Online Banking with NFC-Enabled Bank Card and NFC-Enabled Smartphone

Max Günther, Bernd Borchert

Online Banking with NFC-enabled Bank Card and NFC-enabled Smartphone

Max Günther and Bernd Borchert

Department of Computer Science, University of Tübingen, Germany

Abstract. Banks want to use their genuine strong credential for online banking transaction authorization - the debit card. Customers nowadays are usually equipped with a Smartphone and prefer to not carry a card reader in addition. Methods where developed that use the Smartphone to authorize online banking transactions. These methods are vulnerable to Smartphone malware. We present NFC-TAN as a Smartphone method that combines the two requirements: Strong credential debit card and no additional device. We discuss to what extend this solution decreases vulnerability. Moreover, we consider usability, cost, and integration aspects of NFC-TAN.

Keywords: Online Banking, NFC, Smartphone, Smartcard, Signing.

1 Introduction

Modern online banking methods are secured against content-manipulation attacks with transaction-signing solutions: a separate device computes a signature depending on the details of a transaction. The necessary characteristics of a secure signature creation device have been worked out and explained [21, 32] and corresponding online banking systems have been implemented (see Sect. 2.2) which can be considered secure against content-manipulation attacks.

However, academic approval of security is not the only success factor for online banking methods [25, 32]. Other important factors are usability, system integration complexity, trust, bank-internal policies or business strategies, external regulations, and - maybe most importantly - costs and benefits. That is why

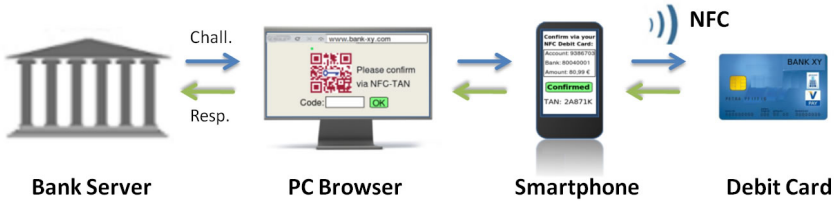

Fig. 1. Basic steps of the NFC-TAN method.

there are many systems with different security, usability, and cost trade-offs in use today.

In this paper, we present NFC-TAN as a method that uses the genuine bank-owned credential debit card (also known as bank card) to authorize PC-based online banking transactions in conjunction with a Smartphone - and nothing else. NFC-TAN works the following way [5]: the Smartphone reads the transaction via 2D code from the PC, shows the transaction data for confirmation on its display, contacts the debit card via NFC and receives a confirmation code from the card; the customer finally transfers this code to the PC (see Fig. 1 and Fig. 2).

We think this approach is well-founded given two assumptions: Banks want to have control over the client side credential and customers do not want to carry any additional devices for authorization purposes. Debit cards offer an array of advantages: They are convenient, well known, copy proof, and already integrated into a banks credential management system.

The enabling technology for this approach is NFC (Near Field Communication): NFC-Smartphones are available and debit cards will be soon NFC-enabled. The NFC-TAN method offers a trade-off between security, usability and cost that was not possible before. This paper contributes an analysis of the security situation and a discussion of the other success factors usability and costs.

2 State of the Art and Related Work

Apart from credential stealing attacks, the customers' insecure Internet clients have been identified as the main vulnerability of online banking systems. Sophisticated attacks such as man-in-the-browser attacks [12, 30, 32] were developed and already anticipated for example in [18]. These content-manipulation attacks can be only defeated if an online banking transaction is authorized by a signature depending on the transaction data and computed by a separate device that also displays the transaction data. If a nonce is used as additional input, also replay and pre-play attacks can be ruled out [4, 28]. A signature in the online banking context may be symmetric or asymmetric and is termed TAN (transaction-authorization-number) or, to underline their dynamic and transaction dependent nature, dynamic-TAN or TAC (transaction-authorization-code [32]). In this paper, we assume traditional username/password authentication at login time as this is used in most online banking systems at least in central Europe - in fact, strong login authentication seems rather unnecessary given transaction-signing solutions.

2.1 Basic Steps of Transaction Signing Solutions

Most modern online banking solutions use two devices in tandem: the PC-browser for convenient input of transaction details and a separated device which displays those details and computes a signature for it. This approach requires two communication paths: the transaction details must be somehow transferred to the signature creation device and the computed signature must be somehow transferred to the PC (or server). The basic steps in most systems therefore are:

1. Enter transaction on the PC-browser (and send it to the server).
2. Transfer transaction details to the separated device.
3. Check (and confirm) the transaction on the display of the separated device, which computes a signature for the transaction.
4. Transfer the signature to the server (possibly via PC-browser).

