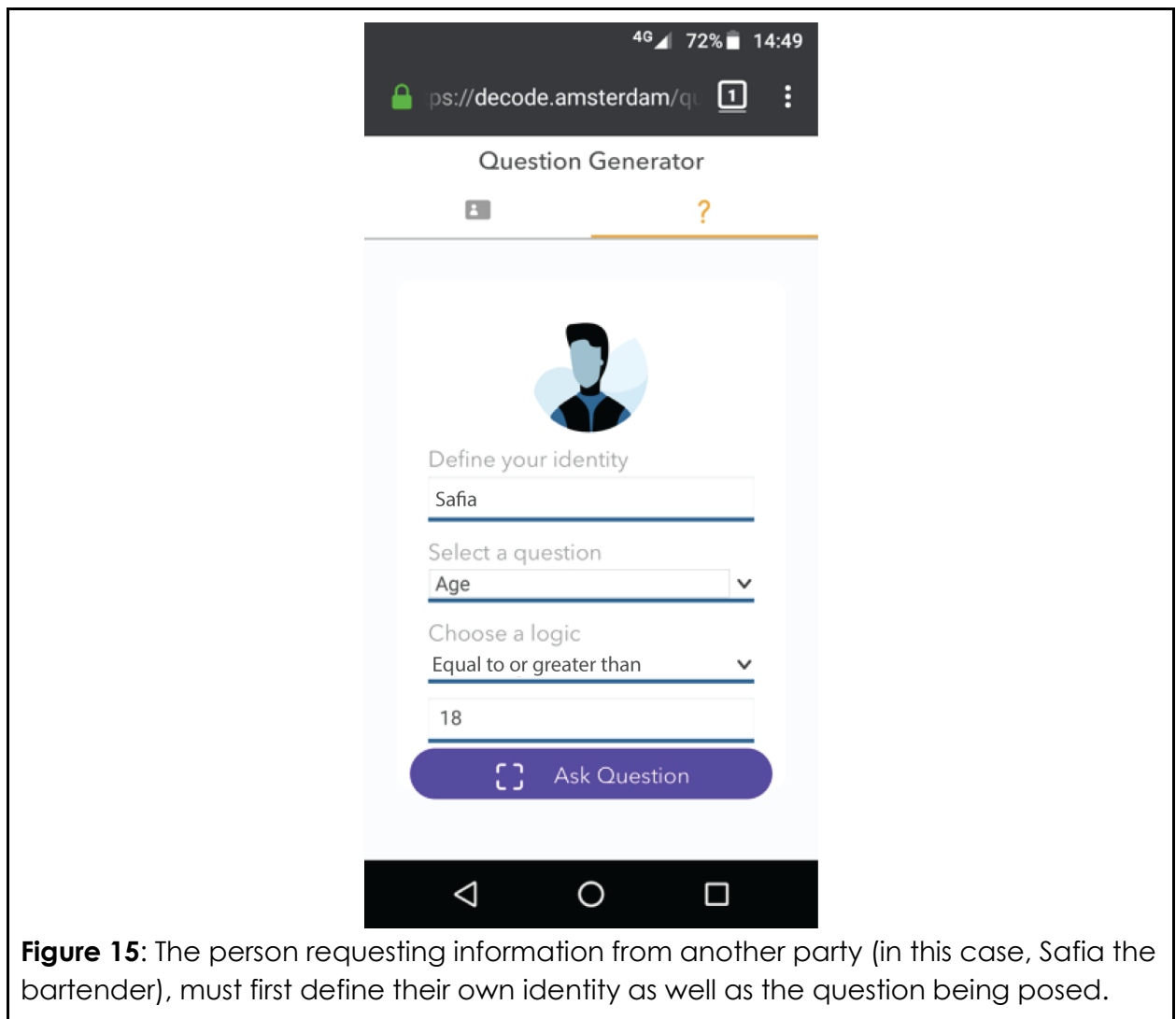


Figure 15: The person requesting information from another party (in this case, Safia the bartender), must first define their own identity as well as the question being posed.

Step 2: Once Safia has defined these terms, a QR code is generated onto her phone, which can be scanned by anybody with the DECODE app.



Figure 16: The question posed by Safia has been translated into a QR code, which can now be read by another device.

Step 3: Stan scans the QR code from Safia's phone with his own phone.

- Text appears, repeating the question ("Safia asks: Age > or = 18?")
- Stan can choose to confirm that he wants to share this information with Safia. Crucially, Stan is not choosing to share his specific age at this point. Rather, he is only choosing to share the answer to the question, yes or no, whether he is over 18.

