Securely derived identity credentials on smart phones via self-enrolment

Fabian van den Broek, Brinda Hampiholi and Bart Jacobs

Institute for Computing and Information Sciences,
Radboud University, Nijmegen, The Netherlands
Email: {f.vandenbroek, brinda, bart}@cs.ru.nl

Abstract. In the last decade traditional identity documents have been equipped with an embedded NFC-chip to enable wireless access to the relevant data. This applies in particular to passports, following the ICAO standard, but increasingly also to other identification documents, such as driver's licenses. Such electronic identity (eID) documents can now be used as "mother cards" by the users to remotely enrol and obtain derived credentials which can in turn be used for identification and authentication, notably on smart phones. These self-enrolment possibilities are becoming popular, because they are easier and cheaper than traditional, face-to-face enrolments.
This paper first describes a protocol for obtaining credentials on smart phones from an eID document, that has been implemented using the "IRMA" attribute-based credential technology. This basic protocol cannot exclude that someone enrols with another person's eID document. Subsequently several mechanisms are discussed for securing a proper binding between the user and the eID document used for enrolment.

1 Introduction

User authentication is a process that confirms the binding between a user and his presented identity to an authenticating entity, for instance, to a service provider. Typically, a service provider authenticates a user by verifying the presented credentials, e.g., a password or a proof of knowledge which are considered as evidences for the user's claimed identity. To ensure that the service providers are guaranteed of the credentials' authenticity during authentication, the credentials have to be issued to the user (i.e., to the user's authenticating device) in a secure manner after verifying the user's identity during an enrolment phase. Thus, secure and trustworthy enrolment plays a very important role in any authentication ecosystem.

Secure enrolment consists of verifying the real-world identity of a user (also called identity-proofing) and registering the user before issuing an identity credential. Traditionally, face-to-face enrolments are required whenever important (physical) identity documents or credentials are issued to users. For example, a passport is issued after the user has applied for it and a government authority has verified the user's identity during a face-to-face meeting at the authority's

office. Such an enrolment gives strong trust assurance to an authenticating entity about the passport holder's claimed identity and about the link between the user and the passport. However face-to-face enrolments are not user-friendly and more importantly, they are very expensive in terms of time, costs and resources. So in recent years there is a push towards remote self-enrolment of users where, of course, security requirements remain strong, but are harder to guarantee.

This paper investigates secure self-enrolment of users in which users can derive their identity credentials from their ICAO[1] standard electronic identification (eID) documents (e.g. e-passports), onto their authenticating devices. In this paper, we follow the definition of 'derived credential' found in NIST Special Publication 800-63-1 [1]:

> *"A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process".*

The trust for the new credential on an authenticating device is derived from the strong identity binding associated with the authenticated eID document during enrolment. For this paper we consider smart phones as authenticating devices, because they can directly connect with enrolment services and can contain capabilities to communicate with eID documents. This paper abstracts from the specific credentials obtained through self-enrolment and its results can be applicable to different types of credentials. However, the motivation for this topic comes from our earlier work in the field of Attribute Based Credentials (ABCs) [2] within an ongoing research project called IRMA[2](I Reveal My Attributes). ABCs have many nice properties, but for this paper it is important to know that these credentials are authentic and non-transferable. But, of course the credentials are only as trustworthy as their issuance process, which is why we are interested in secure self-enrolment.

Self-enrolment via eIDs is convenient for a user as it can be done from any location and is very inexpensive, both time- and cost-wise. It is also secure, in principle, as one builds self-enrolment on top of an earlier face-to-face enrolment that was carried out for eID issuance.

A high level picture of our approach to eID-based self-enrolment is given in Figure 1. The first three steps constitute the enrolment phase, which the user goes through only once for obtaining his credentials. The last 'showing' steps on the right suggest how the issued credentials can be used, selectively, to authenticate to multiple service providers. This paper focuses on these first three enrolment steps, and will especially elaborate the user's interaction with the Enroller and the Issuer. Details will be given in Section 3.

[1] International Civil Aviation Organization standard document 9303 (http://www.icao.int/publications/Documents/9303_p3_v2_cons_en.pdf).

[2] See https://www.irmacard.org/ for more information.