2.2 Secure Signature Creation Device Solutions

In order to be considered immune against content-manipulation attacks, a signature creation device must fulfill some basic requirements. Various secure devices and corresponding online banking solutions have been proposed and implemented. From our understanding the basic properties of such devices are:

- A display that is guaranteed to show the transaction that will be signed.
- A crypto-module that is guaranteed to sign the displayed transaction.
- A signature can leave the device only if the user decides so.
- Secure storage of the credential (tamper-proof and challenge-response).

One approach to enforce the first three properties is to allow only very limited IO-capabilities (number pad + LCD display) that render malware infection virtually impossible. Especially to allow for more sophisticated interaction with the customers PC, the operating system of the signature creation device must be built securely from ground up and a button to trigger the signature computation may be necessary (if the device also has an out-channel for the signature other than the display). Laurie and Singer define a larger set of requirements to ensure the abovementioned basic properties and to add additional value (e.g. non-repudiation, updateable) [21]. The requirement to securely store a customers credential is mostly considered to be sufficiently satisfied by dedicated hardware like smartcards - laboratory-demonstrated attacks on such hardware are too expensive and therefore considered to be irrelevant for online banking systems [32]. Likewise, we consider vulnerabilities arising from implementation deficits like those reported in [3, 13] to be out of the scope of this paper.

We briefly describe six characteristic external-device solutions in use today which all fulfill the abovementioned requirements for a secure signature creation device, further discussions of such and other solutions can be found in [32, 19, 26]. In all solutions, the transaction details are entered on the PC-browser and double-checked on a separate device that also computes a signature but they greatly vary in terms of usability resp. required customer interaction. We distinguish the solutions in terms of communication/user interaction and the used crypto-module:

ChipTAN [10] An offline smartcard reader (aka TAN-Generator) with photodiodes and display. This solution is of special interest for this paper, because our implementation is based on the same specifications, see Section 3.3. The so called TAN-Generator has a rudimentary optical channel consisting of five photodiodes that serially read the transaction data from a flickering code shown on the PC-display. Once the transaction is transmitted, the

TAN-Generator sends it to the plugged in debit card which in turn computes and returns a TAN as a function of the transaction and a secret. The TAN is then shown on the TAN-Generators display.

Manual Smartcard Reader [10] Manual variant of chipTAN without photodiodes. Communication with browser: number pad / display. Credential: secret stored on debit card.

Camera Token [8] An offline token with camera and display. Communication with browser: 2D code and camera / display. Credential: stored on device.

Offline Token [31] An offline token with a number pad and a display. Communication with browser: number pad and display. Credential: secret stored on the device.

ZTIC [32] A smartcard reader with USB connection and display. Communication with server via special protocol. Credential secret stored on smartcard.

USB-Token [24] Token with USB connection and display. Communication with server via special protocol. Credential stored on device.

2.3 Smartphone-Only Solutions

Solutions were proposed and implemented that use Smartphones instead of secure signature creation devices. For a customer the main advantage of those solutions is convenience: He does not have to carry an additional device but can instead use his Smartphone as a second display in order to check the transaction details before confirming them. The Smartphone solutions also provide communication channels for the transfer of transaction data to the Smartphone and for the transfer of the signature to the PC or server.

Photo-TAN. This class of solutions uses 2D codes to conveniently transfer the transaction data to the Smartphone via camera. A Smartphone app then displays the transaction data and computes a signature using a key stored on the Smartphone. The signature is then either sent to the server via mobile Internet or entered manually on the PC browser by the user. Photo-TAN was suggested by several researchers [6, 11, 17, 27] and was recently implemented at some banks [1, 7, 9]. Some of these implementations work in a reversed fashion: The server encrypts the transaction and a TAN and the Smartphone decrypts the message and displays both components. Given the rise of mobile malware, Photo-TAN has severe vulnerabilities because none of the basic requirements for secure signature creation devices introduced above is fulfilled. Smartphone malware is possibly able to steal the customers signature key and send it to any recipient. Moreover it may be able to manipulate the display and the communication with the crypto-module and send signatures to any recipient, see Sect. 4.1.

mobileTAN. Another well-known solution is mTAN. The customer enters the transaction details in the PC browser and sends them to the server. The server sends the transaction and a TAN to the customers mobile phone via text/SMS. In order to confirm the transaction, the customer enters the TAN in the PC browser

(or cancels the operation if the transaction details have been manipulated). Various attack vectors against mTAN have been exploited [29], see Sect. 4.1.

