Using Near-Field Communication for Remote Identity Proofing

Francisco Corella and Karen Lewison

October 29, 2016

Abstract

This is the third of a series of papers describing the results of a project whose goal was to identify five remote identity proofing solutions that can be used as alternatives to knowledge-based verification. This paper describes solutions 3–5, which use Near-Field Communication (NFC) technology for remote identity proofing. Each of the solutions uses a preexisting NFC-enabled hardware token designed for some other purpose as a credential in remote identity proofing. A native app running on an NFC-enabled mobile device serves as a relay between the NFC token and the remote verifier. The token is a contactless EMV payment card in Solution 3, a medical identification smart card in Solution 4, and a passport with an embedded RFID chip in Solution 5.

Contents

1 Introduction **2**

2 Solution 3—Remote proof of possession of a contactless EMV chip card **3**

2.1 Description of Solution 3 3

2.2 Security analysis of Solution 3 6

2.2.1 Adversarial capabilities 6

2.2.2 Verification factors 6

2.2.3 Threats and mitigations pertaining to Solution 3 7

2.2.4 Security posture of Solution 3 9

3 Solution 4—Remote identity proofing using a contactless medical identification smart card 9
3.1 Motivation . . . 10
3.2 Remark—Repurposing EMV technology as a possible shortcut to implementation . . . 10
3.3 Contents of a medical identification smart card . . . 11
3.4 Using a medical identification smart card for remote identity proofing . . . 11
3.5 Security analysis of Solution 4 . . . 13
3.5.1 Adversarial capabilities . . . 13
3.5.2 Verification factors . . . 13
3.5.3 Threats and mitigations pertaining to Solution 4 . . . 13
3.5.4 Security posture of Solution 4 . . . 14

4 Solution 5—Remote Identity Proofing with an e-Passport 15
4.1 Security analysis of Solution 5 . . . 17
4.1.1 Adversarial capabilities . . . 17
4.1.2 Verification factors . . . 17
4.1.3 Threat and mitigation pertaining to Solution 5 . . . 18
4.1.4 Security posture of Solution 5 . . . 18

5 Acknowledgments 19

List of Figures

1 Solution 3 . . . 4
2 Solution 4 . . . 12
3 Solution 5 . . . 16

1 Introduction

This is the third of a series of papers on the results of the research project on *remote identity proofing* [1] that we are currently finalizing. See also a series of posts in the Pomcor blog at `https://pomcor.com/blog/` that summarize and discuss the results.

The outcome of the project has been a set of five remote identity proofing solutions that can be used as alternatives to knowledge-based verification.

Solution 1, described in [2], relies on a *rich credential* to provide three-factor verification of the identity of a subject to a verifier that has no prior relationship with the subject. Solution 2 uses an adaptation of the rich credential that takes advantage of the blockchain to greatly simplify the process of validating the credential against a public key infrastructure. This paper describes the remaining three solutions.

Solutions 3, 4 and 5 use Near-Field Communication (NFC) technology for remote identity proofing. This is paradoxical since, as its name indicates, NFC is designed for short-range transmissions, and by remote identity proofing we mean identity proofing over the Internet. Each of the solutions uses a preexisting NFC-enabled hardware token designed for some other purpose as a credential in remote identity proofing. A native app running on an NFC-enabled mobile device serves as a relay between the NFC token and the remote verifier. The token is a contactless EMV payment card in Solution 3, a medical identification smart card in Solution 4, and a passport with an embedded RFID chip in Solution 5.

Both Android and iOS devices are NFC-enabled. However, iOS only supports NFC Card-Emulation mode (and, furthermore, NFC functionality is not accessible to app developers). Therefore using a native app on an iOS device as a relay in solutions 3–5 requires a hardware accessory that adds NFC reader functionality via the USB port.

2 Solution 3—Remote proof of possession of a contactless EMV chip card

2.1 Description of Solution 3

In this solution, illustrated in Figure 1, the subject proves possession of a contactless EMV chip card that has not been reported lost, stolen or otherwise compromised. The card carries standard attributes such as the cardholder's name and address and the Primary Account Number (PAN) of the card's account, which the verifier obtains by asking the card's payment network to authorize a small charge to the account. If the issuing bank provides identity services, the verifier may be able to obtain additional attributes placed on the card by the issuing bank, or retrieved from the bank.