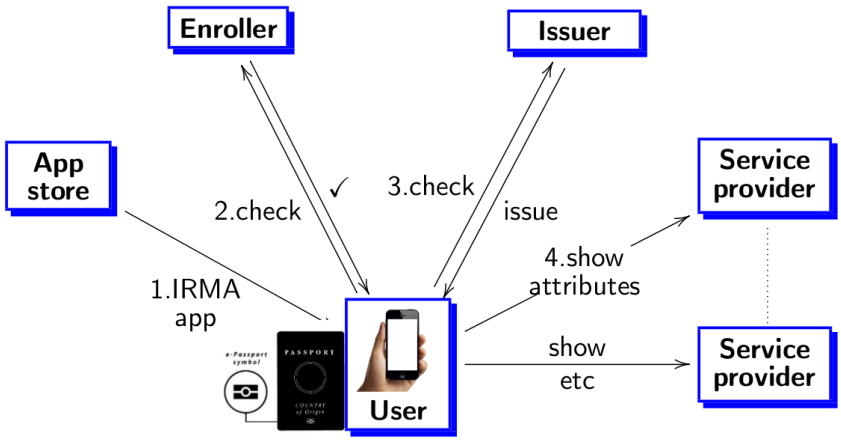

Fig. 1: Self-enrolment using a standard eID document and a smart phone with NFC capability to get derived credentials on the phone.

1.1 Our contribution

Taking our implementations of several experimental forms of self-enrolment within the IRMA context as a starting point, we explore how to guarantee a higher level of trust by combining several options that are available, in principle, to a wider audience. The conclusion that emerges is:

1. attribute-based authentication technology provides a natural setting (ecosystem) for self-enrolment, providing different attributes for different authentication scenarios;
2. several methods exist or are appearing (such as, eID documents with PIN, biometric checks, existing logins) that make trusted self-enrolment a viable new approach in identity management;
3. trusted self-enrolment requires more than a single protocol, and can be realised by combining several self-enrolment protocols, involving possibly overlapping attributes; they lead to higher levels of trust if they yield consistent outcomes; in this way the separate protocols reinforce each other.

2 Background

Attribute-based credentials (ABCs). ABCs can be considered a privacy-enhancing technology (PET). An *attribute* is a characteristic or a qualification of a person. Attributes can either be identifying (e.g,'full name', 'address') or non-identifying (e.g.,'student', 'age over 18'). Collectively, these attributes can constitute the identity of a person. An attribute-based credential is a cryptographic container of a few attributes that is signed by an authoritative party. The creation of an

attribute-based credential is called *issuing*. This is an interactive cryptographic protocol in which an issuer authority digitally signs the user's credentials with his private key. The credentials are issued in such a way that they are associated to the user's secret key that is securely stored on the user's authentication device. Thus, ABCs are authentic and non-transferable. One special thing about an ABC is that the attributes can be selectively disclosed; thus, the ABCs achieve data minimization and privacy protection via contextual authentication.

ICAO standard. The International Civil Aviation Organization (ICAO) runs a 'machine readable travel documents' programme. Its main purpose is to develop and maintain open specifications for automated access to data in passports. This includes embedded chips that can be accessed wirelessly, via Near Field Communication (NFC).

These chips contain the information that is printed on the main page of the passport, such as name, date of birth, picture, date of issuance etc., but possibly more, like fingerprints. Access to these fingerprints is restricted, but the other data can be accessed without prior authorisation. The data in the passport are digitally signed, so that their integrity can be checked. In the current context two protocols are of special importance. For more information, see [3].

- *Basic Access Control (BAC).* The user data in the embedded chip in a passport are cryptographically protected. The required cryptographic keys can be derived from the combination of: document number, date of birth, expiry number. These can be obtained by scanning the machine readable zone at the bottom of the main passport page. They can also be provided manually, like in the screenshot on the left in Figure 3. The protocol that derives the relevant keys and uses them for data transfer is called Basic Access Control (BAC). It is implemented in any device that reads e-passport (including the IRMA app).
- *Active Authentication (AA).* The data that are read via BAC includes a document-specific public key. The associated private key is securely stored inside the chip in the passport. The so-called Active Authentication protocol uses this key pair to verify the authenticity of the passport via a standard challenge-response check[3] to ensure that the passport is not a clone.

3 Basic self-enrolment with eID documents

Our self-enrolment protocol allows the user to enrol remotely (from any location) through his smart phone using his eID document to get authentic, derived credentials on his smart phone. The entities that are involved in this protocol are:

- *User* - Entity who initiates self-enrolment with his eID document and his smart phone in order to get authentic derived credentials on his phone;

[3] See also https://www.commoncriteriaportal.org/files/ppfiles/c0247_epp.pdf

– *Enroller* - Entity who verifies the user's identity (i.e. eID document), carries out enrolment for the user before the credentials can be issued to him;
– *Issuer*- Entity who issues derived credentials to the user upon getting an enrolment confirmation message from the Enroller.

