Three Taps for Secure Machine-to-Machine Communication: Towards High Assurance yet Fully Local Machine Pairing

Sibylle Fröschle
Hamburg University of Technology
Hamburg, Germany
sibylle.froeschle@tuhh.de

Martin Kubisch
Airbus CRT
Munich, Germany
martin.kubisch@airbus.com

ABSTRACT

In this short paper we explore if and how we can securely pair up two machines for secure machine-to-machine communication by means of an NFC system subject to two conditions: firstly, the machine pairing method must be truly local in that we cannot rely on long-term secrets or a public-key infrastructure; secondly, the machine pairing method must be verifiable and certifiable to a high assurance level. We address this question motivated by a demand for this in the aerospace domain, where there is currently a drive to introduce machine-to-machine communication over wireless networks to improve ground processes such as refuelling and air conditioning. In this paper we present preliminary results towards a positive answer to this question.

CCS CONCEPTS

• **Security and privacy** → **Security protocols**; **Formal methods and theory of security**; • **Computer systems organization** → **Embedded and cyber-physical systems**.

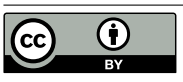
KEYWORDS

Cyber-Physical Systems; NFC; Key Establishment; Distance Bounding; Formal Models and Verification; High Assurance; Resilience

ACM Reference Format:
Sibylle Fröschle and Martin Kubisch. 2024. Three Taps for Secure Machine-to-Machine Communication: Towards High Assurance yet Fully Local Machine Pairing. In *Proceedings of the Sixth Workshop on CPS&IoT Security and Privacy (CPSIoTSec'24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3690134.3694824

1 INTRODUCTION

There is currently a drive in the aerospace domain to adopt machine-to-machine communication over wireless networks to improve ground processes at airports such as refuelling and pre-conditioning. This brings with it the challenge of how to bootstrap a secure communication channel between the aircraft and a ground unit such as a fuel truck or a pre-conditioning unit. Since the aircraft and the ground unit belong to different security domains they a priori do not share a common security context. And without the context of a pre-shared secret or a public-key infrastructure it is not possible to securely establish a session key over an open channel.



CPSIoTSec'24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-1244-9/24/10.
https://doi.org/10.1145/3690134.3694824

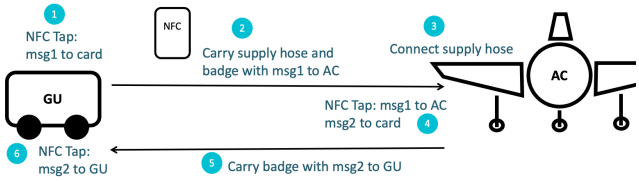


Figure 1: Pairing up a ground unit and an aircraft

For unauthenticated key establishment protocols such as the Diffie-Hellman key exchange (or a post-quantum KEM approach) we at least require an authenticated channel.

This challenge is well-known to the IoT community, where it is very common that devices with no prior security context need to be set up for secure communication in an ad hoc fashion. The solution is often provided by employing secure device pairing (SDP) [19]. The idea behind SDP is to make use of the proximity of the devices to obtain an out-of-band (OoB) channel, over which information can be confirmed in an authenticated manner. The OoB channel is often realized with the help of a user. For example, in Bluetooth pairing with numeric comparison a 6-digit number is displayed, which must be confirmed by the user. Alternatively, the OoB channel is realized by a short-range physical channel such as NFC. However, for such types of OoB channels authenticity cannot be validated to the high assurance level that is required in our setting of safety-critical machine-to-machine communication.

Hence, in this short paper we explore if and how we can lift secure device pairing to high assurance machine pairing. Can we securely set up a session key between two machines subject to the following two conditions? Firstly, the machine pairing method must be truly local in that we cannot rely on a prior security context between the two machines. And secondly, the machine pairing method must be verifiable and certifiable to a high assurance level. To this end we explore whether *TAGA — a Touch and Go Assistant in the Aerospace Domain* can be realized without requiring any common security context between aircraft and ground units.

The idea is that the operator pairs the ground unit (GU) and the aircraft (AC) by means of an NFC system, and in line with setting up the service hose. The GU and the AC are both equipped with an NFC reader, and the operator holds an NFC card. The course of the pairing method is illustrated in Fig. 1. The operator starts off the pairing by an initial NFC tap at the GU reader. Thereby a first message M_1 is transferred to the card. The operator then carries the supply hose and the card to the AC. They first connect the supply hose, and then tap the AC reader with the card. During the tap the first message M_1 is read from the card to the AC reader, and

a second message M_2 is written from the reader to the card. The operator then walks back to the GU. On arrival they perform a final tap, and thereby transfer the second message M_2 to the GU reader. Then the operator switches on the supply to the ground process, such as the fuel pump or air supply. As a result the GU and AC have exchanged two messages, and the physical setup of the ground process is complete.

We will instantiate the two messages according to the basic Diffie-Hellman exchange. But principally, the messages of any two-pass key establishment protocol can be exchanged in this way. The pairing method is carried out in the secure zone of the turnaround, where only authorized personnel are present. Indeed, the latter benefit stands behind the hypothesis that TAGA might provide a suitable OoB channel despite the well-known attacks against NFC transmission, e.g. in the context of contactless EMV payment cards [24, 26].

Our contributions are as follows: (1) We identify that TAGA provides a 3-tap pairing method to pair up machines with minimal user interaction and in line with other setup procedures. (2) We demonstrate that the prototype of the pairing method is still amenable to person-in-the-middle attacks. We systematically elicit the attack vectors and derive an attacker model that incorporates an NFC attacker that is powerful but falls just short of the standard Dolev-Yao attacker. (3) We present the *Secure 3-Tap (S3T)* pairing method, which is designed to withhold such an attacker. We pinpoint and specify what channel authenticity means for the 3-tap method. We provide a preliminary semi-formal proof that the S3T method indeed guarantees channel authenticity. Altogether, we thereby arrive at a secure pairing scheme. Finally, we discuss ongoing work towards high assurance verification and provable resilience properties. The preliminary proofs are provided in the appendix. Part of this work further develops material of [13].

2 RELATED WORK

Secure Device Pairing (SDP) has been an active research field ever since it was put forward by Stajano and Anderson in 1999 (c.f. [19]). Moreover, SDP schemes have been widely adopted for IoT and personal devices. Mirzadeh et al. [23] review device pairing protocols and their security, including group device pairing. Fomichev et al. [9] provide terminology and foundations for a classification and comparison of existing SDP schemes, and a comprehensive survey thereof. Bluetooth is perhaps the most widely used protocol, which foresees SDP for key sharing [29]. We believe that the 3-tap method puts forward a new OoB channel, and a new type of application: it seems SDP has been less investigated and put to practice in the context of pairing up large machines of different security domains.