A key aspect of the solution is that the subject proves possession of the card *remotely*. This is accomplished by using a native app running on an

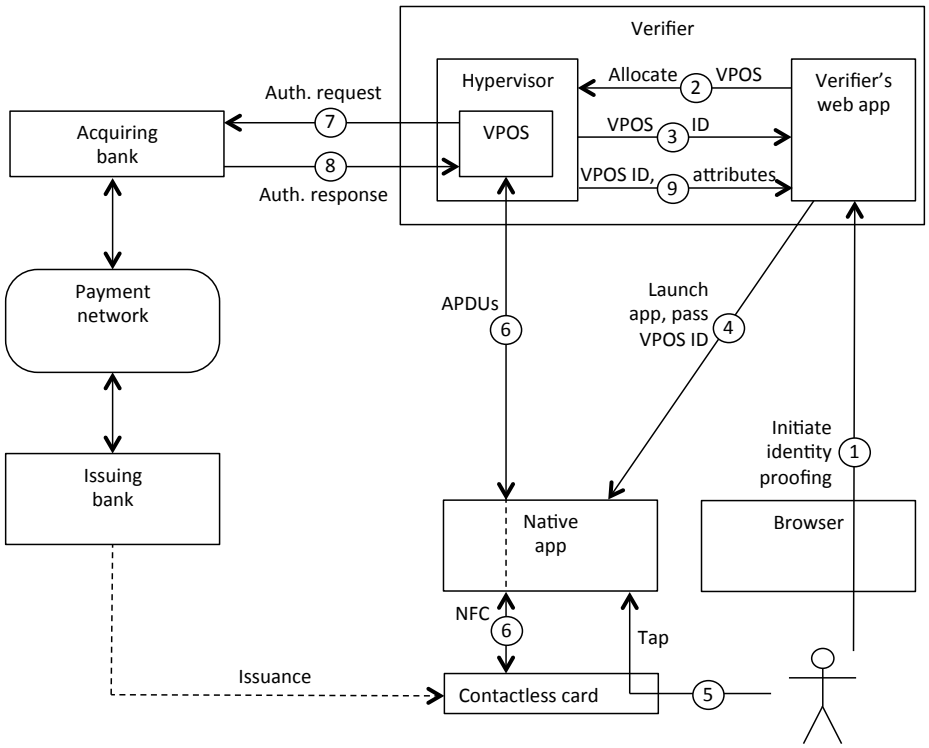

Figure 1: Solution 3

NFC-enabled mobile device in the subject's possession to relay Application Protocol Data Units (APDUs) from the contactless card to point-of-sale (POS) software running in the verifier's site over a TLS connection through the Internet. Such relaying has been used in relay attacks against NFC payment systems, but is used here for benign purposes.

A difficulty with this solution is that ordinary POS software is designed for handling one payment transaction at a time, but the verifier may need to process multiple identity proofing requests simultaneously. This difficulty can be overcome by modifying existing POS software so that it does not have this limitation or, more readily, by running POS software under a POS hypervisor that spawns a virtual point-of-sale (VPOS) for each identity proofing request, or manages a pool of reusable VPOSes. Multiple VPOSes can then process multiple EMV transactions simultaneously, each appearing to the payment network as a separate POS unrelated to the others.

Figure 1 illustrates Solution 3, implemented using a POS hypervisor. The contactless EMV card is issued to the subject by an issuing bank in the usual way, and is used for remote identity proofing as follows:

(1) The subject uses a web browser to access a web application on the verifier's web site.

(2) The verifier's web app asks the POS hypervisor to allocate a VPOS.

(3) The POS hypervisor returns a VPOS ID that identifies the allocated VPOS to the verifier's web app.

(4) The web app launches a native app on a subject-controlled device with NFC-reader functionality, which may be the same device where the browser is running or a different device. The native app is launched for a different purpose but in the same manner as the native app used in Solution 1 for transmission of an audio-visual stream [2, Section 7]. The web app transmits the VPOS ID to the native app as it launches it.