2.4 Trusted-Smartphone plus Smartcard

Smartphone based solutions that assume the existence of a special execution mode sufficiently shielded against mobile malware can of course meet the abovementioned requirements for a secure signature creation device.

Alpár et al. [2] present one such solution using an NFC smartcard as an external crypto module and envision a user triggered *trusted mode* that enables the user to verify the transaction details on a then-trustworthy Smartphone display; Ortiz-Yepes [22] proposed a similar approach with a NFC smartcard as external crypto module. In addition, both works suggested a protocol based on the industry standard EMV-CAP (Chip Authentication Program) that avoids some of the flaws (e.g. not including the transaction data as signature challenge) found by Drimer et al. in other implementations [13]. The results are similar to the HHD protocol which was developed without those flaws from the outset by the German banking industry and that is used by our solution, see Sect. 3.3.

The main difference to our work is the assumption about having a Smartphone with a *trusted mode*. This distinction greatly influences the threat model and consequently mobile malware attacks are not covered in [2] while these are a major part of our security analysis. Another difference is that we focus on two-channel PC-based online banking, while Alpár et al. discuss the natural scenario given a trusted Smartphone: single-channel mobile banking. Although trusted execution technologies for Smartphones are being developed, to our knowledge currently no commercially available device supports the full functionality.

3 NFC-TAN Method

3.1 Motivation

The NFC-TAN method presented below allows for online banking transaction authorization with the customers debit card as credential and his Smartphone as communication device [5, 16, 23]. We belief this approach is justified given two assumptions:

- Banks prefer the debit card over other client side credentials. The credential debit card is already integrated into a banks credential management system: reliable processes for development, deployment and revocation are in use in any bank. A further benefit is the already implemented industry standard EMV that can be used for transaction authorization, see Sect. 3.3.
- Customers do not want an additional device. An additional device is always a burden - one thing more that costs money and can get stolen, lost, or broke. In contrast, customers have their Smartphone and debit card with them anyway. Apart from these physical aspects, the credential debit card is well-known and convenient because the bank is responsible for initialization, deployment and replacement.

3.2 Description

The steps in the NFC-TAN method are quite simple and familiar to a customer because they resemble the four steps of the basic procedure described in Sect. 2.1:

1. Log in on the PC browser, enter transaction and submit it unconfirmed to the bank server.
2. Scan the 2D code shown on the PC screen with the Smartphone.
3. Double-check the transaction on the Smartphone display and confirm with the debit card.
4. Transfer the TAN to the PC browser and submit it to the bank server.

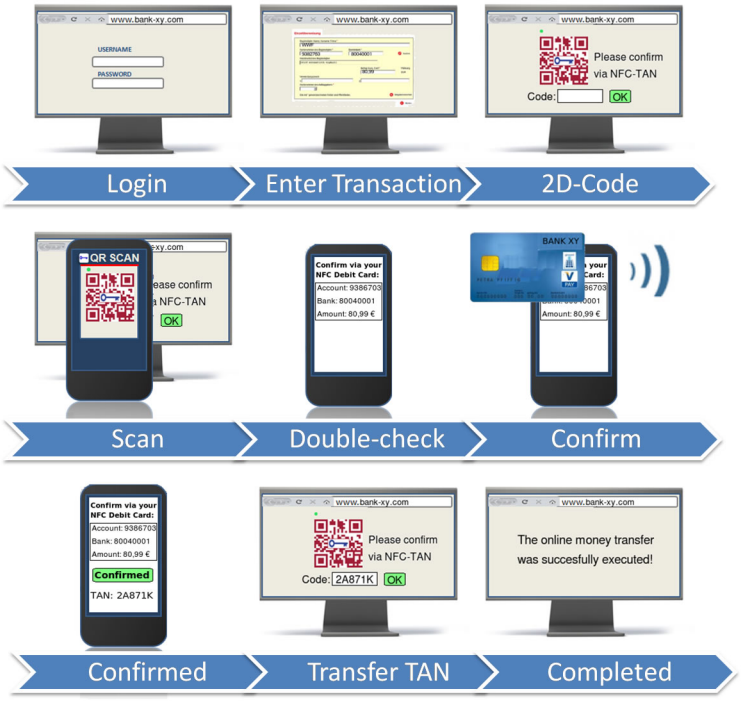

Fig. 2. NFC-TAN procedure from a customer's perspective.

Background interaction. Under the hood, the following interaction and computation is done:

- After receiving the transaction, the bank server generates a 2D code containing the transaction details and a nonce. This 2D code is included in the server response.