NFC has seen many security-relevant applications such as keyless entry systems, contactless EMV payment, transport ticketing, etc. Relay attacks [24] have been pinpointed as an attack that cannot be solved by cryptographic solutions. These attacks are highly relevant in that they are indeed used by criminals, e.g. against payment cards and to steal cars. This has led to a thorough investigation of how relay attacks can be practically mounted; we will review relevant insights in Section 3. The advent of NFC-enabled smartphones has brought new challenges. New attacks have been shown against mobile payment schemes [26]. And the NFC-enabled mobile phone has been realized as a platform to carry out attacks with reduced complexity [10]. In Section 3.1 we will add the idea and proof-of-concept of how to use a hacked phone as a malicious proxy in a secure zone.

We believe that our threat analysis and derived attacker model is new. While the works on payment now mainly concentrate on the execution of attacks with COTS equipment (as this is the yardstick of EMV [26]) we also consider earlier results on expert-designed leeches, and ghosts: our setting is not only safety-relevant but also concerns critical infrastructures. Moreover, we include current knowledge on attacks against ongoing NFC transmissions [15, 25]. (In this context it is important to note that the person-in-the-middle attack of [2] is not on this low level.) Our model of the NFC Intruder strikes a balance between overapproximation where precise knowledge is not available and still reflecting the limitations of the channel. This is crucial for the proof of our main theorem, i.e. Theorem 4.2.

Distance bounding (DB) protocols have been advocated as a countermeasure to relay attacks [7], and also as a neighbour dectection method in ad-hoc wirelss environments [1]. They have first been proposed by Brands and Chaum [5]. The Hancke and Kuhn protocol [14] is one of the most popular in the RFID world. It can also be improved with respect to the success probability relative to necessary rounds [17]. A survey is provided in [3]. As with all security protocols DB protocols are prone to subtle attacks, which has led to techniques for their formal verification [6, 22, 28]. This work applies DB protocols in a new context, and builds on the verification result of [22] on the Hancke and Kuhn protocol in the proof of Theorem 4.2. Moreover, we use DB in a new setting where a secure *proximate* zone is realistic, and if necessary enforceable by scanning equipment for tags. This might also make it possible to work with less tight distance bounds, which are hard to realize.

Integrating machine-to-machine communication in critical domains has to undergo a *safety and security engineering process*. In [11, 12] we address the overall process of how to engineer a key establishment method while considering both safety and security.

3 INVESTIGATING THE 3-TAP CHANNEL

3.1 Proof-of-Concept Attack

Even though the machine pairing takes place in the secure zone of the turnaround the attacker can infiltrate the secure zone via a proxy device and interact with the 3-tap channel. We have devised and demonstrated a proof-of-concept attack against the prototype of the 3-tap pairing scheme. Our attack shows that it is feasible to mount the well-known person-in-the-middle (PitM) attack against the Diffie-Hellman (DH) key exchange using the NFC-capable smartphone of the operator as a proxy. Our only assumption is that the operator is in the habit of storing the card in their pocket next to their phone while they walk from the GU to the AC and back. (They need both hands to carry the supply hose.) The attack is illustrated in Fig. 2.

In preparation, the attacker hacks the smartphone of the operator, and installs the attack code. This can be done in the usual way, e.g. by a Trojan app or a spear phishing email to the operator with a malicious link. The operator performs the first tap, and the GU writes its public DH key R_G on the card. Then the operator puts the

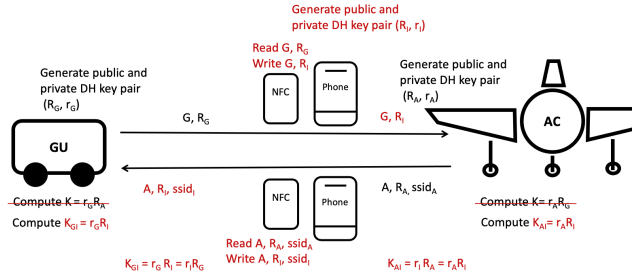


Figure 2: PitM attack via hacked smartphone

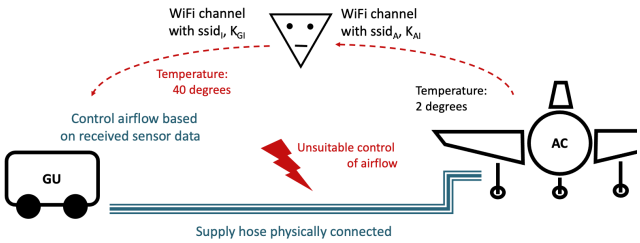


Figure 3: Impact of PitM attack for pre-conditioning

card in their pocket next to the hacked smartphone, and walks to the AC. The smartphone detects the tag and reads R_G from the card. The attacker has prepared their own DH private and public key pair (r_I, R_I), and the smartphone writes R_I to the card replacing R_G. When the operator performs the tap at the AC reader the reader receives the attacker's public DH key R_I rather than R_G. As usual the AC reader writes its own public DH key R_A and its SSID $ssid_A$ for the WiFi connection to the card. The operator puts the card back into their pocket next to the smartphone and walks back to the GU. The smartphone reads R_A and $ssid_A$ from the card, and writes the attacker's public DH key R_I and their own SSID $ssid_I$ to the card. When the operator peforms the final tap at the GU the GU reader receives the attacker's public DH key and SSID. The malware on the phone relays the public keys of the GU and AC, and the SSID of the AC to the attacker's own WiFi access point, which they have set up in preparation.

As a result the AC shares a session key $K_{AI} = r_A R_I = r_I R_A$ for SSID $ssid_A$ with the attacker, and the GU shares a session key $K_{GI} = r_G R_I = r_I R_G$ for SSID $ssid_I$ also with the attacker. Now the attacker can act as the PitM to undermine the ground process as illustrated in Fig. 3 for pre-conditioning. The attack works reliably as long as the operator observes their habit of storing the card next to their phone.

