F. Boutros, N. Damer, M. Fang, M. Gomez-Barrero, K. Raja,
C. Rathgeb, A. Sequeira, and M. Todisco (Eds.): BIOSIG 2024,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2024

A Study on the Next Generation of Digital Travel Credentials

Ana-Teodora Radutoiu [1] Amina Bassit [2] Raymond Veldhuis [3] Christoph Busch [4]

Abstract: Digital travel credential (DTC) is the future passport. The goal of DTCs is to bound a digital passport to a smartphone device for a booklet-free travel experience. However, new security and privacy issues and challenges arise. The main challenges to address are preventing unauthorized cloning of a holder's DTC and ensuring impostors cannot misuse a holder's credentials at the airport. This study researches how to overcome the challenges of cloning and misuse of credentials, by proposing an iris biometric-based solution. We design three protocols: Enrolment of the DTC, active authentication at the airport, and switching smartphone devices (legitimate cloning of the DTC). The protocols mainly focus on preventing unauthorized cloning and misuse of the DTC by impostors using iris biometrics to obtain a private-public key pair. This key pair is used to prove the legitimate holder's physical presence, ensuring that the protocols designed continue to prevent cloning and misuse.

1 Introduction

Many aspects of our daily lives are becoming digitalized for our convenience. The E-passport introduced a chip into the traditional booklet that stores the individual's personal information along with the photograph [In]. The E-passport allows airports to enable self-service passport control, enabling faster border control transition at the airport.

Digital travel credentials (DTCs) offer an alternative to the physical passport that is being used today. The concept of DTC is based on the International Civil Aviation Organization's (ICAO) document 9303 [In21]. The goal of DTCs is to make aviation travel more fluid and thus optimize individuals' time at the airports while maintaining a high security level. The DTC consists of virtual and physical components that are cryptographically linked [In20]. The virtual component (DTC-VC) represents an individual's passport data encoded following the standardized logical data structure (LDS) [In21]. The LDS contains 16 data groups to store relevant passport information. The virtual component resides in the physical component. The individual holds the physical component (DTC-PC) as evidence of identity, the component is linked to the virtual one. ICAO has classified the transition to DTC into the following three levels [In20]:

[1] Technical University of Denmark
[2] University of Twente (now with Michigan State University)
[3] Norwegian University of Science and Technology
[4] Acknowledgments: This research has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121280 (EINSTEIN). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect the views of the EU/Executive Agency. Neither the EU or the granting authority can be held responsible for them.

Level 1: **(eMRTD bound)**. This level consists only of a virtual component and the electronic Machine Readable Travel Document (eMRTD), the E-passport. The virtual component is created by reading the chip data from the eMRTD.

Level 2: **(eMRTD-PC bound)**. This level consists of a virtual component, a physical component, and the eMRTD. The DTC-PC is created on a smartphone device and the eMRTD is an alternate or fallback.

Level 3: **(PC bound)**. This level consists of a virtual and a physical component, with no booklet (eMRTD) as a fallback. The DTC-PC is created on a smartphone device.

Studies regarding the use of DTCs in practice have been initiated by European DTC pilot programs in the Netherlands and Finland [Go23, Th]. They started testing the DTC level 1 at certain airports for specific flights during the border control. These pilot programs still rely on the E-passport. However, they use the smartphone device to share data with border control and answer necessary entry questionnaires prior to flights.

Currently, the security mechanism in the E-passport uses active authentication, a challenge-response technique, to prevent passport cloning. The chip in the passport is associated with a private key in its secure memory, and during active authentication, the chip may prove its knowledge of this private key [In21]. However, at DTC level 3 there is no eMRTD, why one of the main challenges with the transition to level 3 is related to unauthorized cloning of the DTC. Another main challenge is preventing impostors from misusing another holder's DTC at airport control desks.

