# Mobilfizetési megoldások biztonsági kockázatainak elemzése

***Juhász-Nagy Attila***

*Óbudai Egyetem, Neumann János Informatikai Kar*

## Tartalmi összefoglalás

A napjainkban zajló pénzpiaci átalakulások egyik leggyorsabban terjedő területe a mobil fizetési megoldásoké. Néhány éve robbanásszerűen kezdtek terjedni a *PayPass*-os bankkártyák, napjainkban pedig már az okostelefonunkat, vagy akár az okosóránkat is használhatjuk úgy, mint egy *PayPass* képes bankkártyát. A bankkártyás vásárlás ezen formája nemcsak gyors, de nagyon kényelmes és nyugodtan állíthatjuk, hogy még trendi is.

A technológia fejlődése nem minden esetben jár együtt a helyes felhasználói magatartás terjedésével. A technológiai újdonságokra fogékonyabbak rendszeresen élen járnak az új technikai megoldások használatával, de nem szabad megfeledkezni, hogy az újdonságok új kihívásokat és új veszélyeket is rejtenek. Az eszközök és szolgáltatások használata közben a felhasználókra leselkedő biztonsági kockázatok minimalizálása érdekében az embereknek ismerniük kell a fenyegetések részleteit legalább olyan mélységben, hogy lehetőségük legyen tudatosan védekezni ezen kockázatok ellen.

Dolgozatomban arra voltam kíváncsi, hogy milyen veszélyek ismertek az NFC-alapú mobilfizetési megoldásokkal kapcsolatban, és hogy ezek közül melyik kockázat mennyire jelent veszélyt a felhasználókra a mindennapi életben.

## Az NFC technikai áttekintése

Az *NFC* (*Near Field Communication*) technológiát egy globális konzorcium fejlesztette ki, ami számos nemzetközi szabvány által meghatározott technológián alapul. Ez a szabvány lehetővé teszik az információk könnyű továbbítását kis távolságokon (nagyjából 10 centiméter) belül. Az *NFC* képesség egy mobiltelefont (újabban akár okosórát is) olyan eszközzé alakíthat, ami alkalmas fizikai objektumokhoz csatolt adatok olvasására, képes két mobileszköz közötti adatcserére, vagy akár különféle termékek, például tömegközlekedési jegyek/bérletek, belépő- és bankkártyák „utánzására” (Cavoukian 2011).

Az *NFC*-t korábban már létezett és bevált technológiákra építkezve tervezték. Két fő specifikáció határozza meg a működését, melyek az ISO/IEC

14443 és az ISO/IEC 18000-3 szabványnak felelnek meg. Az ISO/IEC 14443 leírja az információk tárolására használt azonosító kártyákat (*ID card* vagy *ID chip*) és azok működését. Ilyenek például az *NFC*-címkékben található *RFID* chipek. Az ISO/IEC 18000-3 szabvány meghatározza az *NFC* eszközök által használt *RFID* kommunikációt (nearfieldcommunication.org 2020).

Az ISO 14443 szabvány definiálja a HF (13,56 MHz) tartományban működő, magas biztonsági szintű, kis hatósugarú (kb. 10 cm), úgynevezett *Proximity RFID*-eszközök működését. A szabvány a közelítőkártyák és olvasók működését szabályozza annak érdekében, hogy a különböző felhasználási területeken (pl.: személyazonosítás, fizetés, tömegközlekedés, biztonság, és beléptetés) kompatibilitást biztosítson. A szabvány négy részre osztott, melyből az egyes modulok leírják az eszközök fizikai jellemzőit, a működés során használt rádióhullámokat és a sugárzási energiát, a jeladó berendezést, az *inicializáló* folyamatot, az ütközésmentesítést (*anti-collision*) illetve az átviteli protokollt (ISO/IEC_14443-4 2018).

Az *RFID* név mögé több szabvány is tartozik, melyek más-más frekvenciákat, eltérő adóteljesítményeket adnak meg, amelyek alapján akár jóval nagyobb távolságból is megvalósítható a kommunikációt két megfelelő eszköz között. Azonban az *NFC* nem valósítja meg az összes ilyen szabványt, csak a közeli kommunikációra vonatkozókat. Csupán említésképpen, az *RFID*-szabványnak van olyan modulja, ami például raktárépületekben árumozgások követését is lehetővé teszi, a címkék leolvasásának lehetőségét több méterről is biztosítva. Mindehhez persze speciális címke és hozzá megfelelő specifikációjú leolvasóberendezés szükségesek. Erre a nagytávolságú átvitelre az *NFC* technológia értelemszerűen nem alkalmas, és nem is kíván az lenni.