3.2 Infiltrating the Secure Zone

We now elicit the methods that an attacker could exploit to infiltrate the secure zone of the turnaround and interact with the readers and/or cards of the 3-tap method. This includes three categories: methods that use equipment outside the zone with a sufficiently long communication range, methods that use malicious devices that are covertly brought into the zone, and methods that use malware brought onto regular devices used in the zone. The attack vectors

Table 1: Infiltrating the Secure Zone

Attack Carrier	Host	Range	C&C
Eavesdropper	Thing in/out of z.	2, 4m / > 10m[1]	Yes
Fake card	Operator	Nominal NFC	No
Leech device	Operator Thing in zone	25cm / < 50cm[1]	Yes
Ghost device	Operator Thing in/out of z.	> 10m[1]	Yes
Malware proxy	Operator Thing in zone	Nominal NFC	Yes

are summarized in Table 1. We also record whether the method allows for a command & control (C&C) channel to an attacker's server via WiFi, e.g. to relay public keys as in the proof-of-concept attack.

Eavesdropper. While the nominal range of NFC communication is only 5-10 cm the range of eavesdropping can be considerably larger. In [8] Finke and Kelter first demonstrate that the communciation between an ISO-14443 reader and tag can be eavesdropped from 1-2 m using a large loop antenna. In [30] Zhou and Xing build an NFC sniffer that improves this to 2,4 m. Moreover, based on simulation Kfir and Wool predict an eavesdropping distance of tens of meters when an active antenna is used [16]. At a parking slot, a large antenna can be hidden in large luggage, sports equipment, prams, wheelchairs, cages for pets, or instruments.

Fake Card. During a break a GU operator might reside in a less restricted area. An attacker with pickpocketing capability could use this as a window of opportunity to swap a counterfeit card for the regular card. Since pickpocketing can include social engineering such a card swap cannot be ruled out even when the card must be worn physically attached to the operator, e.g. by a lanyard.

Leech Device. An important component in relay attacks against electronic payment systems is a *leech*, which is a device that fakes a reader to a card. The leech is smuggled into a victim's pocket or bag so that it is close to their payment card. The leech can then power up the tag of the card, and communicate with it or read out its contents while remaining undetected. The success of a leech depends on whether it is indeed able to activate the victim's card. This can be improved by employing a 'tuned leech' with a range beyond the NFC nominal 5-10 cm, e.g. by increasing the power of transmission and/or using larger antenna. This has been shown to be possible: in [16] Kfir and Wool predict a distance of 40-50 cm by simulation, and in [18] Kirschenbaum and Wool have experimentally confirmed a skimming range of about 25 cm. In our setting, an attacker could plant a leech device into an operator's pocket while they are on a break. A leech could also be planted on equipment within the zone such as the GU or AC itself, e.g. outside operational times.

Ghost Device. The other important component in relay attacks against electronic payment systems is a *ghost*, which is a device that fakes a card to a reader. Our application seems protected from ghost attacks since only authorized personnel can get close to the GU and AC readers. Since we employ passive cards, one would expect that

[1]These values are not experimentally validated (c.f. text).

for a ghost to communicate with a reader it would have to be within their nominal activation range of up to 10 cm. However, in [16] Kfir and Wool show how to build an *active* ghost, which considerably increases the possible distance to the reader. The idea is that the ghost transmits in a non-standard way using its own power but so that to the reader the transmission is indistinguishable from that of a passive tag's. Based on simulation they predict a distance of up to 50 m for bi-directional communication. To our knowledge this has not yet been experimentally confirmed but it shows that a priori we cannot exclude ghost attacks, be it via a proxy device or even from remote.

Malware Proxy. A further threat in our setting is that a standard device such as a smartphone with NFC capability carried by authorized personnel is converted into a leech and/or ghost by malware. We have provided a proof-of-concept implementation of excactly that attack vector. An attacker with standard hacking capability could compromise the smartphone, e.g. by planting malware on the device via a Trojan app or a spear phishing email to the operator. While this allows for purely remote attacks, in contrast to a hardware proxy, the success of a malware proxy is constrained by the standard device's nominal range, and the operator being in the habit of storing it close enough to the card.

Summary. Hence, the attacker is not only able to eavesdrop from outside the zone but they can also engage in an NFC data exchange with a regular reader or card, either via a malicious proxy or even from further away.

3.3 Manipulating Ongoing NFC Transmissions

This leaves open whether and how the attacker can interact with an ongoing NFC transmission. We first summarize how a data link connection between a reader and a card is established (ISO 1444-3) and how data is transmitted (ISO 1444-4).

We employ NFC in the active/passive mode similarly to EMV readers and cards. The reader operates in active mode, which means it generates the electromagnetic field, and also powers up proximate cards by electromagnetic induction. The reader regularly sends out a sense request, to which all cards in range respond. Then follows an anti-collision phase that results in the selection of a single card to be linked. The link is active after attributes such as the maximal frame length and the data rate have been exchanged. Then follows the actual data exchange. Finally the link is deactivated, and the target deselected. The data exchange is carried out in pairs of data exchange request and data exchange response frames. The reader is always the initiator of the request, and the card the target that sends the response. We now summarize how an ongoing transmission can be manipulated by the attacker. This has been investigated in [15] and [25].

As with other wireless channels the attacker can easily *disrupt* an ongoing NFC transmission by overlaying their own signal at high strength. The attacker may also be able to *insert* data without being noticed when the card is slow to respond to a data exchange request. It is more challenging to *modify* transmitted data in a meaningful way. Depending on the encoding it may be feasible or less feasible for the attacker to flip bits; also they may have to adapt the corresponding CRC values to ensure that the modification remains undetected. Since we cannot entirely exclude modification we model this as follows: if data is transmitted that can be predicted by the attacker then we include that the attacker can modify it to a value chosen by themselves. Otherwise we exclude that they can modify the data in any determined fashion.

It is generally assumed that it is practically impossible to carry out a *person-in-the-middle attack* over NFC, especially not in the active/passive mode of our setting. In this mode the reader is always the initiator of a data exchange. If the reader sends out its data in a data exchange request then the attacker can disrupt it. However, to substitute it with its own data the attacker has to generate a second RF field. Since it is practically infeasible to align the two RF fields the card will not be able to receive the data [15]. Also, the reader can easily detect that something is wrong and abandon the transmission. Even if the attacker managed to develop an NFC module (outside the standards) that could send a data exchange request in passive mode then the reader, waiting for a response, would also notice that something is very wrong.