This work aims to develop ideas and designs for how to proceed with the DTC level 3 (PC-bound), and to our knowledge, there are no solutions or designs on the topic. We aim to design protocols that focus on resolving these cloning and misuse challenges at DTC level 3. Our solution is based on iris recognition using the holder's smartphone [Ra17]. Iris recognition is a reliable biometric approach for distinguishing individuals from one another [Ra17]. The encoded iris reference can be stored in data group four (DG4) in the LDS, which is currently unused. The main idea behind our protocols is to use the iris image to derive a private key, as a replacement for the chip in the eMRTD.

This paper will be structured as follows; First, we describe the problem statement and define relevant phases along with design requirements for them. Next, we study different candidate solutions for obtaining a private key from an iris image. Afterward, we present our final design protocols. Lastly, we conclude our study.

2 Problem Statement

With DTC at level 3, there is no booklet as a fallback, and the credentials will rely on the physical component, the individual's smartphone device. We want to enable legitimate cloning from an old smartphone to a new one while preventing unauthorized cloning. By unauthorized cloning, we mean cloning the digital passport to another device without the issuer's consent. For example, if an individual's smartphone is stolen and the stealer seeks to clone the DTC on the stolen phone to another device.

Furthermore, we desire an authentication process at the airport, which will substitute the active authentication process formerly validating the originality of an eMRTD. This new process should be able to deal with the inherent fuzziness in iris images, such that the true DTC holder will not experience authentication issues at the airport. However, the process must prevent impostors from misusing another holder's DTC. For example, if an individual's DTC-PC is lost and an impostor holding the lost DTC-PC attempts to use it to transit through the airport.

Many more challenges and issues arise with the DTC at level 3. However, in our study, we will investigate how to prevent the two major issues regarding cloning and misuse. We have defined the following three phases for DTC level 3:

Phase 1: **Enrolment** A protocol between an individual and the issuer to enroll an individual's smartphone device in the DTC level 3 program.

Phase 2: **Active Authentication** A protocol between the individual's DTC and the airport terminal to verify that the legitimate user is the one claiming the authentication at an airport.

Phase 3: **Switch Device** A protocol between the individual and an online issuer to legitimate clone the DTC from an individual's old device to a new one.

In case a smartphone storing a DTC is lost or stolen, the individual must go through phase 1 again. To ensure that our protocol designs for each of the three phases above prevent cloning and misuse, we define the following design requirements:

- The design must ensure that unauthorized cloning of the DTC without the approval of the government (issuer) cannot occur during phase 3.
- The design must verify during border control transition, that the DTC has not been unauthorizedly cloned.
- The design during phase 2 must ensure that impostors cannot misuse another holder's DTC at the airport.

3 Candidate Solutions

In our setting, the main usage of iris biometrics is to obtain a public-private key pair. The private key is then used in a challenge-response protocol to prevent cloning and misuse. Instead of using iris biometrics directly to obtain the desired private key, we propose that a seed be extracted from the iris image. This unique secret seed can then be used as input to a deterministic algorithm, K, which outputs a public-private key pair,

$$K(s) = \left(k_{\text{pv}}, k_{\text{pb}}\right), \tag{1}$$

where s denotes the unique seed, k_{pv} the private key, and k_{pb} the public key. The public key is stored in data group 15 (DG15) in the DTC, but the private key is not stored or saved.

Three methods based on iris biometrics to obtain the desired seed will be considered: A fuzzy extractor approach, a fuzzy vault scheme, and a simple key generation method from an iris template. Each method will be presented briefly along with the necessary data to store in datagroup four (DG4) in the DTC [In21].

3.1 Biometric Fuzzy Extractor

The biometric fuzzy extractor is a key generation approach, where the key (seed) is generated from the iris image. The main concept of a biometric fuzzy extractor is to use helper data to ensure the same seed is generated for different images of the same iris. To overcome fuzziness in iris an error correction code is used [RU11]. Rathgeb and Uhl proposed a key generation scheme using iris biometrics based on the biometric fuzzy extractor method [RU11]. The helper data, P, consists of two objects, a "bit-mask", and "check bits". The bits in the "bit-mask" link the seed with a specific individual's iris biometric sample, while the "check bits" are for the error correction code (a binary BCH-code). This approach needs to store the helper data in DG4.

