CyberusLabs

A Tale of Two Technologies

Comparison of Cyberus Key to NFC based solutions

INTRODUCTION

What is NFC

Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1.6 in) of each other.

NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smartcards and allow mobile payment to replace/supplement these systems. This is sometimes referred to as NFC/CTLS (Contactless) or CTLS NFC. NFC is used for social networking, for sharing contacts, photos, videos or files. NFC-enabled devices can act as electronic identity documents and keycards.

NFC offers a low-speed connection operating at a frequency of 13.56 MHz.

Use as a Mobile Payment System

Mobile payment is used in stores and to make remote location payment via messages or mobile apps. Different types of mobile payment mediums, such as near-field communication (NFC), have been developed to provide faster money transactions.

The mobile payment industry witnessed an important development when Apple announced the launch of Apple Pay, its new payment feature. This feature enables iPhone 6 and 6 plus customers to make payments at more than 200,000 retail locations in the U.S. In addition, in 2015, Starbucks Corp. launched the Mobile Order & Pay Program across the U.S. to enable customers to preorder and avoid waiting in long queues, thus boosting the market growth. Growth in e-commerce industry, increased penetration of smartphones, change in lifestyle, and the need for quick and hassle-free transactions drive the market growth.

However, **data breaches** and **security concerns** impede this growth.

BENEFITS AND WEAKNESSES

Benefits

Convenient
The convenience of payment is one of this system's greatest advantages. NFC makes it very easy for users to make instant payment via their smartphones and tablets, using their mobile wallet. This process of payment is also simple to understand and use. It helps users perform financial transactions at the mere touch or tap of their screen.

Versatile
NFC is very versatile, in that it covers a range of different industries and services. This mode of payment can be used for the purposes of mobile banking, reserving restaurant seats and movie passes, booking train tickets, getting real-time updates on expenditure and reward points, redeeming rewards and coupons and much, much more.

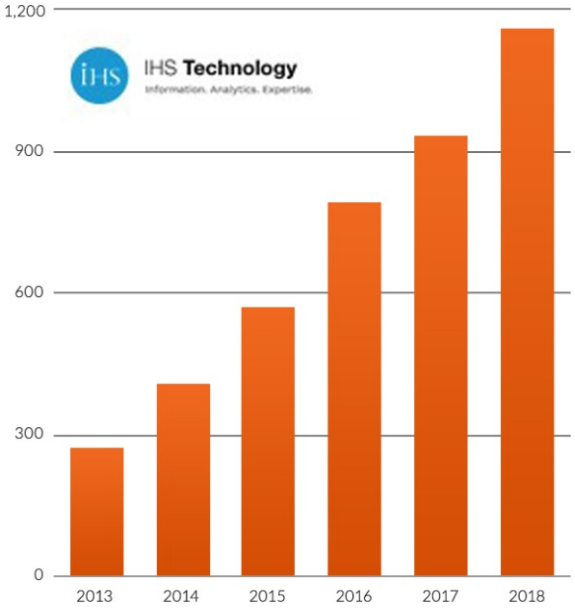
Better User Experience
This system is beneficial for enterprises too – companies that readily adopt the latest technology are viewed by customers as being dynamic and progressive. Using this technology also helps them serve their customers better by presenting them with an easy and hassle-free mode of payment. Offering better user experience helps establishments enhance their own productivity and efficiency, thus enabling them to sustain customer loyalty, while also attracting newer customers.

Weaknesses

LACK OF UNIVERSALITY

Even today, only 64% of all mobile phones shipped in 2018 will be NFC-enabled, up from 18.2% in 2013.

Global shipments of NFC-enabled mobile phones are more than four times higher in 2018 than in 2013, the researchers add, with annual shipments increasing from 275m units in 2013 to 1.2bn units in 2018.



UPBEAT: Forecast for world shipments of NFC handsets, in millions. Source: IHS

HIGH COST OF NFC

It may prove to be much too expensive for companies to adopt NFC-enabled technology; to purchase and maintain related machines and other equipment. While large and well-established companies such as Starbucks have successfully incorporated the technology within itself; smaller companies could find it difficult to sustain their existing turnover and enhance profits. Installing the hardware and software and hiring technicians to maintain the same could result in spiraling expenses.