- The Smartphone app builds a challenge from the transaction details and the nonce and sends it to the debit card. The debit card calculates the response as a function of the challenge and a secret key and returns it to the Smartphone app. The Smartphone app selects the TAN from this response.
- The server can compute the correct TAN since it knows the transaction details, nonce, and secret key and therefore is able to check the TAN received.

Process Requirement. We require that the server has only one open session and only one open transaction at a time for one account. Our security discussion explains why this rather easy-to-implement requirement is important.

Familiarity. For many customers the NFC-TAN method may be familiar because it is similar to the abovementioned chipTAN method, the differences are: a 2D code is shown instead of a flickering code, the device is a Smartphone not a special purpose device, and debit card and device communicate contactless. NFC-TAN can be seen an extension of Photo-TAN for which the credential is stored and used on the debit card instead of the Smartphone.

Performance. Modern Smartphones are able to scan 2D-code within a second and smartcards are able to compute the response within less than a second.

3.3 Debit Card, EMV and HHD

Debit cards, or more general bank cards, are bank issued smartcards that host an array of different applications. NFC-TAN utilizes the debit cards ability to compute a signature as a function of a given challenge and a secret stored on the card. The inter-operation of terminal and card for this functionality is specified by EMV [14], a generic industry standard based on ISO7816 (contact) resp. ISO14443 (contactless). On the basis of EMV, card issuers developed standards for applications like ATM, POS, and online banking - with MasterCards CAP being a prominent example. The German banking industry committee *Central Credit Committee*, developed the standard HHD (hand held device) [33] which is used for online banking transactions. As the EMV protocol has no notion of transaction details like beneficiary's account number and amount, HHD specifies how reader devices aggregate those details into a challenge for the smartcard. The abovementioned chipTAN solution is one implementation of HHD, where the transaction is transmitted to the TAN-Generator, which aggregates the transaction and hands it over to the plugged in debit card.

We based our implementation of NFC-TAN also on the HHD specification. Consequently, the Smartphone app of NFC-TAN contains a software implementation of the TAN-Generator. NFC-TAN is therefore currently compatible with the chipTAN solution but is adaptable to many solutions using EMV based or other specifications since the only strong requirement towards the smartcard is the ability to compute a response for a challenge using a stored secret.

4 Security

Attacks against online banking services can be classified into three main categories: software attacks, physical attacks, and social attacks [32]. Software attacks are the most common and the most threatening attack vectors, because they can be launched against a large number of customers with comparatively small effort and are harder to trace back than social or physical attacks [32].

4.1 Software Attacks

Credential-Stealing and Credential-Abusing Attacks. The credentials of the NFC-TAN method are: password for login authentication and the signature key for transaction authorization. The password could be stolen by key loggers, phishers or social engineers. In addition, mobile malware can steal the password on the Smartphone from balance-checking bank apps which are usually protected by the same password. With NFC-TAN, the signature key is stored on the debit card and therefore out of reach of both malware and tampering.

However, malware on the Smartphone may not have to steal the signature key at all: it may be enough to be able to send a challenge to the debit card and obtain a signature. We describe how this attack is prevented in the NFC-TAN method by two countermeasures the server can implement, assuming state of the art server side session handling: (i) Only one open login-session for one customer is allowed at a given time, (ii) the server-challenge includes a nonce. Because the customer only brings the card to the Smartphone in order to confirm a transaction (and therefore has an open session) an attacker cannot initiate a transaction on its own (he would need to have an open session). The nonce prevents pre-play attacks, because a challenge obtained earlier is invalidated when the associated session is closed (at the latest), and the customer cannot open a session if the attackers is still open.

In a variant of this attack - with a collaborating malware on the PC that hijacked the customers session - Smartphone malware could try to forward an additional, malicious challenge to the debit card while the user is holding his card close to the Smartphone. This attack is prevented by allowing only one transaction at a given time and introducing a pause of some seconds between transactions.

We can conclude that the use of the debit card as a credential protects the NFC-TAN method against credential-stealing attacks. Credential-abusing attacks by Smartphone malware alone are much harder to conduct because the debit card is not permanently connected to the Smartphone. We assume a responsible and attentive customer and the server side countermeasures described above, namely (1) allowing only one session per user, and (2) one open transaction per session at a given time, (3) using a nonce, and (4) enforcing a delay of a few seconds between the completion of one transaction and the start of another one.

