Traveler Authentication at Airports Provisional Patent Application

Francisco Corella   Karen Pomian Lewison

August 30, 2019

1 Background

Today a traveler is authenticated at an airport security checkpoint by presenting a boarding pass and an identity document such as a passport, a driver's license or a national identity card. A security officer checks the identity document for signs of tampering, visually matches the traveler's photo printed on the document to the traveler's face, and checks that the name printed on the document is the same as the name printed on the boarding pass. Later, at the boarding gate, the traveler is authenticated by presenting a paper boarding pass with a printed QR code or bar code, or showing the code on the screen of a mobile phone.

These authentication methods have several security weaknesses:

- At the security checkpoint, the security officer has no way to determine whether the document has been revoked.
- Counterfeiting experts are able to create identity documents that pass the tampering checks performed by the security officer.
- Photos printed on identity documents are small and of poor quality, making visual identification difficult and potentially inaccurate.
- When checkpoint lines become long, security officers work under time pressure, which may cause them to be less thorough and make mistakes.
- The identity of the traveler is not verified at the boarding gate. This may allow an attacker who gains access to the concourse, e.g. as an

employee of an airport store, and steals a paper boarding pass or a phone carrying a boarding QR code or bar code, to board the flight.

These security weaknesses may allow terrorists to board planes.

Advances in face recognition technology have made it possible to identify a traveler with good accuracy by comparing an image taken by a security camera to an image of the traveler stored in a database. However, storing the facial image in a database creates a grave privacy risk for travelers, as databases are known to be vulnerable to security breaches.

There is thus a need for a method of using face recognition technology to authenticate travelers at airports without storing their facial images in a database.

2 Traveler authentication method

We propose a method of authenticating a traveler by means of a facial image, where the image is included in a digital credential rather than in a database. The method is described herein as it applies to air travel, but it is also applicable to other means of transportation.

2.1 Traveler credentials

In some embodiments of the proposed method, illustrated in Figure 1, the traveler carries a digital travel credential (DTC) and one or more digital boarding passes (DBPs), one for each leg of the trip, in a smart phone.

The DTC is issued by a country that implements the proposed method of authenticating travelers in its airports and is digitally signed by a Travel Certificate Authority (TCA) set up by that country. In the United States, the role of the TCA could be played by the Transportation Security Agency (TSA). The TCA has a key pair pertaining to a digital signature scheme such as RSASSA-PSS, RSASSA-PKCS1-v1_5, DSA or ECDSA, comprising a private key and a public key. The signature on the DTC is computed using the private key and verifiable using the public key, which is known to the security checkpoints of the country. A country may obtain the public key of the TCA of another country through an international organization or through diplomatic channels, and distribute it to its security checkpoints so that they can identify passengers carrying DTCs issued by the other country.

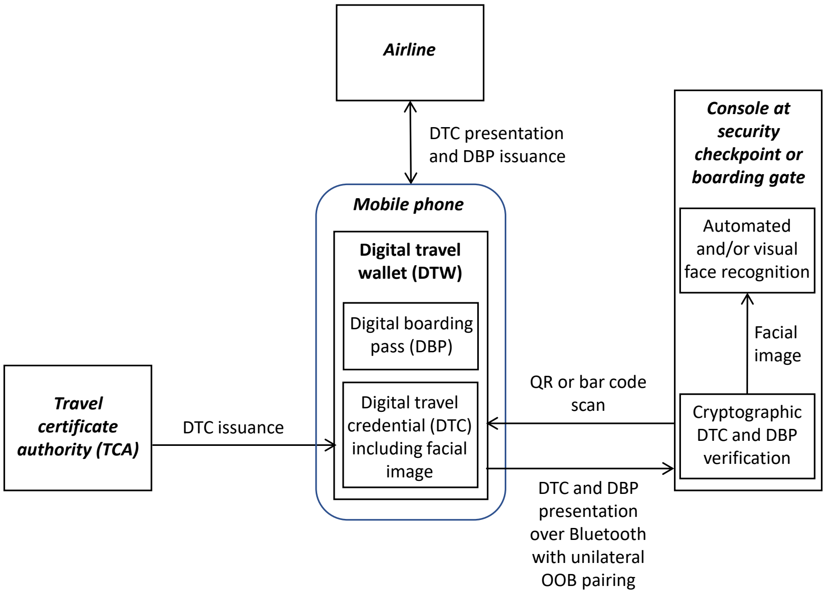
Airline
DTC presentation and DBP issuance
Console at security checkpoint or boarding gate
Mobile phone
Digital travel wallet (DTW)
Automated and/or visual face recognition
Digital boarding pass (DBP)
Facial image
QR or bar code scan
Travel certificate authority (TCA)
DTC issuance
Digital travel credential (DTC) including facial image
Cryptographic DTC and DBP verification
DTC and DBP presentation over Bluetooth with unilateral OOB pairing