The high cost of NFC is already slowing down adoption of NFC-based solutions in small and mis-sized companies – who will be at a disadvantage, as they stand to lose current customers looking for easier, more integrated and contactless methods of payment.

CYBERSECURITY WEAKNESSES

Eavesdropping

Eavesdropping is arguably the number one threat facing all NFC contactless payments. The term refers to a criminal "listening in" on an NFC transaction.

Interception Attacks

In addition to eavesdropping attacks, users are also vulnerable to interception attacks. They function in a similar way to man-in-the-middle attacks: a hacker receives information from one device, alters it, then passes it to the intended recipient.

Proximity Attacks

Researchers presented a demo of a real world attack, to which all NFC capable Android phones are vulnerable. This attack, delivered through infected apps, exploits the NFC feature allowing hackers to steal money from victims' credit cards anytime the cards are near the victims' phone.

MiTM & Malware Attacks

ENISA in its report *Security of Mobile Payments and Digital Wallets* has identified **a list of the major risks** related to mobile payment applications.

Mobile Payment Application Users Threats directed against the users of mobile payment applications are:

- Phishing and social engineering attacks
- Installation of rogue applications and malware
- Mobile Payment & Digital Wallet Applications Threats Reverse engineering the application source code
- Exploit of mobile payment application vulnerabilities
- MiTM attacks against the POS contactless terminal and POS server connections
- Relay attacks against NFC enabled POS contactless terminal
- Payment fraud

The report also states that for Providers that relay on fingerprint biometrics for user authentication: *"Extensive research has proven that fingerprint authentication can be bypassed and has been shown to be breakable."*

USER EXPERIENCE WEAKNESSES

Typing in Usernames, Passwords and Codes.
This is another weakness of any NFC based login/transaction system. It touches not only security (as those elements are the target for cybercriminals) but also is a poor UX. When using NFC based system to perform transaction user typically must:

1. log in to his/her bank's mobile app user must put some Log-in details to get in = a) cybersecurity threat and b) poor UX – user needs to remember and type login details which is frustrating and wasting of time.
2. user receives 6-digit code = a) cybersecurity threat (code can be taken over by hackers) and b) poor UX as this slows down the confirmation process
3. user types 6-digit code = poor UX again
4. user confirms transaction on the smartphone.

This is anything but an easy and simple to use system. Users are still forced to receive and retype codes which are especially frustrating when it needs to be rewritten on the same device (in case of using the mobile app).

A TRULY SIMPLE & SECURE ALTERNATIVE

Cyberus Labs has developed a revolutionary new technology platform called CYBERUS KEY that enables secure transactions between devices using high-frequency sound-waves. Comparing to NFC's "universality" among the devices actually limited to 64% of the newest ones on the market that are NFC enabled (not to mention lower percentage in the older ones), 99% mobile devices have speakers and microphones so this is the first method which is the most universal and easiest to adapt for the largest audience. This communication protocol works across all mobile, laptop and hardtop devices with no extra hardware needed and no linking process – just place the devices in proximity and secure communication can occur.

SECURITY

Below we present list of reasons **why CYBERUS KEY is better than NFC-based systems**:

1. CYBERUS KEY only requires an app on users cell phone, no NFC chip, so it's more universal
2. CYBERUS KEY only requires a regular, browser capable tablet as POS. No special NFC POS required, so it's more universal.
3. All CYBERUS KEY sonic traffic is encrypted and it's only an OTP, no credit card information is transmitted.
4. NFC relay attacks are a form of Man in the Middle, CYBERUS KEY transaction confirmation defeats that.