3.4 Attacker Model

We now translate both types of attack vectors into an abstract attacker model. As usual our model is an overapproximation. By including the concept of NFC data link we manage to obtain a model that includes all identified *potential* capabilities but still falls short of the Dolev-Yao Intruder. The *NFC Intruder* can

(1) eavesdrop on any NFC transmission,
(2) pose as a card, be linked to any reader, and exchange data with it,
(3) pose as a reader, establish a link to any card, and exchange data with it,
(4) disrupt any ongoing NFC transmission with the result that at least one of the regular owners of the link will quit the data link connection,
(5) insert data into any ongoing NFC transmission,
(6) modify any transmitted data that can be predicted by the attacker to data chosen by the attacker,
(7) modify any transmitted data that is a priori unknown to the attacker to data that cannot be chosen by the attacker.

The NFC Intruder can carry out these actions both in parallel and sequentially against an unbounded number of regular readers and cards, and their NFC transmissions. They can decompose and compose messages with the same capability as the Dolev-Yao Intruder. Moreover, the NFC Intruder can collude with the Dolev-Yao Intruder on other open channels such as WiFi.

4 A SECURE 3-TAP PAIRING SCHEME

4.1 S3T — A Secure 3-Tap Pairing Method

We now describe our improved pairing method. The protocols run on the readers and cards are depicted in Fig. 4. They consist of three subprotocols corresponding to the three taps.

Binding the Card to the GU. Our method requires that every GU, say G, is equipped with its own card. A shared symmetric key K_G is pre-installed on both the GU reader and its card. (This can be done outside usual operation within a shielded high-security environment.) The shared key provides a trust anchor for the GU reader and card to run an authenticated key establishment (AKE)

Authenticated Key Establishment				
1.	C_G	$\longleftrightarrow$ R_G :	$AKE(K_G)$	
		:	Result: shared secret K_S	
2.	C_G, R_G	:	$K_G^D = KDF_1(K_S)$	
3.	C_G, R_G	:	$K_G^M = KDF_2(K_S)$	
Distance Bounding				
4.	C_G	$\longleftrightarrow$ R_G :	$DB(K_G^D)$	
Authenticated Message Transfer				
5.	R_G	$\longrightarrow$ C_G :	$M_1, mac(M_1, K_G^M)$	

(a) Initial Exchange between GU Reader and Card

Key Establishment				
1.	C_G	$\longleftrightarrow$ R_A :	$DHKE$	
		:	Result: shared secret K_S	
2.	C_G, R_A	:	$K_A^D = KDF_1(K_S)$	
3.	C_G, R_A	:	$K_A^M = KDF_2(K_S)$	
Distance Bounding				
4.	C_G	$\longleftrightarrow$ R_A :	$DB(K_A^D)$	
Authenticated Message Exchange				
5.	C_G	$\longrightarrow$ R_A :	$M_1, mac(M_1, K_A^M)$	
6.	R_A	$\longrightarrow$ C_G :	$M_2, mac(M_2, K_A^M)$	

(b) Exchange between AC Reader and Card

Authenticated Message Transfer				
1.	C_G	$\longrightarrow$ R_G :	$M_2, mac(M_2, K_G^M)$	

(c) Final Exchange between GU Reader and Card

K_G	Key shared between GU reader and its card
M_1, M_2	1st and 2nd message of two-pass KE protocol
$AKE(K)$	Authenticated key establishment based on K
$KDF_i(K)$	Key derivation function for ith derived key
$DB(K)$	Distance bounding protocol based on K
$DHKE$	Diffie-Hellman key exchange
$mac(M, K)$	MAC computed over M with key K

(d) Acronyms

Figure 4: The protocol sequence of the S3T method

protocol when a new 3-tap session is initiated with the first tap: to mutually authenticate each other and establish a session secret K_S. From K_S two session keys are derived, K_G^M for message authentication and K_G^D for distance bounding. The first will be used to secure the message transfer during both the first tap as well as the final tap. This is crucial for security: thereby the taps are cryptographically bound together, which avoids state confusion attacks. As the AKE we use here the protocol specified in ECMA NFC-SEC-04, i.e. ISO/IEC 13157-1 (ECMA-385).

Distance Bounding. As with EMV cards the cryptographic authentication leaves open that an attacker carries out relay attacks. Even in the secure zone of the turnaround we cannot exclude that this might be carried out via proxy devices (c.f. Section 3). The relay could involve a recently "lost" card or a card carried by the operator in the cafeteria. This can be prevented by distance bounding (DB) protocols [21], which guarantee an upper bound on the distance of the card to the reader. To this end the reader measures the round-trip time of challenge/response pairs it poses to the card. We use here the DB protocol by Hancke and Kuhn [14], and the verification results of [22]. As is essential for security (e.g. to prevent distance hijacking [6]) the protocol binds in a key pre-shared by the reader and the card. Here we use K_G^D, one of the keys derived from the secret initially established by the AKE protocol.

Securing the Link between Card and AC. Since the card and AC reader cannot share any long-term keys (unless we break the device pairing paradigm) we do not have any trust anchor to run an AKE protocol between them. Instead, we proceed as follows. First, we rely on the characteristics of the NFC channel that does not allow PitM attacks during an ongoing NFC transmission. Thereby justified we use the basic Diffie-Hellman (DH) key exchange to establish a session key (while we do not know yet with whom this key is established). Second, the AC reader runs the DB protocol rooted in the DH key to ascertain that with whomever it has established the DH key is also in close proximity. Note that this does not rule out that the card is tricked to negotiate a key with an NFC leech (c.f. Section 3). However, this will be detected during the next tap: now the card will expect to communicate with the GU using the same session key as established during the first GU tap, which in turn is anchored in a secret shared between the GU and its card only.

Secure Proximate Zone. While distance bounding makes sure that the AC and GU reader only communicate with a device close by, we cannot a priori rule out that this is indeed a malicious proxy. The risk is reduced by a measure that is implemented by EMV readers: we require the 3-tap readers to abandon the pairing session if a collision is detected during the establishment of the NFC data link. This rules out that readers communicate with a proxy carried by an operator in addition to the authentic card. In addition, we rule out that readers communicate with a proxy planted on proximate equipment by process measures: by directionality of the NFC field and enforcing that no other equipment is placed within distance d from the readers, where d is the precision of the DB protocol. Alternatively, operators can scan for tags prior to the turnaround. E.g. [27] reports a distance error of 15 cm for their DB realization.

4.2 Channel Authenticity of the 3-Tap Method

We now define precisely what it means for a 3-tap pairing method to guarantee an authentic message exchange. Building on the standard notions of protocol verification [20] we capture authenticity in terms of agreement of local sessions. We define local sessions of readers in terms of events of NFC data exchange, and local sessions of operators in terms of events of NFC taps respectively. We

first provide these definitions, and also define when an NFC event coincides with a tap event.