Az *NFC* nemcsak kompatibilis a már széles körben elterjedt *RFID*-technológiákkal, de erősen épít is ezekre, amelyek milliónyi hozzáférési, fizetési és azonosítókártyán megtalálhatók. Így hozzáférhetünk információkhoz vagy használhatunk olyan adatokat, amelyek elérhetők egy kialakult *RFID*-infrastruktúrán keresztül. Ide kell érteni a különböző helyeken megtalálható *RFID*-címkéket (*tag*-ek, pl.: pályaudvarokon, boltokban vagy múzeumokban), és az *RFID*-leolvasókészüléket (pl.: bankkártyaterminálok, beléptetőrendszerek, kártyaolvasók). Az *NFC* különösen jól használható mobileszközökben, ahol működését és viselkedését az eszköz tulajdonosa ellenőrzi (Cavoukian 2011). A működés ellenőrzésének köszönhetően az *NFC* képességgel rendelkező eszközök különféle üzemmódokban más és más funkció ellátására lesznek képesek, melyek a következők:

*Reader/Writer* – ez az *NFC*-üzemmód lehetővé teszi a mobileszközök számára a nyilvános plakátokba, kijelzőkbe és termékekbe ágyazott passzív *RFID*-címkékben tárolt kódolt adatok kiolvasását, és azokra az adatokra való reagálást, amelyek tartalmazhatnak egy *URL*-címet vagy más szöveges adatot. Ez lehet egy fájl vagy egy weboldal címe és az eléréshez szükséges egyéb adatok. Továbbá a bekódolt információ lehet hívás kezdeményezésére vonatkozó utasítás vagy az SMS-üzenetek küldéséhez vagy internethozzáféréshez tartozó beállítás. Az alkalmazási területek közé tartozik továbbá a kommunikációs kapcsolatok létrehozásához szükséges adatcsere (pl.: bonyolultabb, magasabb szintű kapcsolatok, *WiFi*, *Bluetooth* beállítási adatai) gyorsítása, valamint az eszközök közötti azonosítási folyamat (pl. mobiltelefon – *headset* párosítása) gyorsítása vagy elvégzése (Curran et al. 2012). Ez az *NFC*-mód lehetővé teszi továbbá a mobileszközök számára, hogy adatokat írjanak egyes címkékbe vagy akár más mobileszközök virtuális címkéibe.

*Card Emulation* – egy *NFC*-eszköz kártyaemulációs-módba is kapcsolható, hogy kompatibilis legyen más érintés nélküli intelligenskártya-szabványokkal. Ez a működési mód lehetővé teszi, hogy a mobileszközöket azonosítási, fizetési és beléptetőalkalmazásokhoz használják. Így lehetősége nyílik a mobileszköz-tulajdonosoknak, hogy érintés nélküli üzleti tranzakciókat hajtsanak végre, ugyanúgy, mint manapság az intelligens (*PayPass*-képességgel bíró) bankkártyákkal. Számos alkalmazás elérhető okostelefonokra és okosórákra, amikkel kiválaszthatjuk, hogy az eszközünk milyen kártya működését utánozza le.

*Peer* – ez az *NFC*-mód lehetővé teszi a mobileszközök számára, hogy könnyebben lépjenek kapcsolatba egymással (ehhez mindkét telefonnak rendelkeznie kell *NFC*-vel és az engedélyező alkalmazásokkal), hogy gyorsan elindítsák a mobilkommunikációt az adatok egymás közötti megosztásához, akár névjegykártyák cseréjéről, fotók vagy dokumentumok, esetleg más típusú személyes adatok *peer-to-peer* adatátviteléről van szó.

Az *NFC* tehát egy rövid hatótávú kommunikációs szabványgyűjtemény, általában mobileszközök között (pl.: mobiltelefon, okostelefon, okosóra), vagy mobileszköz és aktív/passzív *NFC*-eszköz között. Az *NFC* magába foglal egy kezdeményező- és egy céleszközt. A kezdeményező, ahogyan a névből is következik, *iniciálja* a kapcsolódást és a kommunikációt, illetve ő állítja elő a működéshez szükséges *RF*-jelet(rádió frekvenciás, elektromágneses), és ellenőrzi az adatcserét.

Az *NFC*-protokoll két kommunikációs módot is megkülönböztet: AKTÍV és PASSZÍV. Egy jó példa az aktív eszközre a bankkártyaterminál (*POS*) az üzletekben történő fizetés estén, ahol a kommunikációs kérésre egy passzív eszköz (bankkártya vagy okostelefon) válaszol (Curran et al. 2012).