Note that in specific scenarios the Enroller and Issuer can be the same entity.

In our basic self-enrolment protocol, we assume that the user's eID document has an NFC chip and that the user's smart phone supports NFC, so that the eID document can be read by/via the phone. Below we describe the protocol that summarizes the communication between the user's phone, Enroller and an Issuer during self-enrolment. See also Figure 2.

1. A user connects to the Enroller securely (e.g. via TLS) through his phone, requests for derived credentials using his eID document, enters the BAC (see Section 2) data present in the eID: document number, date of birth and document expiry date on his phone, and holds his eID document against (the NFC reader of) his phone.
2. The Enroller reads the user's eID via the user's phone's NFC interface and performs the following checks on the eID:
   – a check for data integrity: by verifying the digital signature on the (hashes of the) data groups, the Enroller verifies if the eID data are not altered;
   – a check for authenticity: using the ICAO-defined active authentication (see Section 2), the Enroller verifies if the eID is not cloned;
   – a check of the user's eID against a database of revoked (e.g. lost/stolen) eID documents. This check is possible only if the Enroller has access to such a database, which is typically maintained by public authorities.
3. If the above eID checks are successful, then the Enroller sends a digitally signed user-identity confirmation message to the Issuer. This message contains the user's eID data that the Issuer can sign and issue to the user as derived credentials.
4. The Issuer verifies the Enroller's signature on the confirmation message, connects to the user's phone and issues signed eID credentials to the user's phone — so that the phone is ready to be used as an authentication device.

The above protocol considers the user's eID document as a *mother card* from which an Issuer derives user's identity credentials and issues them securely to the user's phone. After this issuance, the user can use his phone as his authenticating device and authenticate to any entity with the issued credentials. The self-enrolment protocol, although remotely done, ensures that the user is in possession of a valid eID and that the identity credentials are derived onto his phone from that authentic source.

The above approach may give clearly separated roles between public and private parties. Public authorities are the traditional trusted root for identity information about citizens. They remain so in our basic enrolment protocol, via the eID documents that they issue. Private parties may develop smart phone apps for derived identity credentials and play the roles of Enroller and Issuer,

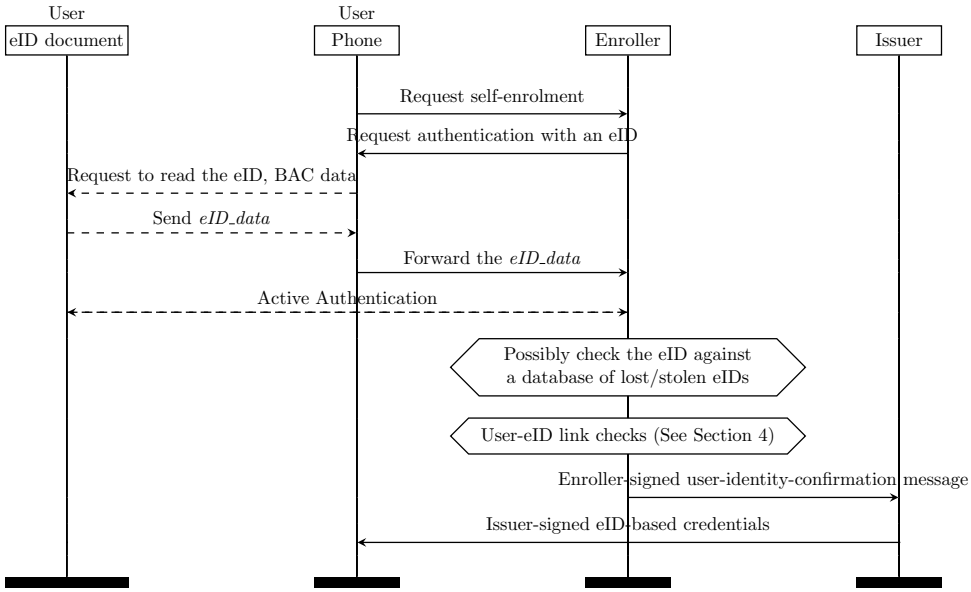

Fig. 2: Basic self-enrolment protocol using a standard eID document. The dashed arrows in the figure indicate the phone as a NFC reader and the solid arrows indicate the phone as the currently enrolling user-device (potential credential carrier).

and thus build innovative identity management systems on top of the publicly issued e-documents.