An *NFC data exchange event (short: NFC event)* of a reader R is an event *nfc*, during which R establishes an NFC link with a card C, exchanges data with C, and then closes the link. Often the data exchange will consist of a pair of messages m_r and m_s such that m_r is received by R and m_s is sent by R. Then we denote m_r by $msg\text{-}r(nfc)$ and m_s by $msg\text{-}s(nfc)$. The *session of a GU reader* consists of a sequence of two NFC data exchange events (nfc_1, nfc_2), and the *session of an AC reader* of one NFC data exchange event (nfc). The *partial session of a GU reader* consists of one NFC event.

An *NFC tap event (short: tap event)* of an operator O is an event *tap* during which O brings an NFC card close to a reader, and perceives the feedback of the reader to be successful. We assume readers are equipped with a status display, and each reader will signal on its display whether an NFC event has been completed successfully or not (e.g. green or red light). We denote the reader tapped during *tap* by $reader(tap)$. The *session of an operator* consists of a sequence of three *NFC tap events* $(tap_{ini}, tap_{mid}, tap_{fin})$ The *partial session of an operator* is a sequence of one or two tap events.

Given a tap event *tap* of an operator O and an NFC event *nfc* of a reader R, we say *tap* and *nfc coincide* when $reader(tap) = R$ and O perceives the feedback that R displays upon completion of *nfc* as the reply to *tap*. We then write $tap \approx nfc$.

We are now ready to define our notion of *channel authenticity*. It asserts that if there is a GU session then there must be an AC session with matching messages as well as an operator session whose taps coincide with the NFC events of the GU session, and that of the AC session in the obvious way. And we require the analogue for the other direction.

Definition 4.1 (Channel Authenticity). Let M be a 3-tap pairing method. We say M guarantees *channel authenticity to the GU* if, whenever a GU reader has completed a session (nfc_G^1, nfc_G^2) then some operator has completed a session $(tap_{ini}, tap_{mid}, tap_{fin})$, and some AC reader has completed a session (nfc_A) such that

(1) the tap and NFC events agree as follows: $tap_{ini} \approx nfc_G^1$, $tap_{mid} \approx nfc_A$, and $tap_{fin} \approx nfc_G^2$, and
(2) the messages agree as follows: $msg\text{-}s(nfc_G^1) = msg\text{-}r(nfc_A)$, and $msg\text{-}s(nfc_A) = msg\text{-}r(nfc_G^2)$.

Similarly, we say M guarantees *channel auhenticity to the AC* if, whenever an AC reader has completed a session (nfc_A) then some operator has carried out a partial session (tap_{ini}, tap_{mid}), and some GU reader has carried out a partial session (nfc_G^1) such that

(1) the tap and NFC events agree as follows: $tap_{ini} \approx nfc_G^1$, and $tap_{mid} \approx nfc_A$, and
(2) the messages agree: $msg\text{-}s(nfc_G^1) = msg\text{-}r(nfc_A)$.

We say M guarantees *channel authenticity* iff M guarantees this to both parties, GUs and ACs.

Theorem 4.2. *The S3T method guarantees channel authenticity.*

So far we have proved this theorem semi-formally within an ad hoc event-based model. On the one hand, we prove that the S3T method guarantees certain authenticity properties to the GU reader, the card, and the AC reader. To illustrate this further, for the GU this means: if a GU reader has successfully completed a (partial) session then it can be certain that there is an authentic card with matching NFC events, during which the card was proximate. On the other hand, we show that if these authenticity properties are given and measures as described in 'secure proximate zone' are in place then we can infer that an operator's tap events must coincide with such authentic NFC events, and hence that channel authenticity is given. The preliminary proof is provided in Appendix A.

4.3 Secure 3-Tap Pairing Schemes

A 3-tap pairing scheme consists of a pair $S = (M, P)$ where M is a 3-tap pairing method, and P is a two-pass key establishment protocol. Such a pairing scheme is secure iff (1) M guarantees channel authenticity, and (2) P guarantees secrecy and key freshness in the presence of passive adversaries.

Corollary 4.3. *The scheme (M, P) where M is the S3T method and P is the basic Diffie-Hellman exchange is a secure pairing scheme.*

5 CONCLUSIONS

We have provided a method and semi-formal proofs that affirm that it is indeed possible to have high-assurance machine pairing. We have investigated this in the context of ground processes of an airport but the method is equally applicable to other settings such as marine ports or production facilities.

The next step is to obtain a formal and tool-based proof of the main result that the S3T method guarantees channel authenticity. We plan to use the protocol prover Tamarin [4] to this end. This will involve developing several new verification techniques: firstly, to model the NFC Intruder as an attacker theory in Tamarin, and integrate it alongside the standard attacker theory; secondly, to include aspects of physicality such as the path of the operator and the physical NFC taps, and their agreement with the NFC cyber sessions; thirdly, to verify the composition of the various types of protocols that underlie the S3T method.

We have employed the DH key exchange in two ways: (1) to secure the mid tap with the AC, and (2) as the conrete two-way protocol that is carried out via the S3T channel. Both of these uses can be replaced by a post-quantum secure key exchange based on a KEM such as Kyber. However, if we wish to ensure that both parties have a share in the key we need a three-way rather than a two-way exchange. For use (1) this is necessary for security but does not pose any change (apart from performance, which still needs to be investigated for NFC, in general). For use (2) this is not absolutely necessary. Also, a three-way key exchange based on KEMs can be securely realized by sending the third message over the WiFi channel. At the same this discussion highlights the preference and demand for a post-quantum secure *two-way* key exchange.

Our fully local approach to establish a key brings with it resilience against multi-instance attacks. We pinpoint a metric for resilience against parallel scaling of attacks as follows: *The effort for the attacker to successfully attack n parallel sessions of the S3T method grows linearly with n wrt a factor of physical effort the attacker has to spend.* This can be shown to hold by an informal argument since an attack requires the attacker to interact locally with the setting. In future work, we will explore how to formally define and prove such resilience metrics.

REFERENCES

[1] Adnan Abu-Mahfouz and Gerhard P. Hancke. 2013. Distance Bounding: A Practical Security Solution for Real-Time Location Systems. *IEEE Transactions on Industrial Informatics* 9, 1 (2013), 16–27. https://doi.org/10.1109/TII.2012.2218252

[2] Sajeda Akter, Sriram Chellappan, Tusher Chakraborty, Taslim Arefin Khan, Ashikur Rahman, and A. B. M. Alim Al Islam. 2021. Man-in-the-Middle Attack on Contactless Payment over NFC Communications. *IEEE Transactions on Dependable and Secure Computing* 18, 6 (2021), 3012–3023. https://doi.org/10.1109/TDSC.2020.3030213

[3] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan Čapkun, Gerhard Hancke, Süleyman Kardaş, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo-Rasua, and Serge Vaudenay. 2018. Security of Distance-Bounding: A Survey. *Comput. Surveys* 51, 5 (2018).