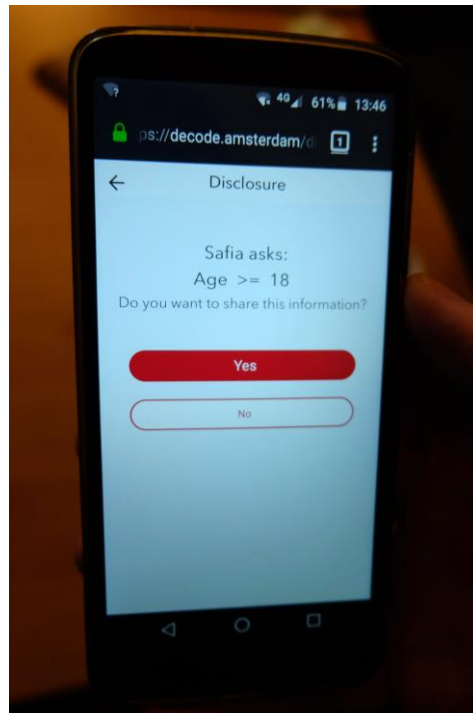


Figure 17: Here, Stan can choose whether or not to share with Safia if he qualifies as 'Over 18'.

Step 4: When Stan agrees to send this information, both he and Safia receive confirmation that he is above 18 years old. There are two features that help to prove that Stan's credential is legitimate:

- A photo of Stan appears on his phone, which he can show to Safia, in the same way that a normal ID card contains a photo to link it to its owner.
- A border appears around the check mark on Safia's phone, and also around the border of Stan's photo. In this case, both are yellow, demonstrating that their phones are both referring to the same transaction.

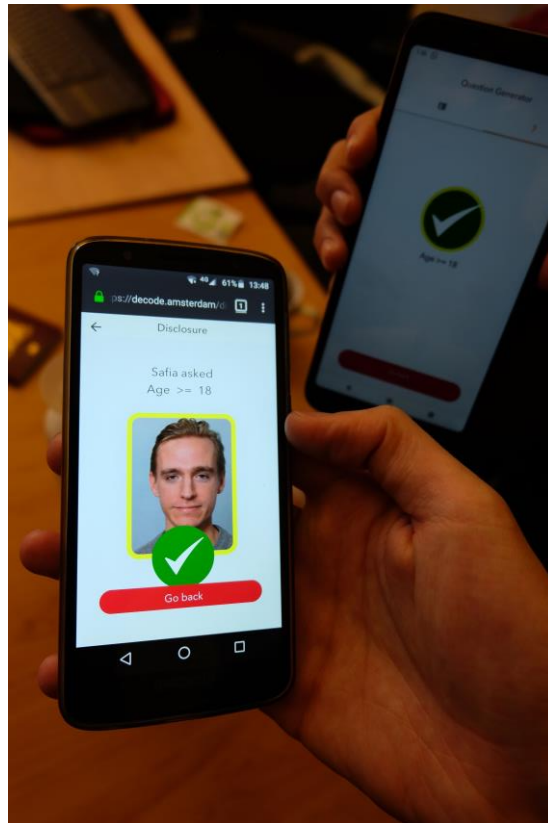


Figure 18: The final step in attribute based disclosure is seen here, with confirmation that Stan is above 18.

3.3 Results and User Engagement

The Passport Box is the main tangible output of the Claim Verification (18+) pilot. It has been publicly tested twice: A soft launch took place on 18 December, 2018 at the CTO office in Amsterdam, with local citizens and public administrations present. A second demo was held at the “State of the Internet” event at Pakhuis de Zwijger on 15 January, 2019, where the Passport Box was tested live with attendees who brought their passports. These public tests were followed by an internal day of usability tests.



Figure 19: The passport box during a demo at the 'State of the Internet' event.

Based on the results of this pilot and Waag's Policy Framework for Digital Identity, the City of Amsterdam has decided to develop an actual, operational implementation of ABC in one of the services the cities offers: A team from the city of Amsterdam has been dedicated to further explore and apply this research through an ABC-based 'Stadspas' (city pass). Additional developments may include research into a system of credentials for undocumented citizens, and exploring data minimization via ABC on the local FairBnB registry.