(5) The native app prompts the subject to bring the card into the NFC field of the device, allowing the native app to interact with the card, emulating a payment terminal.

(6) The native app communicates with the card via NFC and relays the APDUs exchanged with the card through a TLS connection to the

allocated VPOS, identified by the VPOS ID.

(7) The VPOS sends an authorization request to the issuing bank via the verifier's acquiring bank and the payment network.

(8) The issuing bank returns an authorization that travels back by the reverse route to the VPOS. The VPOS informs the web app that the authorization has been granted, and passes the subject's attributes revealed by the transaction to the web app.

2.2 Security analysis of Solution 3

2.2.1 Adversarial capabilities

Adversarial capabilities applicable to all five solutions are discussed in the general threat model of [2, Section 8.1]. An adversary against Solution 3 has the following specific *NFC attack capabilities*:

NFC eavesdropping. While NFC is a short distance protocol, intended to work over distances of a few centimeters, it is possible to eavesdrop on NFC communications from a distance of several meters [3].

NFC relay attack. In a relay attack [4], the adversary surreptitiously relays traffic between an NFC target device such as a smart card or an RFID chip and a remote reader by bringing an NFC initiator device such as an Android phone near the target device. The initiator device exchanges APDUs with the target device via NFC and relays those APDUs to a remote reader over the Internet.

NFC eavesdropping is no different from other network eavesdropping and can be mitigated by encryption. But it deserves to be mentioned because it is often not mitigated. The EMV contactless protocols, in particular, do not encrypt the NFC channel. (Some vendors of payment solutions tout end-to-end encryption, but they can only encrypt traffic between the point-of-sale and the merchant's payment processor or the acquiring bank. Traffic between the point-of-sale and the card via NFC is not encrypted.)

2.2.2 Verification factors

As described so far, Solution 3 provides only one verification factor, "something that the subject has", viz. the contactless card. But two options are

available for strengthening the solution with additional verification factors.

The first option is to take advantage of the *Dynamic Data Authentication (DDA)* of the EMV Specifications [5, Section 6.5]. An EMV card configured to perform Dynamic Data Authentication (DDA) holds an RSA private key and a certificate signed by the issuing bank binding the associated public key to card data, which the card presents to the terminal with a proof of possession of the private key. If the issuing bank included a facial image in the card data, the verifier could match the image against an audio-visual stream of the subject reading prompted text while performing spoofing detection, as in Solution 1 [2, Section 7]. This would add a "something that the user is" biometric verification factor to the solution. (The facial image could also be displayed on a merchant's terminal during in-store payments, increasing the security of card-present transactions in brick-and-mortar stores without inconveniencing the customer or adding latency to the transactions.) The EMV specifications also have a provision, not used in the US but commonly used elsewhere, for verifying a PIN entered when the card is used for payment. Such a PIN could also be used in remote identity proofing, providing full three-factor verification with "something that the subject has", "something that the subject knows", and "something that the subject is".

The second option is to ask the subject to find and report the amount of the authorization transaction after logging in to the issuing bank's web site. Multiple authorization transactions could be used to increase the entropy. This would provide proof of ownership of the card's account as an additional verification factor.

If the first option is not used, Solution 3 does not require the subject to submit a biometric sample. It is then well suited to be combined with any of the other solutions, all of which include biometric verification.

2.2.3 Threats and mitigations pertaining to Solution 3

Threat 1

An adversary carries out a relay attack to impersonate the subject. The adversary executes the card presentation protocol of Figure 1 using the contactless card of the subject without the subject being aware that the card is being used, by coming near the subject while the card is in the subject's wallet and using an NFC initiator device such as an Android phone to relay APDUs between the card and the native app of Figure 1, which is controlled

by the attacker. Notice that two relays take place in this attack scenario.

Mitigation of Threat 1

There is no general purpose mitigation for a relay attack against the existing EMV contactless protocols. The *distance bounding defense* of [6] requires modification of the protocol and the card. The specific attack against Solution 3 can be mitigated by asking the subject to report the amount of the one or more authorization transactions that the verifier has obtained from the payment network. As noted above in Section 2.1, this amounts to using proof of ownership of the card's account as an additional verification factor.