Figure 1: Traveler authentication system

In some embodiments the DTC comprises a private key, the facial image, and a certificate that contains fields comprising: a cryptographic hash of the facial image computed by means of a cryptographic hash function such as SHA-256; traveler data such as the traveler's name, address and date of birth; a public key associated with the private key; and certificate metadata such as a validity period, a serial number and the name of the TCA that has issued the DTC. Although the facial image is not included in the certificate it is indirectly covered by the signature on the certificate, which covers the hash of the image contained in the certificate, and bound to the traveler data by the signature. The facial image in the DTC is thus certified by the TCA.

Such a DTC can be used for two-factor authentication by face recognition and proof of possession of the private key, or for one-factor cryptographic authentication by proof of possession of the private key without presentation of the facial image to the verifier, or for one-factor biometric authentication without proving possession of the private key.

In some embodiments where the DTC comprises a private key, the facial image and a certificate as described above, the certificate is more specifically an X.509 public key certificate as profiled by the IETF [1], where the cryptographic hash is included as the value of an extension.

In other embodiments the DTC is a rich credential as described in US patent application 15/468,100, where the traveler data is encoded as a collection of attributes and the facial image is included in a biometric template matching (BTM) subtree in the role of a biometric template to be matched against a facial image taken by a camera at the security checkpoint. In such embodiments the digital signature is included in the rich certificate component of the rich credential, and computed on the root label of the typed hash tree component of the rich certificate and on the metadata and public key components of the rich certificate.

In other embodiments the DTC is a kind of rich credential where the rich certificate component contains the root label of the typed hash tree instead of the typed hash tree itself, the typed hash tree being a separate component of the rich credential. In such embodiments the digital signature is computed on the contents of the rich certificate other than the signature itself.

The DBP is issued and digitally signed by the airline a short time (e.g. 24 hours) before the flight. Like the TCA, the airline has a key pair pertaining to a digital signature scheme such as RSASSA-PSS, RSASSA-PKCS1-v1_5, DSA or ECDSA, comprising a private key and a public key. The signature is computed using the private key and verifiable using the public key, which is known to the security checkpoints and boarding gates of the airports where the airline operates.

In some embodiments the DBP contains data that uniquely identifies the flight such as the date of the flight and a flight code, data that uniquely identifies the DTC such as the name of the TCA name and a serial number, and the digital signature, which is computed over the contents of the DBP other than the digital signature itself. In some such embodiments the DBP is an X.509 attribute certificate as profiled by the IETF in RFC 5755, which is linked to the DTC by inclusion of the data that uniquely identifies the DTC in the Holder field.

In some embodiments the flight code used to identify a flight consists of the two-letter IATA airline designator code and a 1-to-4 digit flight number. A flight may be marketed by multiple airlines under a codesharing agreement. It may then have multiple flight codes and the DBP may include any of those flight codes to identify the flight.

2.2 Digital travel wallet

In some embodiments the DTC and one or more DBPs to be used in a trip are carried in a native app installed in a smart phone, which we call a digital travel wallet (DTW). Being carried in the DTW means being kept in storage controlled by the DTW, preferably protected against tampering and malware, such as key chain storage located within a Secure Element, a Trusted Execution Environment (TEE) such as the Apple Secure Enclave, or a Trusted Platform Module (TPM). In some embodiments data in the DTW is encrypted by the operating system of the smart phone and the traveler is required to authenticate to the operating system with a PIN, a fingerprint or face recognition before the data is decrypted and the DTW can be used.

Travelers with multiple nationalities, or with residence in a country other than their country of citizenship, may have DTCs issued by multiple TCAs. In some embodiments the DTW is an app trusted by the traveler and downloaded from a trusted app store, which may be used to carry DTCs issued by multiple TCAs. In other embodiments the DTW is provided by a TCA and does not carry DTCs issued by other TCAs; in such embodiments the DTW app is downloadable over the Internet from a web site hosted by the TCA, or over a secure wireless network in a facility visited by the traveler for in-person proofing as described below in Section 2.3.

In some embodiments the DTW has a user interface that allows the traveler to obtains DBPs and select the DBP to be presented at the next security checkpoint or boarding gate.

2.3 Issuance of the DTC

In some embodiments a traveler obtains a DTC from a TCA by means of an in-person proofing procedure. The traveler visits an office of a Travel Registration Authority (TRA) associated with or licensed by the TCA and provides physical documentation of the traveler data to be included in the DTC, e.g. by presenting a passport, a national identity card, or a driver's license.