Credential-Stealing and Credential-Abusing Attacks are more Dangerous without Debit Card. Photo-TAN is an example of a method in which both credentials password and signature key can be stolen by malware, actually by malware on the Smartphone alone. The signature key is stored on the Smartphone and any attempt to secure it (e.g. key encryption via a pin or another key) is ultimately vain with respect to powerful malware, because malware could just imitate the steps executed preceding the signing algorithm, and finally will find the key. Even a pin will not prevent this because the pin is first tapped and then used in the imitating process. Malware doing this has to be sophisticated and it is not clear what the success expectation of such an attack is in practice. Nevertheless, if such an attack is successful the consequences are fatal: Malware could send the credentials to a remote attacker who can execute any banking transaction at any time! One way to store a key copy-proof on the Smartphone is a Secure Element that never exposes the key but only has a challenge-response interface. For example, Photo-TAN could be extended with such a Secure Element provided by the bank and integrated physically into the Smartphone [27]. Malware then cannot steal the signature key but abuse it by communicating with the Secure Element and conduct an attack in the following way: First the password is tapped when the customer enters it on the Smartphone to check his account balance. Afterwards malware can open an online banking session at any time and can abuse the Secure Element to compute a signature for an arbitrary transaction without knowing the key. Restricting access to the SE for all but some signed apps may hinder this attack considerably.

This example demonstrates that using a Secure Element with permanent contact to the Smartphone can lead to vulnerabilities not present in the proposed NFC-TAN solution. It also shows that the variant of the NFC-TAN method with an NFC chip stuck on or plugged into the Smartphone is a severe degradation in terms of security though its usability is desirable. Another security issue is the distribution of the credential to the users Smartphone. A practical disadvantage for a bank is the administration effort of yet another credential.

The mobileTAN solution uses the phone number as credential. Regarding Smartphone malware that approach suffers from the fact that text/SMS messages are not considered deserving special protection on Smartphones and are generally accessible by apps, once the user granted a permission to do so – quite a common permission to ask for by all sorts of apps offered. One attack that exploits this situation is described in [29]. Another possible attack is executed by Smartphone malware alone: after stealing the account password mobile malware logs into the customers bank account and initiates a malicious transaction, intercepts the text message on the mobile phone, picks the tan and confirms the transaction. This attack can be conducted anytime the mobile is online and completely without notice to the user as no user interaction is required.

Content-Manipulation Attacks. A man-in-the-browser can manipulate the communication between bank server and PC-browser showing the transaction the customer entered, but communicating a forged one - a second display suffi-

ciently separated from the PC defeats this attack. If a Smartphone with Internet access is used as second display, a content-manipulation attack can only be conducted by collaborating malware on PC and Smartphone, because both displays have to be manipulated:

PC malware cannot manipulate the transaction because the Smartphone will display it again.

Mobile malware cannot manipulate the transaction because the correct transaction was displayed on the PC and is already known to the server.

Only collaborating malware on PC and Smartphone can perform a distributed men-in-the-middle attack by manipulating both displays. This remains a vulnerability of the NFC-TAN solution and is another example of the fact that two insecure systems do not result in a secure system.

Both malware instances need to know the original transaction (to be able to display it) and the forged transaction (in order to send it to the server resp. the debit card). They may communicate the transactions via 2D code, Wi-Fi, or an Internet server. The attack preparation includes finding and infiltrating both devices of one customer with malware. The actual independence of PC and Smartphone therefore is an important measure for the estimation about how complicated and how probable such attacks are. For example, sharing a Wi-Fi network or establishing a cable connection to synchronize calendars may increase the likelihood of a double infection.

Double infection is only a necessary prerequisite for an attack on NFC-TAN the attack itself still has to be conducted as a real-time manipulation attack. The difficulty of the attack step against the Smartphone app is probably comparable to the key theft from a Photo-TAN Smartphone app. The coordination of two distributed malware instances on PC and Smartphone alone is neither a real obstacle to attackers. Nevertheless, the attack has to involve the customers debit card and therefore the customer's interaction. Firstly, this greatly reduces the opportunities of an attack from 'nearly always' to about 'once every few days'. Secondly, the attack has to be executed in the moment the user wants to confirm a transaction, that is, within a few seconds. Therefore this attack is more difficult than the double infection attack on mobileTAN reported in [29].

4.2 Physical Attacks.

Physical attacks are often considered to be less important in the online banking context because they cannot be launched against a large number of customers. In general we agree with that estimation, therefore we only discuss one aspect particularly interesting for NFC-TAN:

Wireless Attack. Enabling access to the TAN computation functionality of the debit card via NFC introduces new vulnerabilities and customers' concern because an attacker could contact the debit card unnoticed by the owner. However, the attacker still would have to know the account number and account

password to complete his attack. Depending on the implementation neither the account number nor the card number can be read via NFC. Even if an attacker can associate a card with an account number and has stolen the password, a real-time attack is necessary because the server-challenge includes a nonce that prevents replay and pre-play attacks: the attacker would have to have simultaneously: an open bank session, a valid challenge and a NFC-connection within a range of 25cm [20]. Summarizing, the wireless attack is a negligible threat to NFC-TAN.