3.2 Fuzzy Vault Scheme

The concept of the fuzzy vault scheme is to lock some secret (the seed) under a set A using a polynomial, f, to encode the secret. If the set A and a new set B overlap substantially, the vault can be unlocked with B, thus acquiring the secret [JS06]. The set A and B are the reference and probe templates respectively of some biometric samples. Tams proposed an unlinkable minutiae-based fuzzy vault, which is an improvement of the original scheme [Ta16]. Tams' fuzzy vault was originally designed for fingerprint biometrics, but it will be assumed that such an approach is also achievable using iris biometrics [Ra16]. The vault, V, must be stored in DG4 to retrieve the secret with a probe template.

3.3 Bloom Filter Based Approach

Rathgeb et. al. proposed a cancelable iris biometric template based on Bloom filters [RBB13, Ra14]. A Bloom filter is a data structure that represents a set, it uses a single hash function to store the elements from the set in the filter [RBB13]. Their approach splits the iris code into K blocks, and each relevant row in the block is represented in a Bloom filter. However, before representing a row in the Bloom filter, the row is `XOR`ed with an application-specific and/or user-specific secret, T, in order to enable unlinkability across different applications. The approach results in a set of K separate Bloom filters as the biometric template. A simple key generation method is to concatenate the Bloom filters,

$$\text{seed} = [\, b_1 \; b_2 \; \ldots \; b_K \,] \in \{0,1\}^{K \cdot 2^w}, \tag{2}$$

and use the concatenation as the secret seed. While the bloom filter approach has built-in tolerance to intra-class variations, some additional error correction codes might be added

to address the fuzziness of biometric iris samples. Only the application-specific secret, T, will be necessary to store in DG4. We further assume that each individual has a unique T.

3.4 Comparison of the Candidate Solutions

The three methods will be compared (Tab. 1) based on the criteria listed below,

- The biometric templates stored must satisfy the biometric template protection requirements: **Irreversibility** and **unlinkability** [IS22]. **Irreversibility:** The original iris sample cannot be retrieved using the iris template. **Unlinkability:** Two different templates cannot link to the same individual.
- **Intra-class robustness**. The approach should be able to handle the fuzziness in an individual's iris biometric samples. While ensuring that the seed cannot be acquired when using a biometric sample from a different individual.
- **Privacy protection**, in terms of what data is necessary to store.
- **Complexity** of the approach; Whether the approach is simple or more complex, and requiring more computations both at enrolment and authentication time.

Criteria	Fuzzy Extractor, Rathgeb & Uhl [RU11]	Fuzzy Vault, Tams [Ta16]	Bloom Filters, Rathgeb et. al. [Ra14]
Irreversible	✓	✓	✓
Unlinkable	(✓)	✓	✓
Intra-class robustness	✓	✓	✓
Privacy protection	helper data P	vault V	secret T
Complexity	complex	complex	simple

Tab. 1: Conclusions on the five criteria for each approach are made from the respective literature. The checkmark, ✓, denotes that the approach satisfies the criteria. For privacy protection, the data needed to be stored in DG4 is noted.

The iris biometrics solutions show strong intra-class robustness, thus being able to overcome enough fuzziness in the iris images. The cancelable iris template based on Bloom filters [RBB13, Ra14] proves to be both irreversible and unlinkable. Furthermore, the fuzzy vault scheme by Tams [Ta16] overcomes well-known problems of cross-matching, why this updated approach is also both irreversible and unlinkable. On the other hand, within fuzzy extractor methods cross-matching issues are present [Ke11], why the key generation scheme by Rathgeb and Uhl [RU11] is not necessarily unlinkable without additional solutions [Ke11]. Considering Table 1, simply using the cancelable biometric template with Bloom filters designed by Rathgeb et. al. [RBB13, Ra14] appears to satisfy all criteria while being a simple method and storing the least amount of information. We chose to move forward using this approach for key generation.