Threat 2

A physical attacker steals the contactless card and uses it to impersonate the subject.

Mitigation of Threat 2

Asking the subject to report the amounts of the authorization transactions also provides mitigation against Threat 2.

Threat 3

An adversary eavesdrops on the unencrypted NFC communication between the contactless card and the native app of Figure 1. The data that can be obtained by this attack does not allow the attacker to impersonate the subject, because in a payment or authorization transaction the card authenticates by signing a challenge with a symmetric key that the card shares with the issuing bank and does not leave the card. (This is true in both modes of operation specified by the EMV contactless specifications [7], called *EMV mode* and *mag-stripe mode*.) But the attacker obtains the subject's attributes carried in the card and revealed to the verifier, which is a violation of the subject's privacy.

Instead of eavesdropping, the attacker can obtain data from the card by interacting with the card as in a relay attack. But eavesdropping can be done from farther away because the attacker does not have to interact with the card [3].

Lack of mitigation of Threat 3

We do not have a mitigation for Threat 3. However the privacy risk incurred by the subject from Threat 3 when using the contactless card for remote identity proofing is no different from the privacy risk the he or she incurs by tapping the card on a contactless payment terminal.

2.2.4 Security posture of Solution 3

The security posture of Solution 3 can be summarized as follows:

- An adversary can impersonate the subject by stealing the subject's contactless card or performing a relay attack. This can be mitigated by asking the subject to report the amounts of the authorizations obtained by the verifier in the course of the identity proofing event, which requires the subject to log in to the web site of the issuing bank and access the card's account.

- An adversary can obtain the subject's attributes by eavesdropping on the NFC communications that take place during the identity proofing event or by interacting with the card as in a relay attack. However eavesdropping, or interacting with the card without relaying, does not allow the adversary to impersonate the subject vis-à-vis a verifier.

- A subject can repudiate participation in a remote identity proofing event by claiming he or she was the unwitting victim of an NFC relay attack, a believable claim. If the mitigation of threats 1 and 2 is used, the subject must also claim that he or she was impersonated vis-à-vis the web site of the issuing bank. Both claims together may not be believable.

3 Solution 4—Remote identity proofing using a contactless medical identification smart card

In this solution, the NFC-enabled hardware token is a smart card containing a private key and a public key certificate that binds the associated public key to attributes of the subject and to a facial image of the subject. For the sake

of specificity, we assume that the card is a medical identification card, but any other identification card containing such data could be used similarly.

3.1 Motivation

A year ago, the Medicare Access and CHIP Reauthorization Act [8] instructed the Secretary of Health and Human Services to consider the use of smart cards as Medicare beneficiary and provider cards. As patients travel and often receive care from providers with whom they may not have a prior relationship, there is a glaring need for a uniform means of patient identification across the health care industry. A Medicare smart card could be the first step towards a nationwide patient identification system. This would not necessarily require interoperable medical records or a uniform system of medical record numbers; only the smart card technology and a few attributes carried on the card would have to follow a medical identification smart card standard. In Solution 4 we assume that such a nationwide patient identification system will eventually exist.

3.2 Remark—Repurposing EMV technology as a possible shortcut to implementation

Although EMV technology is very specifically intended and designed for payment transactions, we believe that it may be possible to repurpose it for the implementation of medical identification smart cards. The use of EMV technology to that purpose would simplify and accelerate the implementation of a nationwide patient identification system by leveraging a small portion of the EMV standards and the ecosystem that is in place for implementing EMV smart card technology. It would also make it easy to combine a credit card and a medical ID in a single smart card. That would be convenient for patients, and if such a combined card were used for the purpose of identity proofing, it would allow the subject to provide evidence originating from two identity sources by presenting a single credential.

An EMV card implements two cryptographic protocols that are mostly independent of each other: (i) a protocol based on symmetric cryptography, in which the card signs a request that is verified by the issuing bank using a key shared with the card, the symmetric signature being known as a cryptogram; and (ii) a protocol based on asymmetric cryptography (RSA signatures) in

which the terminal verifies a signature received from the card, that protocol being known as Offline Data Authentication. There are three versions of Offline Data Authentication. In Static Data Authentication (SDA), the signature covers static data and is computed by the issuing bank when the card is issued. In Dynamic Data Authentication (DDA), the signature is computed with a private key carried in the card, and covers a challenge sent by the terminal in addition to static card data. In Combined DDA/Application Cryptogram Generation (CDA), the signature covers a cryptogram in addition to a challenge by the terminal and static card data; CDA is the only aspect of the technology in which the symmetric and asymmetric protocols interact.