A kezdeményező- és a céleszköz az alábbi táblázatnak (*1. táblázat*) megfelelően lehet aktív vagy passzív:

*1. táblázat* NFC eszközök működési módjai

| | **Kezdeményező** | **Cél eszköz** |
|---|---|---|
| **Aktív** | Lehetséges<br>pl. POS-terminál | Lehetséges<br>pl. Peer-to-peer mobileszköz |
| **Passzív** | Nem lehetséges | Lehetséges<br>pl. PayPass bankkártya |

Abban az esetben nevezzük AKTÍV-nak a kommunikációt, mikor a kezdeményező és a cél egyaránt kommunikál saját elektromos mezőjének létrehozásával. Félduplex módban teszik mindezt, vagyis deaktiválják a saját RF-mezőjüket arra az időre, amíg a másik eszköz továbbít adatokat. Ebben az üzemmódban általában mindkét eszköz saját tápegységgel rendelkezik.

A PASSZÍV üzemmód jelenleg a legelterjedtebb alkalmazási mód, ahol a kezdeményező az egyetlen eszköz, amely *RF*-jelet generál, a céleszköz a hívásra úgy válaszol, hogy módosítja a meglévő mezőt, amelyet a létrehozó eszköz meghallgat, majd feldolgozza az érkezett adatokat. A jelenleg támogatott adatsebességek a következők: 106, 212, 424 vagy 848 Kbit/s (Curran et al. 2012).

Az *NFC*-kapcsolódás lehetséges egyszerűbb, passzív, energiatáplálást nem igénylő eszközzel is, az úgynevezett *NFC*- vagy *RFID-tag*-gel. Ilyen eszköz többek közt a *PayPass* fizetésre alkalmas bankkártya. Ez esetben az *NFC-tag*-en tárolt információkat aktív eszköz segítségével lehet leolvasni (Haselsteiner/ Breitfuß 2006).

Az *NFC* az adatcserék során az *NFC Data Exchange Format* (*NDEF*) formátumot használja. Az *NDEF* egy szabványos formátum a kódolt adatok *NFC*-címkéken történő tárolásához és az adatok *NFC*-eszközök közötti, *peer-to-peer* kapcsolatokon keresztüli továbbításához.

**Biztonsági kérdések**

Az NFC egy újnak mondható és innovatív technológia, futurisztikus felhasználással, de a technológiának ára van. A legrelevánsabb kérdések talán azok, hogy az új technológia mennyire sérülékeny, mennyire tudhatjuk biztonságban személyes és pénzügyi adatainkat a használata során (Chattha 2014).

Az *NFC*- és az *NDEF*-technológia egyre növekvő számú alkalmazásával egyre több biztonsági fenyegetés vált nyilvánvalóvá, mivel egyre több tapasztalat gyűlt össze a biztonsági hiányosságokkal kapcsolatban (Roland et al. 2011). Éppen ezért indokolt az adatvédelem és a biztonsági szempontok beépítése a mobileszközök architektúrájába, beleértve a fizikai kialakítást, az operációs rendszereket, az alkalmazásokat és a szolgáltatásokat, különös tekintettel a hatékony felhasználói felületekre és az alapvető adatvédelmi lehetőségekre.

Számos tervezési szempont áll a fejlesztők rendelkezésére, hogy a lehetséges veszélyeket kezeljék. A *Design by Privacy* az egyik ilyen szempont, melynek alapelvei a mobileszközök és megoldások tartományára is érvényesek. A mobil adatvédelmi ökoszisztéma, ahogyan sok más rendszer, több komponens és protokoll együttműködéséből épül fel. A kommunikációs láncolat minden elemének biztonságosnak kell lennie, hiszen ennek kritikus szerepe van a felhasználók bizalmának megtartásában és növelésében (Cavoukian 2011).