For ENISA's list of threats for Mobile Payments and Digital Wallets CYBERUS KEY is a perfect solution and eliminates all of them:

- **Phishing and social engineering** – no passwords or/and actionable credentials eliminate the reason for those attacks.
- **Installation of rogue applications and malware** – installation of the malware is pointless as there is no user/card data stored in the device or browser and Out-of-band communication prevents from the system being exploited and gives an early warning in such exploitation's attempt.
- **Mobile Payment & Digital Wallet Applications Threats Reverse engineering the application source code** – application is only a signal/one-time token decoder and no reverse engineering is possible. On merchant/POS side only regular browser is required so no Reverse engineering is possible. Any Browser compromising thanks to Out-of-band communication results in such compromise detection and early warning to both: merchant and user.
- **Exploit of mobile payment application vulnerabilities** – CYBERUS KEY eliminates the root of this problem by eliminating the use of any credentials: user login, credit card/bank account details and provides strong user authentication.
- **MiTM attacks against the POS contactless terminal and POS server connections** – POS being a simple tablet or laptop is being only a one-time token transmitter via browser. As there are no user/credit card/ bank account information in use installation of the malware is pointless. The entire user authentication cycle and payment process is fully anonymous for the unauthorised 3rd party.
- **Relay attacks against NFC enabled POS contactless terminal** – there is no use for rely attacks in case of CYBERUS KEY as the entire authentication cycle takes approx. 200 ms and uses Out-of-band communication in connection of one-time tokens so the token cannot be used for any other than transaction. CYBERUS KEY defeats the purpose of the relay attacks.
- **Payment fraud** – CYBERUS KEY is a proximity based user authentication system that provides by its nature a geofencing feature.

As the most recent research revealed cyber attacks that are after user credentials, passwords and identity **(phishing, man in the middle, social engineering attacks)** are **responsible for 80% of all data breaches**.

CYBERUS KEY eliminates all those kinds of attacks and by the game-changing approach of post-credential-era user authentication **solves over 80% of cybersecurity threats leading to data breaches**.

User Experience

CYBERUS KEY is not only more secure than any other user authentication technology. It provides also much improved user experience – so much desired by companies. CYBERUS KEY provides not only the bank-level security but also great UX:

- Easy clients onboarding (users will not have to remember, type in any usernames /passwords anymore)
- Frictionless, one click login CYBERUS KEY cuts down user multifactor user authentication to only 2 clicks!
- Faster login / transaction confirmation than any other system – 3 sec vs 1 minute average = 20 times faster.
- No more rewriting/typing received codes via SMS which is particularly frustrating when login with one device.
- CYBERUS KEY Out-of-band channel does the secure authentication automatically

USER LOGIN/TRANSACTION CONFIRMATION PAINS:

USERS' PAINS	CYBERUS KEY SOLUTION
pain of remembering, storing, using passwords	eliminates passwords
login with passwords takes long time	1 min traditional login vs 3 sec CYBERUS KEY logon = **20 x faster**
passwords can be mistyped and lock account	no need to retype anything
use call centre to unlock account/recover password	no such need - no passwords
poor UX in user authentication (incl. biometrics)	1 click = 3 sec 2 factor CYBERUS KEY logon
complicated transaction confirmation	1 click transaction confirmation
long time for transaction confirmation with SMS rewrite	25 sec transaction with token vs 3 sec with CYBERUS KEY - 1 click = **8 x faster**
frustrating UX in transaction confirmation	nothing to retype, 1 click confirmation

Entire CYBERUS KEY Login UX with mobile app has been cut to:

1. Start the app (this performs already proximity based 1st factor of authentication ensuring fraud prevention within one second).
2. Use fingerprint sensor to confirm user identity and provide 2nd factor.

Transaction confirmation is cut down to 2 steps:

1. See the transaction confirmation message on the mobile device (that in case of compromised browser shows the fraudulent transaction info).
2. With one click user either confirms or (unlike with other systems) has a chance to refuse transaction.

A TRULY UNIVERSAL PAYMENT SYSTEM – CYBERUS PAY

CYBERUS PAY is a fully universal PAYMENT SYSTEM for ALL merchants and ALL customers. Brings bank-level security and extreme ease of use to the masses.

CYBERUS PAY is the game-changing solution and the most universal payment system ever provided.

CYBERUS PAY architecture enables the turn of each and any ordinary tablet or laptop that any type of merchant can use – from a fruit stand to luxury car dealer – to an easy to use and secure POS.