[4] David Basin, Cas Cremers, Jannik Dreier, and Ralf Sasse. 2022. Tamarin: Verification of Large-Scale, Real World, Cryptographic Protocols. *IEEE Security and Privacy Magazine* (2022). https://doi.org/10.1109/msec.2022.3154689

[5] Stefan Brands and David Chaum. 1994. Distance-Bounding Protocols. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '93)*. Springer-Verlag, 344–359.

[6] Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, and Srdjan Capkun. 2012. Distance Hijacking Attacks on Distance Bounding Protocols. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 113–127.

[7] Saar Drimer and Steven J. Murdoch. 2007. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. In *16th USENIX Security Symposium (USENIX Security 07)*. USENIX Association.

[8] T. Finke and H. Kelter. 2005. Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. Bundesamt für Sicherheit in der Informationstechnik.

[9] Mikhail Fomichev, Flor Álvarez, Daniel Steinmetzer, Paul Gardner-Stephen, and Matthias Hollick. 2018. Survey and Systematization of Secure Device Pairing. *IEEE Communications Surveys & Tutorials* 20, 1 (2018), 517–550. https://doi.org/10.1109/COMST.2017.2748278

[10] Lishoy Francis, Gerhard Hancke, and Keith Mayes. 2013. A Practical Generic Relay Attack on Contactless Transactions by Using NFC Mobile Phones. *Int. Journal of RFID Security and Cryprography* 2, 1-4 (2013), 92–106.

[11] Sibylle Fröschle and Martin Kubisch. 2023. Security Process for Adopting Machine to Machine Communication for Maintenance in Transportation with a Focus on Key Establishment. In *Proceedings of SIMUL 2023: The Fifteenth International Conference on Advances in System Simulation*. Thinkmind Digital Library, 50 – 58. https://www.thinkmind.org/index.php?view=article&articleid=simul_2023_1_90_50045

[12] Sibylle Fröschle and Martin Kubisch. 2024. Key Establishment for Maintenance with Machine to Machine Communication in Transportation: Security Process and Mitigation Measures. *International Journal on Advances in Security* 17, 1&2 (2024). https://www.iariajournals.org/security/

[13] Sibylle B. Fröschle, Martin Kubisch, and Marlon Gräfing. 2020. Security Analysis and Design for TAGA: a Touch and Go Assistant in the Aerospace Domain. *CoRR* abs/2004.02516 (2020). arXiv:2004.02516 https://arxiv.org/abs/2004.02516

[14] G.P. Hancke and M.G. Kuhn. 2005. An RFID Distance Bounding Protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. 67–73. https://doi.org/10.1109/SECURECOMM.2005.56

[15] Ernst Haselsteiner and Klemens Breitfuß. 2006. Security in Near Field Communication (NFC). Strengths and weaknesses. In *Workshop on RFID Security*.

[16] Ziv Kfir and Avishai Wool. 2005. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard. In *Proc. of the 1st Intern. Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM '05)*. IEEE Computer Society, 47–58.

[17] Chong Hee Kim and Gildas Avoine. 2009. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In *Cryptology and Network Security*. Springer Berlin Heidelberg, 119–133.

[18] Ilan Kirschenbaum and Avishai Wool. 2006. How to Build a Low-cost, Extended-range RFID Skimmer. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*. USENIX Association, Article 4.

[19] Ming Li, Wenjing Lou, and Kui Ren. 2011. Secure Device Pairing. In *Encyclopedia of Cryptography and Security*. Springer US, 1111–1115.

[20] Gavin Lowe. 1997. A Hierarchy of Authentication Specification. In *10th Computer Security Foundations Workshop (CSFW '97), June 10-12, 1997*. IEEE Computer Society, 31–44.

[21] A. A. Mahfouz and G. P. Hancke. 2013. Distance bounding: A practical security solution for real-time location systems. *IEEE Trans. Industrial Informatics* 9, 1 (2013), 16–27.

[22] Sjouke Mauw, Zach Smith, Jorge Toro-Pozo, and Rolando Trujillo-Rasua. 2018. Distance-Bounding Protocols: Verification Without Time and Location. In *2018 IEEE Symposium on Security and Privacy (SP)*. 549–566. https://doi.org/10.1109/SP.2018.00001

[23] Shahab Mirzadeh, Haitham Cruickshank, and Rahim Tafazolli. 2014. Secure Device Pairing: A Survey. *IEEE Communications Surveys & Tutorials* 16, 1 (2014), 17–40. https://doi.org/10.1109/SURV.2013.111413.00196

[24] Steven J. Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. 2010. Chip and PIN is Broken. In *IEEE Symposium on Security and Privacy*. 433–446. https://doi.org/10.1109/SP.2010.33

[25] Steven J. Olivieri. 2015. *An Investigation of Security In Near Field Communication Systems*. Ph.D. Dissertation. Worcester Polytechnic Institute.

[26] Andreea-Ina Radu, Tom Chothia, Christopher J.P. Newton, Ioana Boureanu, and Liqun Chen. 2022. Practical EMV Relay Protection. In *2022 IEEE Symposium on Security and Privacy (SP)*. 1737–1756. https://doi.org/10.1109/SP46214.2022.9833642

[27] Kasper Bonne Rasmussen and Srdjan Čapkun. 2010. Realization of RF Distance Bounding. In *Proceedings of the 19th USENIX Conference on Security* (Washington, DC) *(USENIX Security'10)*. USENIX Association, USA, 25.

[28] Patrick Schaller, Benedikt Schmidt, David Basin, and Srdjan Capkun. 2009. Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks. In *22nd IEEE CSF Symposium*. 109–123. https://doi.org/10.1109/CSF.2009.6

[29] Jianliang Wu, Ruoyu Wu, Dongyan Xu, Dave Jing Tian, and Antonio Bianchi. 2022. Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities. In *2022 IEEE Symposium on Security and Privacy (SP)*. 2285–2303. https://doi.org/10.1109/SP46214.2022.9833777

[30] Ruogu Zhou and Guoliang Xing. 2014. nShield: a noninvasive NFC security system for mobiledevices. *Proceedings of the 12th annual international conference on Mobile systems, applications, and services* (2014).