Az *NFC*-szabvány terjedésére bizonyosan erős fékező hatással lenne a felhasználók részéről érkező negatív megítélés, ha biztonsági problémákról és adatlopásokról, meghamisított tranzakciókról, meghiúsult vagy éppen indokolatlan belépésekről lehetne hallani a technológia használata során. A felhasználók szeretik személyes, lokáció, pénzügyi és igazából különösebb válogatás nélkül az összes adatukat biztonságban tudni. Vannak, akik az információbiztonságra nagyobb figyelmet fordítanak, és vannak, akik kevésbé óvatosak. Viszont ha az emberek nincsenek tisztában azzal, hogy a technológia hogyan védi az adataikat, a privát zónájukat, és ezért bizalmatlanok a technológiával szemben, akkor nem fogják azt használni. Ez gátat szab az adott megoldás terjedésének, illetve könnyen ki is szorulhat a piacról más helyettesítő megoldások által. Fontos, hogy a felhasználók minél inkább tisztában legyenek az eszközök (legyen az szoftver, hardver vagy szabvány) nyújtotta lehetőségekkel és kockázatokkal. Ehhez a fejlesztés oldaláról is ismerni kell ezeket a lehetőségeket és kockázatokat.

**NFC alapú mobilfizetés**

Az NFC-eszközök, hála a gyors terjedésnek, kiválóan használhatóak érintésmentes fizetési eszközként, elektronikus jegyként, valamint helyettesítik, kiegészítik vagy megvalósítják a mobilfizetési megoldásokat. Utóbbira jó példa a GOOGLE (*Android Pay*) az APPLE (*Apple Pay*) vagy többek közt az OTP (*Simple*) szolgáltatása, ahol a felhasználó bankkártyájának adatait egy virtuális pénztárcában tárolják és NFC-kompatibilis eszközzel használva érintésmentes fizetésre használható például a MASTERCARD *PayPass*-termináljain.

Az *NFC* biztosítja a vásárlók számára a fizetési információk cseréjét, például a vásárló mobilkészüléke és a kereskedő *POS*-terminálja (értékesítési pont) között, egyszerűen a mobileszközöket a terminál közelében (általában 10-20 cm) tartva. Előfordulhat, hogy a biztonság fokozása érdekében bizonyos összeghatár felett a felhasználónak PIN-kódot vagy jelszót kell megadnia a tranzakció jóváhagyásához.

A fogyasztók számára az *NFC*-mobilfizetés több előnnyel is rendelkezik. Ezek közé tartozik a megbízhatóság, a biztonság, az érintésmentes fizetés lehetősége, a könnyű használat és a kényelem. Továbbá a gyakori használatra nyújt lehetőséget az, hogy nagyon sok elfogadóhelyen fizethetünk *NFC*-vel. Az előnyöket tovább szélesítik a telefonra letölthető változatos funkcionalitású alkalmazások (Liu et al. 2013).

2012 és 2014 között volt egy jelentős ugrás a magyarországi mobilfizetési megoldások terjedésében. Ekkor jelent meg több bank a *PayPass* képességgel rendelkező bankkártyákkal. Ezt követően már csak pár év kellett ahhoz, hogy a külföldön népszerű *NFC*-képességű, okostelefon-használaton alapuló mobilfizetés Magyarországon is terjedni kezdjen 2017 környékén.

Ez a terjedés várhatóan a jövőben is tart, és több feltételnek az együtteséből is adódik. Szükség van arra, hogy a hazai okostelefon-felhasználók jelentős arányban használjanak olyan készüléket, ami képes *NFC*-t használva bankkártyaként működni. Továbbá szükség van az egyes mobilplatformokon olyan alkalmazásokra, amik itthon is elérhetőek, esetleg valamely hazai pénzintézet saját fejlesztése. A harmadik tényező, amit érdemes figyelembe venni, az az emberek kíváncsisága, fogékonysága az új dolgok iránt, mely szintén fokozhatja egy új technológia terjedését.

**Az NFC gyengeségei**

Nem szabad megfeledkezni a vezetéknélküli kommunikációk azon jellemzőiről, melyek a rádiófrekvenciás átvitelből következnek. Ezek közé tartozik, hogy

könnyen lehallgathatók az üzenetek, zavarható a csomagok átvitele, esetleg részben vagy egészében meghamisíthatók a közlekedő adatcsomagok. Ezeket a lehetőségeket mindig érdemes észben tartani, amikor az *NFC*-s fizetést használjuk (Trottmann 2012).

Az *NFC*-képesség megléte a mobiltelefonokban, okosórákban és minden egyéb mobileszközön, amibe beépítésre kerül, hasonlóan a *Blueetooth*-hoz, új lehetőségeket és új fenyegetéseket jelent. Míg az *NFC* gyökeresen megváltoztatja a vásárlások teljesítésének módját, ugyanakkor lehetőséget nyit rosszindulatú személyek, csoportok számára, hogy visszaélhessenek az *NFC* által kínált lehetőségekkel és kényelemmel. Ez a veszély magában foglalja azokat a károsnak minősíthető *NFC*-címkéket, amelyek egy mobiltelefon veszélyeztetésére képesek. Továbbá rosszindulatú eszközöket, bankkártya-leolvasókat, amelyek hamis mobil fizetési tranzakciókat próbálnak létrehozni, vagy éppen értékes pénzügyi információkat próbálnak meg ellopni (Gummeson et al. 2013).