3.1 Implementation of basic self-enrolment protocol.

We have implemented the basic self-enrolment protocol in an attribute-based credential (ABC) [2] framework based on a technology called IRMA that has been developed at Radboud University, Nijmegen, Netherlands. IRMA has created an efficient and simple smart card and smart phone implementation of ABCs, based on Idemix from IBM [4,5,6]. The fundamental idea of credential design and a broader non-technical description of the IRMA technology is given in Alpar et al. [7]. Our implementation[4] uses:

- eID documents such as passports, identity cards or driver's licenses as the standard identity documents;
- Android-based smart phones enabled with NFC as the user-devices;
- an IRMA (Android) app;
- an Enroller server;
- an Issuer server.

[4] IRMA self-enrolment implementation details can be found at https://github.com/credentials/irma_mno_server/blob/master/README.md.

In our implementation, the user chooses to enrol with his eID document via his smartphone's IRMA app[5] and enters the BAC data manually or by scanning a QR code that is printed on the latest version of Dutch driver's license. The IRMA app essentially functions as a remote card reader for the enroller, reading some data from the eID document and sending it to the Enroller server. This server then verifies the validity of the document, extracts some user's personal data from it, and requests the Issuer server to issue some credentials containing the extracted data to the smart phone[6]. Some of the screenshots of the IRMA app handling self-enrolment are provided in Figure 3 below.

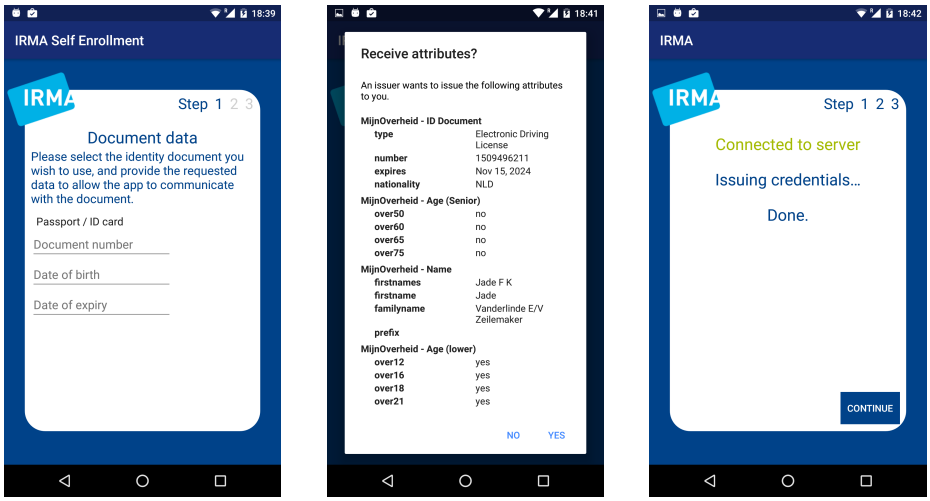

Fig. 3: Screenshots from an IRMA self-enrolment session

3.2 Weakness of basic self-enrolment

Although the basic self-enrolment protocol is user-friendly, inexpensive for both user and the Enroller, and results in authentic credentials on the user's smart phone, it has an important weakness: a malicious user might use someone else's eID document (stolen, lost or borrowed) and carry out the protocol. This would lead to the malicious user wrongfully getting the eID owner's credentials issued to his phone as his identity credentials. From then onward, the user can impersonate the eID-owner during online authentications with his phone. This attack is possible because there is little binding between the user and the identity document (or the mother card) that is used for the enrolment. We will address this weakness by considering several user-binding solutions described in Section 4.

[5] More details on IRMA smartphone app can be found at https://www.irmacard.org/irmaphone/

[6] How IRMA enrolment works can be seen in action in the Youtube video https://www.youtube.com/watch?v=q6IihEQFPys, see especially from 1:24 to 1:52.

3.3 Deriving credentials from Common Access Card (CAC)

On a conceptual level, our self-enrolment approach has some overlap with methods developed for deriving credentials from special US-identity cards such as Common Access Card (CAC), but it also differs in several essential aspects.

A CAC is a Personal Identity Verification (PIV) card issued by the U.S. Department of Defense that is meant for closed user groups (e.g. employees of government agencies). An application that uses CAC as the mother card to derive PIV credentials on mobile devices is Entrust Mobile Derived Credential solution[7]. It requires the user to undergo a derived credential enrolment process which involves his PC (desktop or laptop) that is connected to a CAC via the card reader, his mobile device and Entrust's Self Service Module (SSM). The enrolment takes place as follows.