4.3 Social Attacks

For NFC-TAN customers, one reasonable briefing is important: "Only introduce your debit card to the Smartphone if you want to confirm an online banking transaction you initiated!" Then the abovementioned credential-abusing attack can be defeated because the customers open online banking session on the PC prevents Smartphone malware from opening a parallel covert one. The NFC-TAN user has a chance to prevent such an attack without an in-depth notion of the underlying security.

The user could still be tricked into signing a bogus transaction (e.g. for "service test reasons") with the NFC-TAN solution like with almost all other solutions including secure signature creation devices. This kind of attacks is easily prevented by reasonable instructions and customers attentiveness but very hard to prevent without.

4.4 Protocol / Cryptography

Since our implementation does not introduce a new protocol but reuses the specification for transaction authorization with debit cards HHD, we did not perform a security analysis of the protocol or the involved algorithms. The Smartphone does neither store a credential nor perform critical computation exactly like the TAN-generator in the HHD implementation. Since the secret on the debit card is symmetric our implementation of NFC-TAN is also symmetric. A public key implementation of NFC-TAN would be possible with suitable debit cards.

5 Usability

One obvious usability disadvantage as compared to other Smartphone solutions is the additional step of holding the debit card close to the Smartphone. This is balanced by the following advantages.

No Additional Device. This is especially important in a mobile scenario (e.g. in an Internet cafe) because the user does not want to carry an additional device he can lose or forget.

Convenient Communication and Display. The transaction is transferred from the PC to the Smartphone via a 2D code resp. a 2D code scanner on the Smartphone. This is usually completed in less than a second and familiar to users, as 2D codes are quite widespread. The user checks the transaction on the Smartphone display where it is possible to show a transaction completely and comfortably. In fact, the customer may check the transaction only on the Smartphone, because a manipulation by malware on the PC alone would not be a threat.

Offline Availability. The NFC-TAN method does not require an active mobile Inter-net connection on the Smartphone and therefore can be used abroad or in areas with bad network connection. This is a usability advantage compared to other solutions like mobileTAN.

Exchangeable Smartphone. As the Smartphone is a mere communication device, it is exchangeable, for example by a newly bought one or a friends one. Likewise, the credential can easily be delegated since it is stored on the debit card - this may be of benefit in a company account scenario. However, customers may prefer if Smartphone and debit card are paired, e.g. because they may consider this as an additional prevention of the abovementioned wireless relay attack.

Increasing Penetration of NFC-enabled Smartphones. In 2012 over 26% of all Smartphones sold in Europe were NFC-enabled [15], global numbers should be similar. It is to be expected that a significant part of the customers will have NFC-Smartphones in the near future.

6 Complexity: Implementation, Integration and Administration

Minimal Credential Administration Changes on the Server. Banks already maintain debit cards as credentials. The NFC-TAN solution can be integrated into this system without changes to server-side credential management and distribution. Especially, no further credential is introduced and has to be administrated in parallel on the server side. If a bank already uses chipTAN/HHD for online banking, our NFC-TAN implementation can be integrated with minimal server-side efforts: only the flicker-code has to be replaced by a 2D code. This is only a user interface change, whereas business logic on the background servers remains unchanged. Consequently, both methods can be offered simultaneously to the customer.

Smartphone Application Development. In order to support NFC-TAN, a bank's Smartphone app needs to be extended by the following functionality: 2D code scanner, software implementation of the smartcard reader (TAN-Generator), and NFC communication. Although this is not trivial, there is no implementation risk because the technologies are well-known.

NFC-enabled Debit Cards. NFC-TAN needs only minimal software changes on the EMV/HHD debit card - probably only the activation of NFC is necessary (*Dual Interface*). In Germany, debit cards may be NFC-enabled in the medium term for this functionality - currently an electronic purse application on the debit card of some banks can be accessed via NFC.

7 Costs

As online banking providers are profit-oriented companies, their primary attention clearly lays on cost. Other factors are important mainly because they affect costs and revenue. This means that investments for better security measures including implementation, integration and administration have to pay off at the end of the day.

Non-Recurring expenses. The implementation of the NFC-TAN method requires development and integration costs for server and Smartphone software, see Section 6. The distribution of the NFC-enabled cards will most likely occur within the regular exchange of bank cards. Moreover, no additional software needs to be developed and installed on the debit card, see Section 6. In other words, the requirement of NFC-enabled debit cards adds no expense - neither for banks nor customers.