EMV payment processing is very complex, but offline data authentication is relatively simple, and that is all that is required to implement a medical identification smart card. DDA could be used to implement a smart card, leveraging existing EMV software development kits.

3.3 Contents of a medical identification smart card

We envision that a future medical identification smart card standard will specify that a medical identification smart card must contain a private key and a public key certificate that binds the associated public key to attributes of the subject and to a facial image of the subject.

To mitigate the risk of exposing medical data, the attributes carried in the card should include a card identifier and a minimal set of biographic and insurance data, but no medical data. The card identifier should not be the medical record number. Qualified medical personnel will be able to access the medical record number and other medical data by means of the card identifier, but a non-medical party such as a medical insurer of the verifier in a remote identity proofing event should not be allowed to do so.

3.4 Using a medical identification smart card for remote identity proofing

A medical identification smart card with the above contents could be used by a patient, in the role of subject, to prove his/her identity to a remote verifier. The verifier would obtain the patient's name and biographic data from the card, and could use the card identifier to obtain additional attributes from the card issuer if the card issuer agreed to provide an identity service.

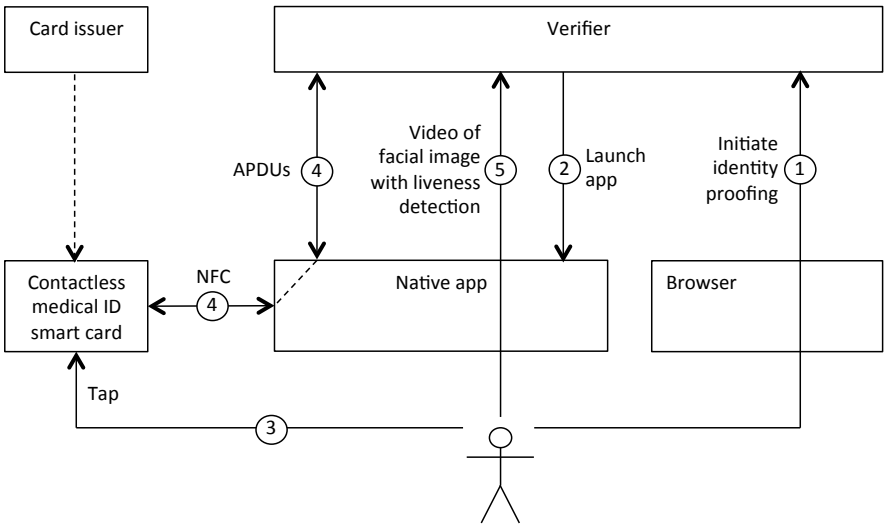

Figure 2: Solution 4

Figure 2 illustrates how the patient identifies him/herself to the verifier. The process comprises the following steps:

(1) The subject uses a web browser to access a web application on the verifier's web site.

(2) The web app launches a native app on a subject-controlled device with NFC-reader functionality, which may be the same device where the browser is running or a different device. The native app is launched as described in [2, Section 7] in connection with Solution 1.

(3) The native app prompts the subject to bring the card into the NFC field of the device, allowing the native app to interact with the card.

(4) The native app communicates with the card via NFC and relays the APDUs exchanged with the card through a TLS connection to the verifier. The native app sends the public key certificate containing the facial image to the verifier, and proves possession of the private key by signing a challenge. This can be accomplished by executing the EMV DDA protocol if EMV technology is repurposed to implement medical identification smart cards as suggested above in Section 3.2.

(5) As in Solution 1, the native app submits to the verifier an audio-visual stream of the subject reading prompted text. The verifier matches the face in the video to the facial image in the certificate, uses speech recognition technology to verify that the subject is reading the text that was prompted, and verifies that the audio and video channels of the stream are in synchrony by matching distinguishable visemes in the video channel to phonemes in the audio channel.