1. The user navigates to the SSM's web page through the web browser on his PC and authenticates to the SSM using his PIV/CAC smartcard. The CAC gets activated by the user-specific PIN.
2. The SSM validates PIV credential on the card and lets the user select the link to request a derived PIV credential.
3. To ensure a secure user-device binding, the SSM uses 'Email with password via encrypted email' activation method in which two emails are sent to the user's pre-registered email address:
   - the first email is unencrypted and contains an encrypted link back to the SSM's web page for issuance of the derived credential, that can be decrypted using the password in the second email;
   - the second email is encrypted and contains a one-time password. This email can be decrypted only with the PIV credentials found on the user's CAC smartcard.
4. On entering the correct password on the mobile device, the user obtains the derived PIV credential from the SSM.

Entrust's enrolment is available only to a closed group of government agency's employees who already have a CAC smartcard and a government-issued secure email account. This type of enrolment achieves user and device binding by sending one-time password to the pre-registered email address of the user.

In comparison with the enrolment process described above, our self-enrolment implementation:

- is not restricted to a closed group with separate channels — via pre-issued email address;
- uses the phone's NFC capability to read out the ICAO standard eID document (e-passport or a driver's license) that are in principle available for everyone;
- supports eID documents without the PIN code activation — although eIDs with PIN are emerging, see Subsection 4.1;

[7] https://www.entrust.com/wp-content/uploads/2014/10/Mobile-Derived-Credential-WEB2-Nov15.pdf

– works in the context of attribute-based credentials (ABCs) instead of PKI certificates.
– does not achieve user-binding in its current form.

4 User-binding solutions

In this section, we describe several solutions that can achieve the much needed user-eID binding during self-enrolment.

4.1 PIN code check during self-enrolment

Probably the simplest solution for achieving user-binding is to equip an ICAO standard identity document with a PIN that is only known to the owner of the document — like for Common Access Cards (CACs). In the Netherlands, electronic driver's licenses with an experimental PIN are currently being tested for strong online authentication. Such a PIN is typically delivered to the user via a separate channel, like a (secure) PIN mailer. While using the eID document during enrolment, the user will have to enter the PIN to unlock either some of its data fields (other than mandatory data fields required for a passport functionality) or some specific functionality such as signing. For instance, the electronic identification card (nPA) in Germany requires the user to enter a correct PIN to unlock its signature function[8]. This aspect can be added to basic self-enrolment, whereby the user signs a fresh consent statement, in order to ensure the Enroller that the user is the legitimate owner of the eID document. In essence, this adds user-binding by having the user prove knowledge of the PIN. We can include such a PIN verification in the basic self-enrolment protocol in addition to the authenticity and integrity checks on the eID document.

4.2 Biometric check during self-enrolment

A second option is to extend our basic self-enrolment protocol with biometric checks in order to achieve user binding. ICAO documents digitally store a photo of the user and optionally fingerprints as well. Since fingerprints can usually only be read from the eID by authorised states, we focus on biometric face verification. We describe a possible scenario in several steps.

1. As in the basic self enrolment protocol, a user initiates enrolment via his phone, upon which the Enroller remotely accesses the user's eID via the phone's NFC interface and performs the eID checks.
2. If the eID checks are successful, the Enroller reads and stores the eID data that includes the user's identity data and his photo.
3. Next, the Enroller requests the user to present a biometric evidence in the form of a live video or some other form of face recognition.

[8] http://www.die-eid-funktion.de/unterscheidung_der_eid_funktion_und_der_qes.php

4. Then the Enroller matches the user's photo from the eID to the user's biometric evidence from the video.
5. If there is a match, then the Enroller proceeds to issue a signed confirmation, which guarantees the Issuer that the eID document is bound to the user and that his identity has been checked by the Enroller.
6. Finally, the Issuer signs the user's identity data (attributes) and issues them as credentials to the user's phone.

We briefly consider two methods, namely WebID video legitimation technology[9] and iProov[10], that could be used for performing the biometric check during self-enrolment.