At the TRA office a TRA officer verifies that the traveler is carrying a suitable smart phone and asks the traveler to install a DTW on the smart phone if one is not already installed. In embodiments where the DTW is provided by the TCA, the DTW may be downloaded from a TRA computer located in the TRA office over a secure wireless network. In other embodiments the DTW is downloaded over the Internet through a secure connection.

The TRA officer operates a TRA console equipped with a data entry terminal, a camera, and a scanner for reading QR codes or bar codes. The officer uses the terminal to enter the traveler data, as well as traveler contact information such as an email address or a phone number where the traveler can receive text messages, into a registration record. Then the TRA officer asks the traveler to operate the DTW to generate a random high-entropy registration code. The DTW generates the registration code, displays it on the screen of the smart phone as a QR code or bar code, and retains it for later use. The officer scans the registration code into the console, which derives an encryption key and a retrieval key from the registration code using a key derivation function such as HKDF, then deletes the registration code. The retrieval key is universally unique with high probability because the registration code is generated at random with high entropy. The officer operates the console camera to acquire an image of the face of the traveler, which the console encrypts by means of a symmetric encryption algorithm such as AES using the encryption key. The console adds the encrypted facial image and the retrieval key to the registration record and deletes the plaintext facial image and the encryption key. Then the console sends the registration record to the TCA over a secure connection.

The TCA stores the registration record in a database, where the retrieval key can be used as a database primary key to retrieve the record. The facial image is not at risk of capture in the event of a breach of the database, because it is encrypted and the symmetric encryption-and-decryption key can only be derived from the registration code, which can only be found in the traverler's smart phone. As an additional precaution, the registration code is only stored in the database for a limited time, while waiting for the traveler data to be verified and the DTC to be issued. The record is deleted if verification fails, or after issuance, or when the time limit is reached if issuance has not taken place for any reason.

The TCA verifies the traveler data, then uses the contact information in the registration record to send a message notifying the traveler that the DTC is ready to be issued. Upon receiving the message, the traveler operates the DTW to request issuance of the DTC. If the DTW is not specific to a particular DTC, the traveler tells the DTW what TCA to use by entering a URL of the TCA or selecting the TCA from a menu built into the DTW. The DTW sends a request to issue the DTC to the TCA over the secure connection, conveying the registration code. The TCA derives the retrieval key and the encryption key from the registration code, uses the retrieval key to retrieve the registration record from the database, and uses the encryption key to decrypt the facial image.

In some embodiments where a DTC comprises the facial image and a public key certificate containing a hash of the facial image as described above, the DTW generates a key pair comprising a public key and a private key before sending the request to issue the DTC to the TCA. The DTW includes the public key in the request along with the registration code, signs the request using the private key, and retains the private key. The TCA verifies the signature, computes a cryptographic hash of the facial image, constructs a preliminary data structure comprising the hash, the traveler data, the public key and metadata, signs the preliminary data structure, constructs the certificate by adding the signature to the preliminary data, sends the facial image and the certificate to the DTW over the secure connection, and deletes the registration record from the database. The DTW assembles and stores the DTC, which comprises the private key, the facial image and the certificate.

In embodiments where the DTC is a rich credential, the DTC is issued as described in US patent application 15/468,100.

2.4 Issuance of a DBP

The DTW obtains a DBP for a flight by accessing a server provided by the airline over a secure connection, using the DTC to authenticate to the airline.

In some embodiments where a DTC comprises the facial image and a public key certificate containing a hash of the facial image as described above, the DTW authenticates to the airline with one-factor cryptographic authentication by sending the certificate and proving possession of the private key. To protect the traveler's privacy, the facial image is not sent. It does not need to be sent for one-factor cryptographic authentication because it is not included in the certificate.

In some of the above embodiments where the certificate is more specifically an X.509 certificate and the secure connection is more specifically a TLS connection, the DTW authenticates to the airline during the TLS handshake by using the certificate in the role of a TLS client certificate.

In some embodiments where the DTC is a rich credential, the DTW authenticates to the airline using the rich credential with one-factor cryptographic authentication only.

2.5 Credential revocation

In some embodiments, a DTC is revoked by placing its serial number in a credential revocation list signed by the TCA, a.k.a. a certificate revocation list (CRL) in embodiments where the credential comprises a certificate, and verifiers check for revocation by obtaining the latest copy of the CRL, verifying the signature, and looking up the serial number in the list

In other embodiments credential verifiers check whether a DTC has been revoked by querying a server made available by the TCA using an online credential status protocol, a.k.a. an online certificate status protocol (OCSP) in embodiments where the credential comprises a certificate, and obtaining a signed response stating whether the credential has been revoked or is still valid.