3.5 Security analysis of Solution 4

3.5.1 Adversarial capabilities

Adversarial capabilities applicable to all five solutions are discussed in the general threat model of [2, Section 8.1]. An adversary against Solution 4 has the NFC attack capabilities described above in conjunction with Solution 3.

3.5.2 Verification factors

Solution 4 provides two verification factors: possession of the card, and facial recognition.

3.5.3 Threats and mitigations pertaining to Solution 4

Threat 1

An adversary steals the medical identification smart card and uses it to initiate a remote identity proofing event with the verifier. This does not allow the adversary to impersonate the subject, since Solution 4 is a two-factor verification solution. But the native app of Figure 2, controlled by the adversary, obtains the certificate containing the subject's attributes and facial image, which is a violation of the subject's privacy.

Mitigation of Threat 1

The card requires entry of a PIN to initiate the remote identity proofing protocol. The subject supplies the PIN via the native app.

Threat 2

An adversary initiates a relay attack as in Threat 1 against Solution 3, by coming near the subject while the card is in the subject's wallet and using a smart phone to relay traffic APDUs between the card and the native app of Figure 1, which is controlled by the attacker. The attacker is not able to impersonate the subject, but obtains the certificate containing the subject's attributes and facial image as in the Threat 1 scenario.

Mitigation of Threat 2

The mitigation of Threat 1 applies to Threat 2 as well.

Threat 3

An adversary obtains the certificate containing the subject's attributes and facial image by eavesdropping on the NFC communication between the card and the native app of Figure 2.

Mitigation of Threat 3

Eavesdropping can be prevented by encrypting the NFC channel between the card and the native app. Since the adversary is passive, this can be achieved with a shared key established using an unauthenticated Diffie-Hellman (DH) or Elliptic-Curve Diffie-Hellman (ECDH) key exchange.

We would like to point out that simple unauthenticated DH or ECDH could similarly be used to establish a shared key for encryption of the NFC communications of a PIV or CAC card, instead of the more complex OPACITY-based protocol described in [9, Section 4.1].

3.5.4 Security posture of Solution 4

The security posture of Solution 4 can be summarized as follows:

- To impersonate the subject, an adversary must perform a relay attack or steal the card, and submit an audio-visual stream that circumvents spoofing detection by the verifier.
- If a PIN is not required to enable use of the card, an adversary may be able to obtain the subject's attributes and facial image carried in

the card by stealing the card, or by initiating a relay attack even if the attack does not succeed.

- If the NFC channel is not encrypted, an adversary may be able to eavesdrop on a remote identity proofing event and obtain the subject's attributes and facial image carried in the card.

- A subject may be able to repudiate participation in a remote identity proofing event by claiming he or she was the unwitting victim of an NFC relay attack by an adversary who succeeded in defeating the anti-spoofing measures of the verifier. As a defense against fraudulent repudiation, the verifier may record the audio-visual stream submitted by the subject, and ask the subject to include time and space clues in the stream.

4 Solution 5—Remote Identity Proofing with an e-Passport

Since 2007, the US State Department issues Electronic Passports, or e-Passports [10], that carry an RFID chip and conform to the International Civil Aviation Organization (ICAO) standard [11]. The RFID chip in an e-Passport carries the same biographic data that is printed on the passport, a digital facial image, and a digital signature that applies to the biographic data and the image. Passport cards and enhanced driver's licenses also carry an RFID chip, but they do not conform to the ICAO standard, and the only data in the chip is a reference to a record in a database managed by the US Customs and Border Patrol (CBP) [12].