A PROOF OF THEOREM 4.2

Definition A.1. We assume that each reader displays the status of the tap it received (i.e. initial, mid, final), and that the operator's actions are well-defined in the following sense:

(1) The operator taps an AC only as part of the mid tap of a 3tap session.
(2) If during a 3tap walk the operator observes that the display of the GU or AC reader does not confirm the action they expected to carry out (e.g. the tap is (repeatedly) unsuccessful) then they will reset the NFC controller at the GU before carrying out any further taps.

In the following, let N_{S3T} denote the NFC system as defined in Section 4.1. Theorem 4.2 follows from Lemma A.7 and Lemma A.8 below. The first lemma proves that when an NFC system guarantees certain properties to be defined below then under the measure 'secure proximate zone' it will guarantee channel authenticity. The second lemma then argues that N_{S3T} satisfies these properties. Before proving the lemmas we need more definitions and intermediary facts.

If a reader R has an NFC event δ_x, and a card C has an NFC event γ_y, and R and C communicate with each other during these NFC events then we write this by $\delta_x \leftrightarrow \gamma_y$.

A *session of a card* C is a tuple $(\sigma_{ini}, \sigma_{mid}, \sigma_{fin})$ where σ_{ini}, σ_{mid}, and σ_{fin} are successful NFC events of C such that $msg\text{-}r(\sigma_{ini}) = msg\text{-}s(\sigma_{mid})$, and $msg\text{-}r(\sigma_{mid}) = msg\text{-}s(\sigma_{fin})$.

Let τ be an operator tap event. Then by $card(\tau)$ we denote the card the operator uses during the tap.

Due to 'secure proximate zone' and distance bounding we can infer operator taps from NFC events of the GU and AC reader, and vice versa:

Proposition A.2. *Let N be an NFC system with distance bounding, and assume 'secure proximate zone' holds.*

(1) *If a GU or AC reader R has an NFC event δ_x and $partner(\delta_x)$ is proximate during δ_x then there is an operator tap τ_x such that*
   (a) $card(\tau_x) = partner(\delta_x)$, *and*

(b) $\tau_x \approx \delta_x$.

(2) *If there is an operator tap τ_x and reader(τ_x) is a GU or AC reader R then R has a NFC event δ_x such that*
   (a) *card(τ_x) = partner(δ_x), and*
   (b) $\tau_x \approx \delta_x$.
   (c) *If R is a GU reader then C is authentic.*

Proof. (1) This follows from 'secure proximate zone'.

(2) Since the operator visually verifies that the reader has successfully completed an NFC exchange (e.g. green light) δ_x exists. By distance bounding and 'secure proximate zone' the exchange must have indeed been carried out with the operator's card. If the reader is a GU then the GU will check authenticity of the card during the initial exchange, and indirectly via the derived mac key during the final exchange. In both cases the NFC exchange will fail if the card is not authentic (e.g. red light). □

Proposition A.3 (Taps and reader sessions).

(1) *If there are operator taps τ_x, τ_y and a GU session $(\gamma_{ini}, \gamma_{fin})$ such that $\tau_x \approx \gamma_{ini}$ and $\tau_y \approx \gamma_{fin}$ then there must be an operator session $(\tau_x, \tau_{mid}, \tau_y)$ for some τ_{mid}.*
(2) *If there is an operator tap τ_{ac} and an AC session (α_{mid}) such that $\tau_{ac} \approx \alpha_{mid}$ then there must be an operator session $(\tau_{ini}, \tau_{ac}, \ldots)$ for some τ_{ini}.*

Proof. (1) By Def. A.1(2) the operator will immediately abort the GU session if τ_x wasn't the first tap of a session $(\tau_x, \ldots)$. Since G receives the last NFC event the latter must be true. By definition of operator session the next tap the operator will carry out is with the AC. By Def. A.1(2) the tap is either successful or the operator will immediately abort G's session. Since G receives the last NFC event the former must be true. But then τ_{mid} exists as required.

(2) This follows from Def. A.1(1) . □

The following are guarantees that the NFC system must provide to the GU, card, and AC.

Definition A.4 (Guarantees to GU). Let N be an NFC system.
We say N guarantees *'authenticity of initial tap to a GU G'* if, whenever G has a session $(\gamma_{ini}, \ldots)$ then there is an *authentic* card C with a session $(\sigma_{ini}, \ldots)$ such that

(1) $\gamma_{ini} \leftrightarrow \sigma_{ini}$ and $msg(\gamma_{ini}) = msg(\sigma_{ini})$, and
(2) C is proximate to G during σ_{ini}.

We say N guarantees *'authenticity of final tap to a GU G'* if, whenever G has a session $(\gamma_{ini}, \gamma_{fin})$ then there is an authentic card C with a session $(\sigma_{ini}, \sigma_{mid}, \sigma_{fin})$ such that

(1) $\gamma_{ini} \leftrightarrow \sigma_{ini}$ and $msg(\gamma_{ini}) = msg(\sigma_{ini})$,
(2) $\gamma_{fin} \leftrightarrow \sigma_{fin}$ and $msg(\gamma_{fin}) = msg(\sigma_{fin})$, and
(3) C is proximate to G during σ_{ini} and σ_{fin}.

Definition A.5 (Guarantees to Card). Let N be an NFC system.
We say N guarantees *'authenticity of initial tap to a card C'* if, whenever C has a session $(\sigma_{ini}, \ldots)$ then there is some GU G with a session $(\gamma_{ini}, \ldots)$ such hat

(1) $\gamma_{ini} \leftrightarrow \sigma_{ini}$, and $msg(\gamma_{ini}) = msg(\sigma_{ini})$, and
(2) C is proximate to G during σ_{ini}.

We say N guarantees *'authenticity of mid tap with AC to a card C* if, whenever C has a session $(\sigma_{ini}, \sigma_{mid}, \ldots)$ and $partner(\sigma_{mid})$ is an AC A then A has a session (α_{mid}) such that $\alpha_{mid} \leftrightarrow \sigma_{mid}$ and $msg(\alpha_{mid}) = msg(\sigma_{mid})$.