In other embodiments the TCA and the credential verifiers are nodes of a distributed ledger protocol with on-ledger storage (or a blockchain with on-chain storage as a specical case), as described in US patent application 15/599,249. The TCA revokes a DTC by issuing a ledger transaction with an instruction to store the serial number of the DTC in a revocation store that the TCA controls, and the verifiers check for revocation by looking up the serial number, each in its local copy of the revocation store. As the order of transactions does not matter, in other embodiments a gossip protocol is used as an unordered distributed ledger instead of a traditional ordered ledger. In some such embodiments the gossip protocol is more specifically an orchestrated gossip protocol, where nodes discover neighbors by requesting lists of neighbors from trusted orchestrators.

In some embodiments the DBP is issued shortly before the flight and is not subject to revocation because it is only valid for a short period of time, which terminates when the flight takes off or is canceled.

2.6 Presentation of the DTC and the DBP at the security checkpoint

In some embodiments the traveler authenticates at the security checkpoint by operating the DTW to present the DTC and a DBP to a security console over a wireless connection initiated by the DTW.

The connection is secured using keys for encryption and message authentication derived from a shared secret that is established using a key exchange protocol such as Diffie-Hellman or ECDH, where each party (the phone and the console) has a key pair comprising a private key and a public key, sends its public key to the other party and computes the shared secret from the other party's public key and its own private key. To prevent a man-in-the-middle attack that might cause the credentials to be sent to the attacker rather than to the security console, the DTW authenticates the console by verifying that the public key of the console, or a cryptographic hash of data including the public key of the console, agrees with an authentic value of the public key, or with an authentic value of the cryptographic hash, obtained from a trusted source. In some embodiments the authentic value is contained in a data structure that is encoded as a QR code or bar code affixed to the console or presented by the console on a computer display.

In some embodiments the wireless connection is a Bluetooth connection with unilateral OOB pairing as described in [2, §2.3.5.6.4]. In such embodiments the cryptographic hash to be compared to the authentic value is Cb = f4(Pkb,Pkb,rb,0), where f4 is a cryptographic hash function specified in [2, §2.2.6], Pkb (used as first and second arguments to the function f4) is the public key of the non-initiating device, i.e. the console, and rb is a random value chosen by the console. The QR code or bar code is an encoding of a data structure containing the Cb and the rb, which is presented on a computer display and changes from one authentication to the next.

After the secure connection has been established, the DTW submits the DTC and the DBP to the security console over the connection.

In some embodiments where the DTC comprises the facial image and a certificate comprising a hash of the facial image as described above, the DWP proves possession of the private key, e.g. by using it to sign a challenge, and sends the certificate, the facial image, and the DBP to the console. The console performs the following verifications: (i) it verifies the proof of possession of the private key using the public key contained in the certificate; (ii) it verifies the signature on the certificate using the public key of the TCA; (iii) it verifies that the DTC has not been revoked; (iv) it verifies the signature on the DBP using the public key of the airline; (v) it verifies that the DBP contains data that correctly identifies the DTC, such as the name of the TCA and the serial number of the DTC; and (vi) it verifies that the DBP is for a flight, identified by its date and flight code, that is scheduled to take off from the airport where the security checkpoint is located within a short period of time such as a few hours.

If all the verifications succeed, biometric authentication is performed by matching the face of the traveler to the facial image received from the smart phone by the console.

In some embodiments the biometric authentication is performed automatically, using a face recognition algorithm to compare the facial image to a photo of the traveler taken by a camera located on or near the console. In such embodiments the console may be unmanned, a security gate being opened automatically upon successful authentication.

In other embodiments the biometric authentication is performed visually by the security officer, who compares the face of the traveler to a display of the facial image received over the secure connection, which the console shows on a screen.

In other embodiments, the biometric authentication is performed both automatically and visually, for additional security.

In embodiments where visual authentication is performed, either by itself or in conjunction with automated face recognition, the visual authentication may be performed remotely in a security control room, by forwarding the photo taken by the camera and the facial image received by the console to side-by-side screens that are compared by the security officer. Upon successful verification, the officer remotely opens a security gate to let the traveler through.

2.7 Presentation of the DTC and the DBP at a boarding gate

In some embodiments the traveler authenticates at the boarding gate in the same manner as at the security checkpoint, by presenting the DTC and a DBP to a boarding console over a wireless connection, such as a Bluetooth connection with unilateral authentication of the console by means of Cb and rb values contained in a data structure that is encoded as a QR code or bar code presented on a computer display. The boarding console performs the same verifications as a checkpoint security console, and also verifies that the date and flight code contained in the DBP correspond to the flight being boarded at the gate.

References

[1] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008. `http://datatracker.ietf.org/doc/rfc5280/`.

[2] Bluetooth SIG. Bluetooth Core Specification version 5.1. Available from `https://www.bluetooth.com/specifications/bluetooth-core-specification/`.