WebID solution. WebID's video legitimation procedure involves a human verifier (e.g., an employee of the Enroller's organization) who does the task of identifying users over video calls. Regardless of the physical separation, sensory perception of the users is possible, since the user who is to be identified and the employee sit opposite one another "face-to-face" through this video transmission and communicate with one another. The user is asked to hold both the front and rear sides of a valid official identity card or passport in front of the webcam. To allow this to be both automatically and manually verified the ID must be tilted several times and moved so that the hologram and further security features can be checked. The identity number is also recorded and photos are made to secure the evidence. Finally a unique transaction number (TAN) is sent to the user by e-mail or text message, with which the legitimation can be confirmed online. The video-legitimation procedure provided by WebID Solutions has been examined and approved by BMF (German Federal Ministry of Finance) and BaFin (German Federal Financial Supervisory Authority). The basis for this type of legitimation is the new interpretation of section §6[11] of the Anti-Money-Laundering Act by the BMF dating from March 2014. A major bank ING-DiBa in Germany has chosen to adopt WebID's solution[12] with which, on opening a new account, customers of ING-DiBa can verify their identity directly online with video transmission from home via their own computer, tablet or smart phone.

Due to its real-time biometric checking capability involving the user and the employee, WebID's video legitimation could be added to our self-enrolment protocol.

iProov Verifier. iProov[13] is a biometric-based authentication solution that checks if the user's face corresponds to the face that was originally enrolled. The user

[9] https://www.webid-solutions.de/en/
[10] https://www.iproov.com/
[11] III. Interpretation of section 6 (2) no. 2 of the GwG ("not personally present") (https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/rs_1401_gw_verwaltungspraxis_vm_en.html).
[12] https://www.webid-solutions.de/en/assets/site/files/presse/140908_pm_ing_e.pdf
[13] https://www.iproov.com/what-we-do

can use any of his personal devices that has front-facing camera to use iProov where he just has to click and stare at the device to authenticate himself. iProov uses Flashmark technology that enables the user's screen flashing a sequence of colours on the user's face and during flashing, the video is streamed to the iProov servers. The iProov server:

- matches the user's face against the enrolment image;
- analyses the reflection of the display light on the user's face;
- examines the pattern of reflection to check it comes from a real face;
- checks the one-time sequence of colours to ensure it is the same as the session Flashmark.

If all the above checks are successful, iProov servers mark the user authentication successful.

A technology such as iProov can also be added to our basic self-enrolment protocol at the Enroller, where the user's real time image from the video is then compared against the user's photo read from the eID document. iProov is an experimental technology that is still being evaluated.

4.3 Data consistency checks during self-enrolment

Another solution to bind the eID document, the user and his device i.e. smart phone is to compare a part of the data from the eID document — say, name or date of birth — to some other reliable data source. If the data match, the enrolment succeeds; else it fails. The data source could come from the phone itself, if it has reliable, i.e. authentic and non-transferable, data of the user. We will explore this direction further in Section 6. The current section focuses on using an outside data-source to verify the enrolment data against. We will first sketch the general idea and then shortly discuss two possible enrollers in this scenario, namely mobile network operators (MNOs) and banks.

We assume the Enroller has access to an external data-source which contains authentic data of the enrolling user that can be matched against his eID data. In this scenario the Enroller also requires an additional way of authenticating the user. Possible enrollers could be institutions such as universities or the government, or companies such as MNOs or banks. We now generically describe the self enrolment protocol with such an Enroller.

1. A user requests the Enroller to carry out self-enrolment through his phone; the Enroller remotely accesses the user's eID via the user's phone's NFC interface and performs the eID checks as before, in Section 3.
2. Additionally, the Enroller requires the user authenticate. A successful authentication results in retrieving the user data from the Enroller's records. This data is then matched against the data read from the user's eID. If matched correctly, it goes to step 3. Otherwise, the Enroller aborts the process with a suitable error message to the user.
3. The Enroller digitally signs a user-identity confirmation message that consists of the user's eID data and sends it to the Issuer.

4. The Issuer verifies the Enroller's signature on the confirmation message, connects to the user's phone and issues the eID credentials.

Naturally, the reliability of such a scheme is dependent on the reliability of the external data-source and the additional authentication step mentioned above. In the following two paragraphs we look at two parties that, under some assumptions, could fulfil the role of an Enroller.

MNO-mediated self-enrolment. Mobile providers, also called Mobile Network Operators (MNOs), could function as the Enroller. Major MNOs in countries like the Netherlands, carry out face-to-face identity proofing for personal subscriptions. This is done at an MNO office or at the user's home, when the SIM (Subscriber Identity Module) card is delivered. Thus we assume that MNOs have authentic identity data and authentic SIM identities of the subscribers in their databases, obtained via a separate channel involving face-to-face authentication. During an enhanced self-enrolment, the enrolling user's eID data could be verified against the MNO's subscriber data in addition to the usual eID checks described in Section 3.