Definition A.6 (Guarantees to AC). Let N be an NFC system.
N guarantees *'proximity of NFC peer to an AC A'* if, whenever an AC A has a session (α_{mid}) then $partner(\alpha_{mid})$ is proximate to A during α_{mid}.
We say N guarantees *'authenticity of mid tap with an authentic card to an AC A'*, if whenever A has a session (α_{mid}) and $partner(\alpha_{mid})$ is an authentic card, say C, then C has a session $(\sigma_{ini}, \sigma_{mid}, \ldots)$ such that $\alpha_{mid} \leftrightarrow \sigma_{mid}$ and $msg(\alpha_{mid}) = msg(\sigma_{mid})$.

Lemma A.7. *Let N be an NFC system, and M a set of process measures such that N implements distance bounding and the guarantees to GU, card, and AC of Def. A.4, A.5, A.6, and M guarantees 'secure proximate zone'. Then N under M guarantees Channel Authenticity.*

Proof. *Guarantee for GU:* Assume G has a session $(\gamma_{ini}, \gamma_{fin})$. Then by 'authenticity of final tap to G' there is an *authentic* card C with a session $(\sigma_{ini}, \sigma_{mid}, \sigma_{fin})$ such that the NFC events and exchanged messages are matching: $\gamma_{ini} \leftrightarrow \sigma_{ini}$, $\gamma_{fin} \leftrightarrow \sigma_{fin}$, $msg(\gamma_{ini}) = msg(\sigma_{ini})$, and $msg(\gamma_{fin}) = msg(\sigma_{fin})$. Moreover, C is proximate to G during σ_{ini} and σ_{fin}.

By Prop. A.2(1) there are successful operator taps τ_{ini}, τ_{fin} such that $card(\tau_{ini}) = C$ and $\tau_{ini} \approx \gamma_{ini}$, and $card(\tau_{fin}) = C$ and $\tau_{fin} \approx \gamma_{fin}$ respectively. Then by Prop. A.3(1) there is an operator with a session $(\tau_{ini}, \tau_{mid}, \tau_{fin})$ for some τ_{mid}.

Further, by definition of operator session we obtain $reader(\tau_{mid}) = A$ for some AC A and $card(\tau_{mid}) = C$. Hence, by Prop A.2(2) A has a successful NFC event α_{ac} such that $partner(\alpha_{ac}) = C$ and $\tau_{mid} \approx \alpha_{ac}$. Let σ_{ac} be defined by $\alpha_{ac} \leftrightarrow \sigma_{ac}$. σ_{ac} takes place after γ_{ini} (and hence σ_{ini}) and before γ_{fin} (and hence σ_{fin}). Hence, we conclude that $\sigma_{ac} = \sigma_{mid}$. Then by 'authenticity of mid tap with AC to C' A must have a session (α_{mid}) and $msg(\alpha_{mid}) = msg(\sigma_{mid})$. Finally, by definition of session of a card it is straightforward to check that the messages of the A session match those of the G session.

Guarantee for AC: Assume A has a session (α_{mid}). Then by 'proximity of NFC peer to A' $partner(\alpha_{mid})$, say C, is proximate. Then by Prop. A.2(1) there is a successful operator tap τ_{ac} such that $\tau_{ac} \approx \alpha_{mid}$ and $card(\tau_{ac}) = C$. Then by Prop. A.3(2) there is an operator session $(\tau_{ac}^{ini}, \tau_{ac}, \ldots)$ for some τ_{ac}^{ini}. By definition of operator session $reader(\tau_{ac}^{ini})$ is a GU G_{ac}, and $card(\tau_{ac}^{ini}) = C$.

By Prop. A.2(2) G_{ac} has a successful NFC event γ_{ac}^{ini} such that $partner(\gamma_{ac}^{ini}) = C$, $\tau_{ac}^{ini} \approx \gamma_{ac}^{ini}$, and C is authentic. Let σ_{ac}^{ini} be defined by $\gamma_{ac}^{ini} \leftrightarrow \sigma_{ac}^{ini}$.

Since C is authentic by 'authenticity of mid tap with authentic card to A' C has a session $(\sigma_{ini}, \sigma_{mid}, \ldots)$ such that $\alpha_{mid} \leftrightarrow \sigma_{mid}$ and $msg(\alpha_{mid}) = msg(\sigma_{mid})$. By 'authenticity of initial tap to C' there is some GU G with a session $(\gamma_{ini}, \ldots)$ such that $\gamma_{ini} \leftrightarrow \sigma_{ini}$, $msg(\gamma_{ini}) = msg(\sigma_{ini})$, and C is proximate to G during σ_{ini}. By definition of session of a card we also obtain that the messages of α_{mid} and γ_{ini} are matching.

Moreover, by Prop. A.2(1) there is a successful operator tap τ_{ini} such that $card(\tau_{ini}) = C$ and $\tau_{ini} \approx \gamma_{ini}$. Hence, it only remains to show that $\tau_{ini} = \tau_{ac}^{ini}$. To the contrary assume this not to be the case. Then by definition of operator session, τ_{ini} must be earlier than τ_{ac}^{ini}, and hence σ_{ini} earlier than σ_{ac}^{ini}. But this leads to a contradication:

since $\tau_{ac} \approx \sigma_{mid}$ and σ_{ini} immediately precedes σ_{mid} on C, we must have σ_{ac}^{ini} earlier than σ_{ini}. □

Lemma A.8. *N_{S3T} implements distance bounding and meets the guarantees of Def. A.4, A.5, A.6.*

Proof. Guarantees to GU: At the first tap the GU reader runs an AKE protocol based on K_G, which is only shared between the GU and the authentic card. Moreover, it runs a distance bounding protocol to ensure that the co-owner of K_G is close by. The communication is secured by the established mac key K_G^M. At the third tap the GU reader verifies that the received message is authenticated using the same key K_G^M. This binds the third tap to the first as required.

Guarantees to card: At the initial tap the card runs an AKE protocol based on K_G shared only with the corresponding GU. Since the GU will only communicate with a card when it can successfully prove its proximity, the card knows that if it has a successful first NFC event then it communicates with a proximate GU. Again the communication itself is secured by the established mac key.

The mid tap will be protected by a key established via the basic DH exchange. Hence, if the mid tap is indeed carried out with an authentic AC then considering that it is practically impossible to carry out a person-in-the-middle attack over NFC in the active/passive mode the communication is secured and the messages are matching.

Guarantees to AC: 'Proximity of NFC peer': This is guaranteed by the distance bounding protocol. Authenticity of mid tap when the tap is carried out with an authentic card follows because the communication is secured by a mac key derived from the established DH secret (considering again that it is practically impossible to carry out a person-in-the-middle attack over NFC in the active/passive mode), and the card only accepts unauthenticated communication as part of its mid tap. □