Recurring Expenses. The NFC-TAN method adds no direct recurring costs for a bank like device costs or per-transaction costs. Nevertheless, there will be special indirect costs like customer support and Smartphone app maintenance and indirect costs like server administration and credential management. These costs are comparable to those of other methods.

Expenses for the Customer. The customer - if he wants to use NFC-TAN - has to buy an NFC-Smartphone. This may be interpreted in the way that banks move parts of their costs to their customer.

8 Variants and Extensions

8.1 NFC-TAN Mobile Banking (Single-Channel)

Customers may demand the following single-channel mobile banking variant of NFC-TAN: the user logs into his bank account on the Smartphone with an app or on the mobile browser and enters a transaction, and confirms it by holding the NFC debit card close to the Smartphone. This raises security issues comparable to those already discussed in Sect. 4.1. The main problem is that mobile malware alone can conduct a transaction manipulation attack. NFC-TAN mobile banking should therefore be protected by further server-side mechanisms like beneficiary white-lists, transaction limits, etc., or a *trusted mode* like suggested in [2].

8.2 OCR instead of 2D Code

In the NFC-TAN method the transaction is transferred from the PC to the Smartphone via a 2D code. Instead, the Smartphone app could take a snapshot of the filled transaction form and recognize the transaction via OCR. This What-You-See-Is-What-You-Sign variant increases usability because the customer does not have to check the transaction on the Smartphone. Moreover, this increases security against a man-in-the-PC-browser which may speculate that user does not double-check the transaction on the Smartphone and therefore manipulate the transaction. This OCR extension of NFC-TAN may also allow a convenient and secure way to allow for collective transfers - no double-checking on the Smartphone is necessary.

8.3 Online NFC-TAN

In the NFC-TAN method, the TAN is manually transferred to the PC and then sent to the server. As a variant, the Smartphone could also send the TAN to the server via mobile Internet. This increases usability because the customer does not have to type the TAN. However, the Smartphone would have to have mobile Internet connection. Another disadvantage is increased implementation complexity on the server-side because the TAN receiving script has to be integrated.

8.4 Secure Displays

The main vulnerability of the NFC-TAN is a result from the fact that common Smartphones do not have a secure display. However, NFC-TAN could be combined with some secure display approaches. One solution would be a smartcard having a display [27] and additional NFC-functionality. Another solution could be a Smartphone with a secure display (ARM TrustZone® / G&D MobiCore®) and still use the debit card as a bank owned external credential in case there are reasons for not storing the credential on the Smartphone, like complexity, integration and administration overhead for a new credential.

9 Conclusion

We present NFC-TAN as a solution for online banking transaction authorization that uses the customers debit card as credential and his Smartphone for communication. The NFC-TAN solution is more secure than pure Smartphone solutions without sacrificing much usability. It is less secure than the secure signature creation device solutions but more convenient. Integration complexity and costs on the bank side are comparatively low since no additional credential needs to be managed. Summarizing, NFC-TAN is an online banking method with a trade-off between security, usability, and costs which was not possible until the recently beginning ubiquity of NFC-enabled devices.

Acknowledgement

We would like to thank Klaus Reinhardt and Matthias Sattler for many interesting discussions and the reviewers for their valuable hints and remarks.