This approach has been discussed and evaluated in detail with a major MNO in the Netherlands. In the end the MNO decided not to implement this enhanced enrolment protocol because its database of subscriber data is well-protected and could not be used for experiments.

Bank-mediated self-enrolment. Banks could also fill the role of the Enroller. In many countries, opening a first bank account with a bank requires a face-to-face identity proofing session. Additionally, many banks have strong online authentication methods, such as authenticator tokens (e.g. ABN AMRO bank's e-identifier[14]), for authenticating online banking transactions. So, during self-enrolment, a bank could use the eID data to look up the user data in its customers database and then require the user to perform an additional authentication step towards the bank. Depending on the authentication process of a particular bank, this could provide strong user-binding. Within the Netherlands, the main banks have started an experimental joint authentication service called iDIN[15], where the different banks authenticate their clients with their existing e-banking tokens, but the result is a uniform identity message. This makes the development of a bank-mediated self-enrolment much simpler. It is experimentally supported in the IRMA ecosystem.

5 Evaluation of the user-binding solutions

In this section, we briefly evaluate the user-binding solutions described in the previous section, based on their security, trustworthiness, ease of deployment and use.

[14] https://www.abnamro.nl/nl/prive/betalen/edentifier/index.html
[15] http://www.connective.eu/financial/idin/

PIN check. Assuming that there are (or will be) eID documents that support PINs, with a restricted number of PIN entry attempts, PIN checks can provide a secure and simple way to achieve user-binding in our self-enrolment scenario. The trust assurance provided by the user PINs depends on how reliably and confidentially they have been generated in the first place and transported to the users. Further, it also depends on how securely the users store and maintain their PINs.

The downside of PINs is that users often forget them. If the PIN was delivered through a PIN mailer, this mail might have been lost at the time of enrolment, hence, making it impossible for the user to carry out self-enrolment. This requires (expensive) help center contacts and re-issuing.

Biometric check. In the biometric checks that we have considered in this paper, the Enroller compares the photo that is digitally read from the eID document to the person's face that appears in a real time video session during enrolment. The trust assurance level of this biometrically enhanced protocol depends on the quality of the biometric comparison mechanisms. In any case, we would either need a human verifier or a server at the Enroller's end to perform the biometric comparison, communicate with the user and make sure that the owner of the eID document and the communicating user are the same person.

In the case of a human verifier, the result of the biometric check is reliable and convincing but the video addition will be costly, since it requires additional personnel, and will increase the length (in time) of each enrolment, especially when it leads to queues for the video procedure. An automated biometric check using a server is relatively cheap and fast but it has a greater chance of producing unreliable result due to false positives/negatives.

Data consistency check. In general an additional data-consistency check seems a cheap way to strengthen self-enrolment. However, it requires at least (1) trustworthy, authentic user data and (2) an additional authentication of the user to the Enroller. MNOs and banks seem natural fits for these roles, which we separately discuss and evaluate below. Entrust's CAC-based self-enrolment that is described in Section 3.3, which uses a one-time password transmitted to a pre-issued e-mail address of the user, essentially also falls in this category.

MNO-mediated self-enrolment. Assigning an MNO as the Enroller can be seen as an advantage in terms of security as the MNO can additionally verify whether a user's eID data matches the user data in his SIM subscription. This check ensures that the phone (SIM card) that will eventually store the issued derived credentials belongs to the enrolling user. Thus, an MNO-mediated self-enrolment gives additional guarantees about the link between the user, his identity document and his SIM card i.e. it provides not only user binding but also device binding.

Moreover, we assume that the user has undergone a prior face-to-face enrolment at the MNO when he bought the SIM card and signed the subscription

contract. This assumption results in self-enrolment being more secure and trustworthy as it is now built upon two previous face-to-face enrolments, one for the eID document and one for the SIM subscription. The downsides of MNO-mediated user-binding are: (1) it is limited only to the MNOs which carry out face-to-face enrolments of its subscribers for obtaining SIM subscription; (2) it is not applicable to users who own prepaid/anonymous SIM cards: they can be obtained without the user having to go through an enrolment at the MNO.