4 Our Solution

In this section, the protocol designs for the three phases, enrolment, active authentication, and switch device, will be outlined.

4.1 Phase 1 Enrolment

This protocol is needed when 1) an individual is first enrolled in the DTC level 3, 2) the digital passport must be renewed, or 3) in case the smartphone device with the DTC incorporated is lost. We outline the protocol in Figure 1. The parties involved are the DTC user and the issuer. For future phases, the issuer stores some information about the DTC and the individual in a separate issuer database. It is assumed such a database exists and can securely store the necessary information. The individual protocol steps are denoted **E1** to **E7**.

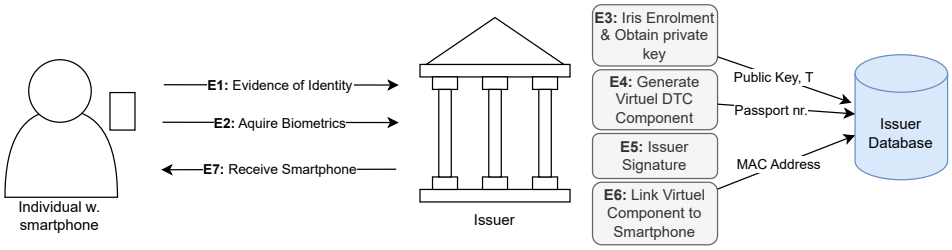

Fig. 1: Design protocol of phase 1, enrolment of the DTC level 3. The protocol steps are denoted **E1** to **E7**.

We assume that the individual has been cleared to participate in the DTC program and has gotten an appointment at the issuer to set up the DTC on their smartphone device. Upon arriving at the issuer, the individual must prove their identity using an identification (ID) document such as the old passport booklet, birth certificate, or entry in the national registry (**E1**). Afterward, the individual's facial and iris images are acquired (**E2**). The issuer enrolls the individual's iris biometric reference using the acquired image (**E3**) in the following steps; 1) The iris code is found, 2) the cancelable reference template based on Bloom filters is found, 3) the seed is extracted from the template, 4) the public key, k_{pb}, is found using K. The key k_{pb} and unique secret T are stored in the issuer's private database. The issuer proceeds to generate the DTC-VC as all relevant information has been acquired (**E4**) and the new digital passport number is stored. For security reasons, the issuer signs the passport number (**E5**). Lastly, the issuer prepares the smartphone device (DTC-PC) and links it to the DTC-VC (**E6**). The smartphone's MAC address is stored in the issuer database and the smartphone is returned to the individual (**E7**).

4.2 Phase 2 Active Authentication

The designed protocol for the active authentication phase is outlined in Figure 2, where the individual protocol steps are denoted **A1** to **A8**. The protocol is between the individual's smartphone device (DTC-PC) and the airport terminal to prevent misuse of the digital passport.

The protocol is initiated by allowing the terminal to scan the digital passport from the smartphone, thus transferring the LDS of the DTC (**A1**). The terminal proceeds to verify

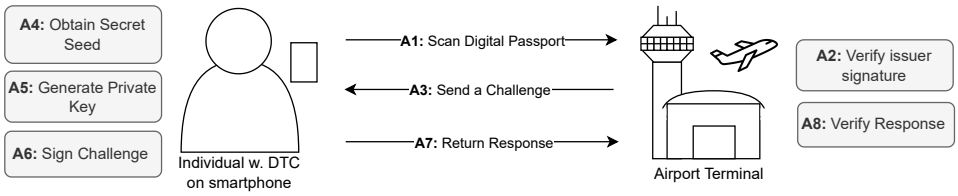

Fig. 2: Design protocol of phase 2, a challenge-response protocol at the airport to prevent misuse and cloning of DTC at level 3. Protocol steps are denoted **A1** to **A8**.