References

1. 1822direkt GmbH: Modernes Online-Banking mit QR-TAN (2012), https://www.1822direkt.com/service/zugangsmoeglichkeiten/
2. Alpár, G., Batina, L., Verdult, R.: Using NFC phones for proving credentials. In: Proceedings of the 16th international GI/ITG conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance. pp. 317–330. Springer-Verlag (2012)
3. Blom, A., Koning Gans, G., Poll, E., Ruiter, J., Verdult, R.: Designed to Fail: A USB-Connected Reader for Online Banking. In: Jøsang, A., Carlsson, B. (eds.) Secure IT Systems, Lecture Notes in Computer Science, vol. 7617, pp. 1–16. Springer Berlin Heidelberg (2012)
4. Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S., Anderson, R.: Chip and Skim: cloning EMV cards with the pre-play attack (2012)
5. Borchert, B.: Sichere Verschlüsselung für Online Accounts durch ein Gerät mit Kamera, Display und Nahfunk als Mittler zwischen Rechner und Geheimnis. German patent DE102009040009B4 (2009).
6. Borchert, B., Reinhardt, K.: Vorrichtung und Verfahren zur abhör- und manipulationssicheren Verschlüsselung für Online-Accounts. German patent DE2007052734B4 (2007).
7. Commerzbank AG: photoTAN, http://www.commerzbanking.de/
8. Cronto Limited: CrontoSign Device (2012), http://www.cronto.com/crontosign-transaction-authentication-device.htm
9. Cronto Limited: CrontoSign Mobile App (2012), http://www.cronto.com/crontosign-transaction-authentication-mobile.htm
10. Die Deutsche Kreditwirtschaft: chipTAN, http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/electronic-banking/chiptan.html
11. Dodson, B., Sengupta, D., Boneh, D., Lam, M.: Secure, consumer-friendly web authentication and payments with a phone. In: Conference on Mobile Computing, Applications, and Services (MobiCASE 10) (2010)
12. Dossogne, J., Markowitch, O.: Online banking and man in the browser attacks, survey of the belgian situation. In: Goseling, J., Weber, J.H. (eds.) Proceedings of the 31th Symposium on Information Theory in the Benelux WICSITB2010. pp. 19–26 (2010)
13. Drimer, S., Murdoch, S., Anderson, R.: Optimised to Fail: Card Readers for Online Banking. In: Dingledine, R., Golle, P. (eds.) Financial Cryptography and Data Security, vol. 5628, pp. 184–200. Springer Berlin Heidelberg (2009)
14. EMVCo LLC: EMV Integrated Circuit Card Specifications for Payment Systems, Book 1-4 (2008), http://emvco.com/
15. GfK SE: Smartphones Bring Fresh Boost (2013), http://www.gfk.com/news-and-events/press-room/press-releases/Pages/Smartphones-bring-fresh-boost.aspx
16. Günther, M.: Sicheres Online Banking via Smartphone mit Nahfunk (NFC). Master's thesis, Universität Tübingen (2011)

17. Handelsblatt: Online-Banking wird sicherer (2008), http://www.handelsblatt.com/technologie/it-tk/it-internet/internet-online-banking-wird-sicherer/3064982.html
18. Hiltgen, A., Kramp, T., Weigold, T.: Secure Internet banking authentication. Security Privacy, IEEE 4(2), 21–29 (2006)
19. Hisamatsu, A., Pishva, D., Nishantha, G.G.D.: Online banking and modern approaches toward its enhanced security. In: The 12th International Conference on Advanced Communication Technology (ICACT). vol. 2, pp. 1459–1463 (2010)
20. Kirschenbaum, I., Wool, A.: How to Build a Low-Cost, Extended-Range RFID Skimmer. In: 15th USENIX Security Symposium. pp. 43–57 (2006)
21. Laurie, B., Singer, A.: Choose the red pill and the blue pill: a position paper. In: Proceedings of the 2008 Workshop on New Security Paradigms. pp. 127–133. ACM, New York, NY, USA (2008)
22. Ortiz-Yepes, D.A.: Enhancing Authentication in eBanking with NFC-Enabled Mobile Phones. In: ERCIM News. No. 76, European Research Consortium for Informatics and Mathematics (2009)
23. Sattler, M.: Einbinden der neuen NFC-Debitkarte in das Fotohandy. Master's thesis, Universität Tübingen (2012)
24. Seal One AG: Seal One USB (2011), http://www.seal-one.com/products-list.en-UK.html
25. Shah, M.H., Braganza, A., Morabito, V.: A survey of critical success factors in e-Banking: an organisational perspective. European Journal of Information Systems 16(4), 511–524 (2007)
26. Singh Brar, T.P., Sharma, D., Singh Khurmi, S.: Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research (2012)
27. Starnberger, G., Froihofer, L., Goeschka, K.M.: QR-TAN: Secure Mobile Transaction Authentication. In: International Conference on Availability, Reliability and Security ARES '09. pp. 578–583 (2009)
28. Syverson, P.: A Taxonomy of Replay Attacks. In: Proceedings of the Computer Security Foundations Workshop VII. CSFW 7. pp. 187–191 (1994)
29. The H Security: Millions stolen with mTAN fraud (2012), http://www.h-online.com/security/news/item/Millions-stolen-with-mTAN-fraud-1763923.html
30. Utakrit, N.: Review of Browser Extensions, a Man-in-the-Browser Phishing Techniques Targeting Bank Customers. In: Australian Information Security Management Conference (2009)
31. Vasco Inc.: DIGIPASS 260 (2013), http://www.vasco.com/products
32. Weigold, T., Hiltgen, A.: Secure confirmation of sensitive transaction data in modern Internet banking services. In: World Congress on Internet Security (WorldCIS). pp. 125–132 (2011)
33. Zentraler Kreditausschuss: Schnittstellenspezifikation für die ZKA-Chipkarte - HandHeldDevice (HHD) (2010)