Bank-mediated self-enrolment. With a bank in the position of the Enroller, we also assume a prior face-to-face enrolment of the user during the opening of the bank account. The bank-mediated self-enrolment can potentially offer the strongest user-binding, based on an out-of-band authentication using a secure authentication token, a bank card and a PIN. Alternatively, it could offer authentication based on username/password. This difference in security level of the authentication methods makes evaluation hard. Still, even in a username/password scenario, it is an additional authentication of a separate factor (something you know), in addition to the possession of the passport. The downside of such a system is the plurality of authentication mechanisms offered by banks. This means development of such a system can be costly, because the authentication mechanisms of all participating banks need to be supported. Additionally, this means all these authentication mechanisms will need to be evaluated separately and the resulting process may not provide a uniform user experience. To be viable, a uniform system of an authenticating service combining several banks, such as the Dutch iDIN, seems necessary.

6 Combining several self-enrolment approaches

Since none of the above presented enhancements for self-enrolment is clearly "the best" it is worthwhile to look into ways to combine these approaches. Since we are working within an ABC framework, we also have the ability to use prior issued credentials during a self-enrolment in order to strengthen the confidence in the user's identity that is presented to a service provider during an authentication.

The enrolment procedure now involves several steps — which is typical for attribute-based systems: the user first obtains credentials from some online identity provider. Next, in an enhanced version of our self-enrolment, these existing credentials are read by the Enroller and compared to the ones from the eID document. In this way several enrolment steps can be built upon each other, to create a reliable and consistent set of attributes.

In IRMA ecosystem, we have an implementation where we use a (federated) identity provider (or the Issuer) such as SURFconext[16], where the user has a login and the Issuer already has some of the user's data that he can issue to the user's IRMA app as authentic credentials. These credentials can then be used within a self-enrolment session to compare with the eID data. Essentially this

[16] https://www.surf.nl/en/services-and-products/surfconext/index.html

comes down to an additional data-consistency check (as described in Section 4.3) with the data provided by the phone.

Within such a multi-step enrolment system one can support credentials of varied trust assurance levels, corresponding to the number (and nature) of the self-enrolment steps that the user performed. The credentials obtained from an online identity provider (e.g. SURFconext) has low assurance but they can be used within an eID-based self-enrolment as mentioned above to obtain higher assurance credentials. Optionally, these credentials could then be used within yet another self-enrolment session, for instance involving a biometric verification to obtain even higher assurance credentials. It would then be up to service providers to decide which assurance level they accept for their service. For instance, an online ticket service would likely accept lower assurance level credentials whereas a higher assurance level credential would be required to review your own patient data at a hospital portal.

7 Conclusion

In this paper, we start from a basic self-enrolment scheme which allows a user with an eID document and an NFC-enabled smart phone to enrol himself from any location (e.g. sitting at home) by connecting to an Enroller entity online. Subsequently, he can get derived credentials issued by an Issuer entity to his smart phone. This type of enrolment is user-friendly, cheap and commercially viable when compared to traditional face-to-face enrolments. Based on the experiences with our smartphone implementation of this basic self-enrolment protocol in an attribute-based credential (ABC) framework, we can claim that it is also practical and efficient. Furthermore, the paper discusses several enhancements of the basic self-enrolment involving different user-eID document binding solutions — which should prevent a malicious user from using someone else's eID document for enrolment.

Which solution works best in which situation depends on various factors, such as availability of a PIN on eID documents, costs, effort, and willingness of different parties to cooperate. Since no solution offers a panacea, the solution that best fits the existing IRMA self-enrolment implementation is the one from Section 6, where eID data is compared to the credentials from a previous self enrolment, to achieve higher assurance levels for user credentials.

References

1. William E Burr, Donna F Dodson, Elaine M Newton, Ray A Perlner, W Timothy Polk, Sarbari Gupta, and Emad A Nabbus. SP 800-63-1. Electronic authentication guideline. 2011.
2. ABC4Trust. Attribute-Based Credentials tutorial. http://www.dime-project.eu/en/Home/dime/events/list/tutorial-on-attributebased-credentials, 2011.
3. J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. Wichers Schreur. Crossing borders: Security and privacy issues of the European e-Passport. In *Advances in*

Information and Computer Security, number 4266 in Lect. Notes Comp. Sci., pages 152–167. Springer, Berlin, 2006.
4. IBM Research Zürich Security Team. Specification of the Identity Mixer cryptographic library. Technical report, IBM Research, Zürich, 02 2012.
5. Pim Vullers and Gergely Alpár. Efficient selective disclosure on smart cards using idemix. In *Policies and Research in Identity Management*. Springer, 2013.
6. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology EUROCRYPT 2001*, pages 93–118. Springer, 2001.
7. Gergely Alpár and Bart Jacobs. Credential design in attribute-based identity management. In *Bridging distances in technology and regulation, 3rd TILTing Perspectives Conference*, pages 189–204, 2013.