the issuer's signature of the passport number (**A2**). For this, we assume a public key infrastructure is working. Afterward, the terminal sends a challenge to the device, a random number n (**A3**). The device must prove its knowledge of the private key, k_{pv}, by signing the challenge. To obtain k_{pv}, the device takes an image of the individual's iris, generates the probe template based on Bloom filters, and concatenates them to obtain the secret seed (**A4**). The private-public keypair is found using K from eq. (1) (**A5**). The device generates the following hash,

$$\text{augmented-challenge} = [\ n\ \ \text{passport-nr.}\ \ \text{MAC-address}\ ]. \tag{3}$$

This links the terminal challenge, n, to the passport and the smartphone device. Using k_{pv}, the device signs the augmented-challenge (**A6**) and returns its response (signed augmented-challenge) to the terminal (**A7**). The terminal generates the same augmented-challenge with the information from the issuer database and the LDS. Afterward, the terminal proceeds to verify the signature by decrypting the response with k_{pb} from DG15 (**A8**). The main goal of this protocol is to prove knowledge of the private key, moreover, it also indirectly checks if the device is the registered smartphone at the issuer.

4.3 Phase 3 Switch Device

This phase is required if the individual wishes to legitimately clone the DTC from an old device (smartphone 1) to a new device (smartphone 2). We outline the protocol in Figure 3, where **S1** to **S6** denotes the individual steps. To prevent the individual's physical presence at the issuer each time a new smartphone is acquired, this protocol introduces an interaction between the individual and an online issuer as an alternative. Unless the individual has valid documentation for needing the DTC on both the old and new smartphone, the DTC on smartphone 1 will be revoked after the legitimate cloning.

The protocol is initiated by the individual, who submits a switch device request (**S1**) by sending the issuer's signature of the passport number to the online issuer. The online issuer must either approve or deny the request. If the request is approved, the online issuer proceeds to request an iris image from the individual (**S3**). The individual sends the iris image and the new smartphone MAC address to the online issuer (**S4**). We assume that it is secure to send the iris image, as we are dealing with a trusted party and protocol. Afterwards, the online issuer must perform a sequence of cloning checks (**S5**), this step

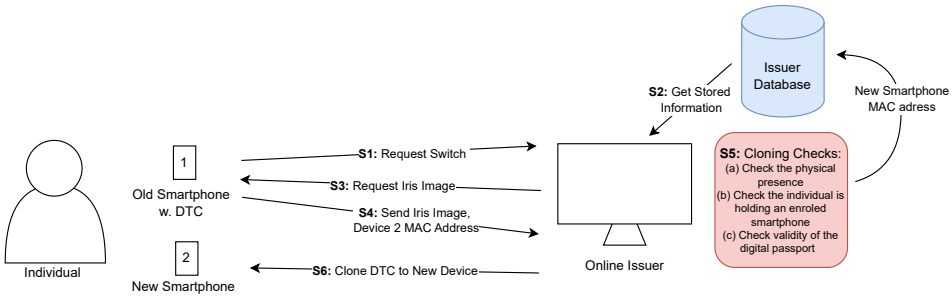

Fig. 3: Design protocol of phase 3, the DTC must be legitimately cloned from an old device (smartphone 1) to a new device (smartphone 2). The protocol steps are denoted **S1** to **S6**.

is essential to prevent unauthorized cloning of the DTC. We suggest the following three steps which the online issuer must check,

(a) *Check the physical presence:* By generating the public key k_{pb} using the iris image given from the individual. The key obtained must correspond to the key saved in the issuer database.
(b) *Check the individual is holding an enrolled smartphone:* By linking the smartphone 1 MAC address with the digital passport number signed by the issuer.
(c) *Check the validity of the digital passport:* By verifying the issuer's signature of the digital passport number.