> *CYBERUS PAY architecture enables the turn of each and any ordinary tablet or laptop that any type of merchant can use – from a fruit stand to luxury car dealer – to an easy to use and secure POS. This enables massive adoption of the contactless payment also in the areas where the we have great volume of small transactions – like ordinary, every-day grocery shopping and others.*

This enables massive adoption of the contactless payment also in the areas where the we have great volume of small transactions – like ordinary, every-day grocery shopping and others.

The massive adoption is enabled by two drivers:

1. ease of use of the system for end clients: 2 click to login and perform transaction – a really frictionless UX
2. merchant does not need to install anything. All the merchant needs is a tablet/laptop and the browser to have fully functional POS at their disposal.

That is the easiest POS setup ever.

Entire infrastructure is enabled by Service provider / Bank installation of the CYBERUS KEY at their side.

Moreover, there is **no internet coverage needed to make a payment transaction**. It is sufficient to have a 5G connection and speakers/microphone activated in both devices e.g. merchant's tablet and client's smartphone.

It has another positive effect on the economy: service providers and the banks can collect the fees that at this moment Apple/Samsung/Google are collecting (which are huge).

END-TO-END SOLUTION FOR NEW REGULATIONS – PSD2

CYBERUS KEY is also a system providing secure user authentication and transaction confirmation required by the PSD2 directive for Banks & TPPs cooperation.

Strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud are among the the main points of the PSD2 directive.

The new directive brings key changes that include:

Security of online payments and account access through the introduction of new security requirements for electronic payments and account access.

The direct connection between retailers and banks will be enabled using Application Programming Interface (API).

A strong customer authentication system – third party access to accounts (XS2A), the use of API's to connect merchant and the bank directly and the ability to consolidate account information in 1 portal.

At the same time the TPPs must ensure that the highest levels of security are implemented also on their side as they will be handling payments of banks customers.

CYBERUS KEY offers a possibility to play a role of the platform connecting banks and TPPs. It is one of the main features of the CYBERUS KEY.

The idea behind the system to:

- enable secure login to user account
- provide quick and secure access to user's account at the bank and TPP based on Federated ID
- enable secure transaction
- secure anonymous online operation while operator has a full information about the payee
- provide with time, date and geolocation information about account login and transaction

CYBERUS KEY is an user authentication and payment confirmation platform that answers the requirements of the PSD2 directive. System enables banks' customer to access the account and make any online transaction.

A crucial part of the system is a CYBERUS KEY Authentication Server (CAS). The installation of CYBERUS KEY within banks IT infrastructure ensures the safety of users' data that the bank is responsible for.

But CYBERUS KEY does much more than that.

For every bank's customer being registered to the service an anonymous profile is created on the CYBERUS KEY Authentication Server (CAS). Only this server and only the data and user profile stored on it is being used for the logon/ transaction confirmation purposes. That means that no actionable user's credentials are being used to perform any of the above mentioned operations. CYBERUS KEY is using the concept of the Federated ID system. The only elements that CYBERUS KEY uses are:

- one-time-code that uses One-Time-Pad methodology generated by the HSM
- app and smartphone unique ID and profile data

That allows to keep actionable users credential within the bank's infrastructure and not to transmit them outside of it and still being able to perform online transactions, without the risk of unauthorized parties being able to intercept those information and misuse it or even steal the credentials.

Why is this so important in case of the PSD2 directive? One of the biggest fears of the banks will be sharing their users' data with TPPs. Another is creating a common platform that uses API to connect with TPPs.

CYBERUS KEY is an answer for this. It is an already existing platform with a ready API that offers a possibility of an anonymous Single-Sign-On solution based on the Federated ID system. Contrary to the present SSO solutions that transmit user credentials, the sign-on process with use of the CYBERUS KEY is anonymous. Only a one-time-code and user profile is being used for this operation.