The RFID chip does not contain a public key certificate and its associated private key, but it contains symmetric keys for encryption and for computation of message authentication codes (MACs), which are obtained by hash-based key derivation from data printed in the Machine Readable Zone (MRZ) of the passport, specifically the passport number, the date of birth and the expiration date, each including a check digit [13, Section 4.3.2]. Extracting the data stored in the chip requires reading the printed data, deriving the keys, and executing a challenge-response protocol with the chip [13, 4.3.1]. This prevents *skimming* the data, i.e. reading it by bringing an NFC initiator near the passport. The challenge-response protocol also gen-

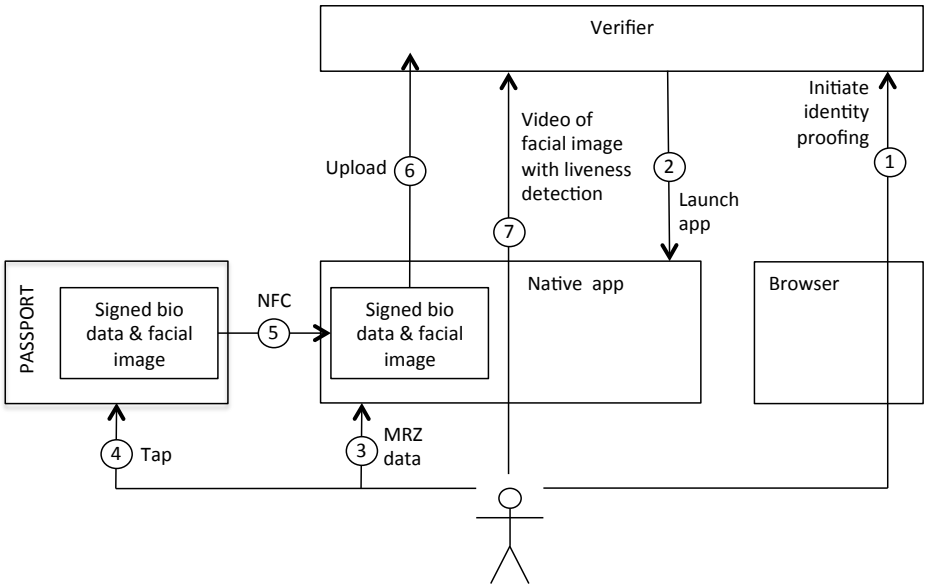

Figure 3: Solution 5

erates session keys for encryption and authentication of NFC traffic, which protects the confidentiality of the data against eavesdropping on the NFC channel.

Figure 3 shows how a subject can use an e-Passport for remote identity proofing. The process comprises the following steps:

(1) The subject uses a web browser to access a web application on the verifier's web site.

(2) The web app launches a native app on a subject-controlled NFC-enabled device with NFC-reader functionality, which may be the same device where the browser is running or a different device. The native app is launched as described in [2, Section 7] in connection with Solution 1.

(3) The subject uses the native app to scan the MRZ of the passport, or types the relevant MRZ data (passport number, birth date and expiration date) into the app.

(4) The subject brings the RFID chip embedded in the passport into the NFC field generated by the NFC-enabled device.

(5) The native app uses the MRZ data to execute the challenge-response protocol with the RFID chip, then reads the biographic data, facial image and signature from the chip.

(6) The native app creates a file with the signed biographic data and facial image and uploads the file over a TLS connection to the verifier, which verifies the signature.

(7) As in solutions 1 and 4, the native app submits to the verifier an audio-visual stream of the subject reading prompted text. The verifier matches the face in the video to the facial image in the RFID data, uses speech recognition technology to verify that the subject is reading the text that was prompted, and verifies that the audio and video channels of the stream are in synchrony by matching distinguishable visemes in the video channel to phonemes in the audio channel.

4.1 Security analysis of Solution 5

4.1.1 Adversarial capabilities

Adversarial capabilities applicable to all five solutions are discussed in the general threat model of [2, Section 8.1]. An adversary against Solution 5 has the NFC attack capabilities described above in conjunction with Solution 3.

4.1.2 Verification factors

Solution 5 provides two verification factors: possession of the passport, and facial recognition. However, the evidence used to verify possession of the passport is weak because there is no private key in the RFID chip. Instead of relying on a proof of possession of a private key that never leaves the chip, the verifier can only rely on presentation of the signed data as a bearer token. This exposes the proofing process to the threat described below. That threat, however, is not dire and only concerns the reduction of the number of factors from 2 to 1. Even if the adversary is able to obtain the signed data, he/she still faces the obstacle of spoofing the audio-visual stream of the subject reading prompted text.