If the online issuer approves all cloning checks, the online issuer goes ahead with the switch. Firstly, the online issuer updates the MAC address in the database with smartphone 2. Next, the online issuer initiates the DTC to be cloned from the old device to the new one and possibly revoked from smartphone 1 (**S6**). We assume that such a legitimate cloning function exists and can be initiated by the online issuer if all is approved.

5 Conclusion

During this study, three protocols; enrolment, active authentication, and switch device, have been designed when using digital travel credentials at level three. By incorporating iris biometrics, these protocols are designed to prevent unauthorized cloning and ensure that a holder's credentials cannot be misused by impostors.Based on a set of criteria, we chose to move forward with the Bloom filter approach. The key pair is then utilized during active authentication at the airport and when switching smartphone devices as the holder's proof of physical presence. We believe these protocols help the DTC at level three to withstand cloning and misuse challenges and thus satisfy our design requirements. The next step to move forward with DTC level 3, would be to implement these design protocols and evaluate their performance with respect to our design requirements.

References

[Go23] Government of the Netherlands: , Dutch participation in European DTC pilot. https://www.government.nl/documents/publications/2023/02/23/dtc, October 27, 2023. Accessed: 2024-04-08.

[In] International Civil Aviation Organization: , ePassport Basics. https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx. Accessed: 2024-04-08.

[In20] International Civil Aviation Organization: Guiding Core Principles for the Development of Digital Travel Credential (DTC). October 2020. Version 4.4. https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guiding%20core%20principles%20for%20the%20development%20of%20a%20Digital%20Travel%20Credential%20%20%28DTC%29.PDF.

[In21] International Civil Aviation Organization: Doc 9303 Machine Readable Travel Documents. Eighth edition, 2021. https://www.icao.int/publications/pages/publication.aspx?docnum=9303.

[IS22] ISO/IEC: 24745:2022 Information security, cybersecurity and privacy protection, Biometric information protection. Second edition, 2022.

[JS06] Juels, Ari; Sudan, Madhu: A fuzzy vault scheme. Designs, Codes, and Cryptography, 38(2):237–257, 2006.

[Ke11] Kelkboom, Emile J.C.; Breebaart, Jeroen; Kevenaar, Tom A.M.; Buhan, Ileana; Veldhuis, Raymond N.J.: Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. Ieee Transactions on Information Forensics and Security, 6(1):107–121, 2011.

[Ra14] Rathgeb, Christian; Breitinger, Frank; Busch, Christoph; Baier, Harald: On application of bloom filters to iris biometrics. Iet Biometrics, 3(4):207–218, 2014.

[Ra16] Rathgeb, Christian; Tams, Benjamin; Wagner, Johannes; Busch, Christoph: Unlinkable improved multi-biometric iris fuzzy vault. Eurasip Journal on Information Security, 2016(1):26, 2016.

[Ra17] Raja, Kiran B.; Raghavendra, R.; Venkatesh, Sushma; Busch, Christoph: Multi-patch deep sparse histograms for iris recognition in visible spectrum using collaborative subspace for robust verification. Pattern Recognition Letters, 91:27–36, 2017.

[RBB13] Rathgeb, C.; Breitinger, F.; Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive bloom filters. Proceedings - 2013 International Conference on Biometrics, Icb 2013, p. 6612976, 2013.

[RU11] Rathgeb, C.; Uhl, A.: Context-based biometric key generation for Iris. Iet Computer Vision, 5(6):389–397, 2011.

[Ta16] Tams, Benjamin: Unlinkable minutiae-based fuzzy vault for multiple fingerprints. Iet Biometrics, 5(3):170–180, 2016.

[Th] The Finnish Border Guard: , DTC Border control faster and smoother. https://raja.fi/en/dtc. Accessed: 2024-04-08.