x
x
x **Groeipad Digitale Identiteit en diensten 2019 - 2020 - 20xx**

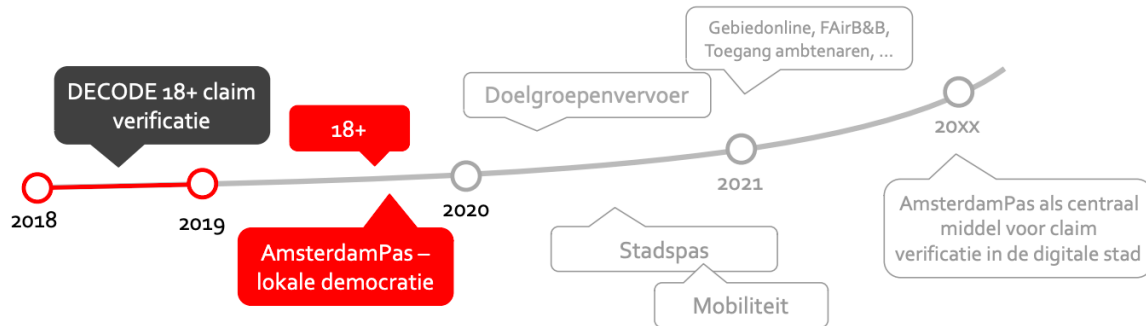


Figure 20: Roadmap: Digital Identity and Services 2019 - 2020 - 20xx. This slide, originally presented by the the City of Amsterdam, shows plans to expand on the DECODE pilot. 2018: DECODE 18+ claim verification. 2019: 18+; AmsterdamPass - Local Democracy. 2019: Transport target group; CityPass; Mobility. 2021 onward: Gebiedonline, FairB&B; AmsterdamPass as a central means for claim verification in the digital city.

During the development of the first prototype, the team at Dyne used the opportunity to perform the first test of Zenroom which led to the implementation of:

- Zencode: a natural language interpreter for smart contracts and data manipulation, as mentioned on the Decode Project's blog post (<https://decodeproject.eu/blog/smart-contracts-english-speaker>)
- Introduction of more robust ECP2 based cryptography (Elliptic Curve Arithmetics with Twisted Curve Pairings), AST (abstract syntax tree)
- “Coconut” credential-based authentication, based on the work of A. Sonnino et al. at UCL (<https://arxiv.org/pdf/1802.07344.pdf>)

3.4 Pilot Roadmap

In the coming months, pilot partners will continue to return to their choices with an increased level of seriousness, maturity, ambition, and thus scope (such as security measures). Prior to expanding to new uses or applications, functionality in this first use case must be fully developed. For these concepts to be taken up in larger use cases, they need to be working functionally, and also need to provide value to users. This is because working with sharing personal data becomes more and more sensitive as it is applied to further use cases and applications.

Pilot partners are still conducting testing and iteration on the box, and are currently seeking to expand upon and apply the technologies and lessons learned from the Passport Box. They will do so under the following general timeline:

- March/April 2019: user research, service design blueprint: Attribute Based Credentials.
- May/June 2019: presenting results
- September/October 2019: final Decode Event.

4. Conclusions and Further Ways to Apply the Technology

'Claim verification' is a central concept underlying the DECODE Amsterdam pilots; not to provide one's data or identity, but to share validated claims when they are needed. Claim verification is a means to data minimization, and data minimization is a means to privacy.

So far in the Amsterdam DECODE pilots, claim verification has been facilitated regarding proving a few attributes, such as one's age and place of residency. Potentially, this could be done with other sorts of verifiable claims, in other situations, in ways that still leave people in control of their own data.

Amsterdam pilot partners will continue to explore this subject and its potential applications alongside citizens and public administrations.

Appendix 1: DECODE criteria for selection, principles, and architectural themes as described in D1.1

Criteria for Selection: (D1.1)

1. Need for the functionality which DECODE provides is the key criterion, and specifically covers the followings aspects:
 - a. Giving people ownership of their personal data
 - b. Decentralized IoT access
 - c. Data shared for the public good
 - d. Appropriate privacy protections
2. Higher level areas are common to the pilots in both cities
 - a. Highly engaged community groups
 - b. Potential for long-term impact
 - c. Innovative idea
 - d. Ability to achieve KPIs: at least one pilot in each city to have a wide enough target audience in order to reach greater than approximately 20,000 people
3. Functionality which is specific to an individual city
 - a. Political issues (e.g. housing)
 - b. Geographical issues (e.g. noise, air pollution)
 - c. Existing city infrastructure

DECODE principles

- Gain information for decision-making by thinking in code
- Seek rapid feedback loops to validate decisions
- Build something that works, then iterate

DECODE architectural themes

- Distributed ledger
- Entitlements (policy and implementation)
- Data ontologies
- Privacy controls (cryptography)
- Smart rules
- Hardware
- DECODE OS
- User Experience
- Integration with DECODE applications
- Continuous Delivery tooling
- Testing and validation (D1.1 p. 67)