How does this solve problem of PSD2 requirements? Every TPP that wants to make transactions for the banks customer needs to be integrated with the use of API with bank. CYBERUS KEY system gives a solutions to banks and TPPs working together and to perform client's online transactions without sharing customer credentials or any identifiable data between banks and TPP during this process. In case of implementing CYBERUS KEY in the bank it is enough that bank's users are also CYBERUS KEY enabled TPPs users or vice versa. TPPs that will adopt CYBERUS KEY will have its own separate data base of the customers that are at the same time customers of the bank behind its own firewall.

> *CYBERUS KEY system gives solutions to banks and TPPs to work together and to perform client's online transactions without sharing customer credentials or any identifiable data between banks and TPP during this process. In this case, when making a transaction for a customer with its bank there is NO user's information/credentials shared between the entities. However – at this same time both operators will receive information about the transaction. That eliminates the biggest threat of any online transaction – user's credentials and payment details being transferred online.*

In this case, when making a transaction for a customer with its bank there is NO user's information/credentials shared between the entities. However – at this same time both operators will receive information about the transaction. That eliminates the biggest threat of any online transaction- user's credentials and payment details being transferred online.

CYBERUS KEY AND PSD2 STRONG CUSTOMER AUTHENTICATION REQUIREMENTS

The PSD2 directive also refers to "strong customer authentication" several times. A strong customer authentication is now a core of the technical security standards for payment services in Europe.

PSD2 *defines "Strong Customer Authentication" as authentication based on the use of two or more elements categorized as:*

- *Knowledge – something only the user knows*
- *Possession – something only the user possess*
- *Inherence – something the user is*

Each are independent, so the breach of one does not compromise the reliability of the others. CYBERUS KEY *uses smartphone as a universal key to any* CYBERUS KEY *enabled online service/website.*

System provides a strong customer authentication required be EU directive with:

a) using a smartphone – something user possess

b) implementing solutions for securing a CYBERUS KEY with:

- PIN code – something only the user knows,
- biometric technology chosen by the operator – something the user is

It is, however, very important to remember that biometric technologies should be used as a second factor authenticator and not the first one.

In case of biometric credentials being stolen users loses a chance to login with use of biometric technologies to their account forever. If biometric is used as a second factor it can easily be replaced with PIN.

For higher security requirements CYBERUS KEY can integrate within one system multiple layers of authentication factors, depending on the operator's needs.

From the PSD2 directive regulations emerges strong need of a one integrated 2 factor authentication system that is easy to install within banks IT infrastructure and is also simple to use and secure for banks customers.

CYBERUS KEY is such system. It not only delivers in one integrated system all the features that at present are being delivered by various systems that need to be integrated later with banks IT system. CYBERUS KEY:

1. is easy to install within any internal bank's IT infrastructure (ready API),
2. uses one-time code that is being used for every login or transaction confirmation,
3. one time code is generated by Hardware Security Module (HSM) and is based on the only unbreakable encryption system called One-Time-Pad or Vernam Cypher,
4. creates anonymous profile of every registered banks customer stored on the CYBERUS KEY Authorization Server (CAS) that is installed behind bank's firewall to ensure security,
5. uses only one-time-code and anonymous user profile to perform online transactions (login and transaction confirmation),
6. no customers' actionable credentials are being used or transmitted during any operation,
7. for all transactions uses out-of-band communication to ensure full security,
8. transaction information includes date, time and geolocation information that are available to the bank and customer. They also may be transferred to fraud engines of the bank and by delivering precise information of made transactions form and analyze customer behavior patterns that will be used to trigger early warning signals preventing fraudulent operations,
9. out-of-band communication also prevent CYBERUS KEY users from performing unauthorized transactions. Even when cybercriminals would be able to infect browser and change the transactions details they will be passed in this changed form to customer who will be able to reject it, fully aware of the fraud attempt,
10. provides integrated 2 factor authentification system.

The above mentioned advantages and features are making CYBERUS KEY a game-changing: universal, easy to use & install multifactor user authentication and payment platform that is also an answer for banks and TPPs cooperation in light of the new legal requirements of the EU's PSD2 directive.

Powered by

Cyberus Labs Sp. z o.o.
ul. Warszawska 6/309
40-006 Katowice, Poland

e-mail: office@cyberuslabs.com
tel.: +48 692 437 857
www.cyberuslabs.com