4.1.3 Threat and mitigation pertaining to Solution 5

Threat 1

An adversary uses social engineering to obtain the MRZ data needed to execute the challenge-response protocol with the RFID chip, and uses it to skim the signed biographic data and facial image from the chip. The adversary still has to spoof an audio-visual stream of the subject reading prompted text in order to impersonate the subject.

The social engineering needed to obtain the MRZ is challenging because passports are rarely used for purposes other than to cross borders. But they are sometimes used for other purposes, such as proving citizenship or date of birth.

Mitigation of Threat 1

The verifier can obtain stronger evidence of possession of the password by asking the subject to show the data page of the password in the audio-visual stream that he/she submits to the verifier, and checking for the presence of visual security features on the page. Such stronger evidence, however, is still not as strong as a cryptographic proof of possession of a private key.

4.1.4 Security posture of Solution 5

The security posture of Solution 5 can be summarized as follows:

- To impersonate the subject, an adversary who is not in possession of the passport must obtain the MRZ data printed on the data page, load it into a smart phone with NFC-reader capability, and bring the smart phone near the passport in order to skim the signed biographic data and facial image from the RFID chip embedded in the passport; and submit an audio-visual stream that circumvents spoofing detection by the verifier.

- A subject may try to repudiate participation in a remote identity proofing event by arguing that an adversary had captured the passport before the event, and succeeded in defeating the anti-spoofing measures of the verifier. As a defense against fraudulent repudiation, the verifier may record the audio-visual stream submitted by the subject, and ask the subject to include time and space clues in the stream.

5 Acknowledgments

This paper is the result of a project sponsored by an SBIR Phase I grant from the US Department of Homeland Security. It does not necessarily reflect the position or the policy of the US Government.

We are very grateful to Prof. Phil Windley for many comments on project working documents.

References

[1] Francisco Corella. Pomcor Receives DHS Grant to Look for Alternatives to Knowledge-Based Verification for Remote Identity Proofing. Pomcor blog post, August 3, 2016. https://pomcor.com/2016/08/03/pomcor-receives-dhs-grant-to-look-for-alternatives-to-knowledge-based-verification-for-remote-identity-proofing/.

[2] Karen Lewison and Francisco Corella. Rich Credentials for Remote Identity Proofing. Pomcor technical report, October 15, 2016. https://pomcor.com/techreports/RichCredentials.pdf.

[3] G. P. Hancke. Eavesdropping Attacks on High-Frequency RFID Tokens. In *Proceedings of the 4th Workshop on RFID Security (RFIDsec08)*, July 2008. http://www.rfidblog.org.uk/Hancke-RFIDsec08-Eavesdropping.pdf.

[4] Gerhard Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. January 2005. http://rfidblog.org.uk/hancke-rfidrelay.pdf.

[5] EMVCo, LLC. EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3. https://www.emvco.com/download_agreement.aspx?id=653.

[6] S. Drimer and S. J. Murdoch. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. In *USENIX Security Symposium*, 2007. https://www.usenix.org/legacy/events/sec07/tech/drimer/drimer.pdf.

[7] EMVCo. EMV Contactless Specifications. https://www.emvco.com/specifications.aspx?id=21.

[8] US Congress. Medicare Access and CHIP Reauthorization Act of 2015. https://www.congress.gov/bill/114th-congress/house-bill/2/text.

[9] David Cooper, Hildegard Ferraiolo, Ketan Mehta, Salvatore Francomacaro, and Ramaswamy Chandramouli. Special Publication 800-73-4—Interfaces for Personal Identity Verification—Part 2: PIV Card Application Card Command Interface. All three parts of SP 800-73-4 are placed together in a single file available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf.

[10] Department of Homeland Security. e-Passports. https://www.dhs.gov/e-passports.

[11] International Civil Aviation Organization (ICAO). Document 9303. http://www.icao.int/publications/pages/publication.aspx?docnum=9303.

[12] Department of State. Card Format Passport; Changes to Passport Fee Schedule. Federal Register Volume 71, Number 200 (Tuesday, October 17, 2006). https://www.gpo.gov/fdsys/pkg/FR-2006-10-17/html/E6-17237.htm.

[13] International Civil Aviation Organization (ICAO). Document 9303, Part 11. http://www.icao.int/publications/Documents/9303_p11_cons_en.pdf.