A telefonban a bekapcsolt *NFC* a szabvány szerint folyamatosan keresi és próbálja leolvasni a címkéket. A címkeadatokat vagy az operációs rendszer funkcionalitása, vagy egy harmadik fél által fejlesztett alkalmazás dolgozza fel, és a feldolgozott adat szerint fog viselkedni az alkalmazás és/vagy a készülék. A folyamatosan bekapcsolt *NFC*-vel fokozott biztonsági kockázatnak tesszük ki az okoseszközünket és saját magunkat. Nem elhanyagolható szempont, hogy az energiaigényes *RF*-kommunikáció miatt bekapcsolt rádióadó a megnövekedett áramfelvétel miatt le fogja rövidíteni az okoseszközünk készenléti idejét, esetleg még a készülék melegedését is okozhatja.

Vannak olyan dokumentált biztonsági fenyegetések, amik megadott NFC-Android verziópáros esetén jelent kockázatot. A számtalan eszköz és az Android operációsrendszer verziókombináció miatt nem minden említett sebezhetőség érinti egyformán az eszközöket. (Bermejo et al. 2020) Számos NFC kommunikációs szabvány nem használ titkosítást az adatcsomagokon, mivel a rövid hatótáv garantálja a kommunikáció lehallgathatatlanságát. Azonban verzióktól függetlenül lehetőség van a felhasználó által meglátogatni kívánt weboldal másolatának elkészítésére és a hamisított oldalnak az eredetihez hasonló *URL*-címet regisztrálni. Az *NFC*-technológia lehetővé teszi, hogy weboldalaknak a címe legyen beégetve egy *RFID-tag*-be, ami elhelyezhető például egy reklámplakát sarkában. Ha a felhasználó nem elég óvatos, és a *tag* leolvasását követően megjelenő weboldal címében és magán az oldalon nem veszi észre a hamisítást, akkor megadhatja a bankkártyaadatait vagy bármilyen más, értékes adatokat a támadók weboldalán. (Bermejo et al. 2020)

**Lehetséges védekezés**

A körültekintő és tudatos felhasználói magatartás mellett a legjobb vagy leginkább javasolt módszer, hasonlóan a *Bluetooth*-hoz és a mobilinternet-kapcsolathoz, hogy csak akkor engedélyezzük az *NFC*-kommunikációt az eszközünkön, ha azt éppen használni készülünk. Így több kellemetlenségtől is meg tudjuk óvni magunkat, eszközünket és adatainkat. Van már lehetőség azonban arra is, hogy ne csak passzívan, az *NFC* használatának és a bankkártyás fizetés szabályainak betartásával, tudatos felhasználói magatartással előzzük meg az adataink vagy pénzünk eltulajdonítását, hanem aktív eszközökkel is.

Egy ilyen eszköz az ENGARDE, amely a telefon hátuljára ragasztható, hogy képes legyen meghiúsítani a rosszindulatú interakciókat. Az ENGARDE teljesen passzív, és ugyanazon *NFC*-forráson keresztül nyeri a működéséhez szükséges energiát, amelynek biztonságáért felel. Ez a megoldás minimalizálja hardverünk fizikai méretét és megkönnyíti az integrációt a mobileszközzel. A legfontosabb technikai kihívásokat sikerül megoldani ebben a kialakításban, ideértve az *NFC*-protokollok széles skálájának támogatását, a rendkívül alacsony energiafogyasztást, miközben minimális hatással van a telefon akkumulátorára. Olyan intelligens zavaró készüléket hoztak létre az ENGARDE megalkotói, amely csak akkor blokkolja az NFC-kommunikációt, ha az eszközbe épített feketelistán szereplő viselkedést észlel a készülék. Amit még érdemes kiemelni, hogy ezek a funkciók a felhasználói élmény veszélyeztetése nélkül olyankor aktiválódnak, amikor a telefon egy legitim külső *NFC*-eszközzel lép kölcsönhatásba (Gummeson et al. 2013).

**Felhasználói észlelt kockázatelmélet**

Csakúgy, mint a termékvásárlások során, a szolgáltatások kiválasztása során is döntési helyzetbe kerülnek a fogyasztók. Ez a fogyasztói döntések során a racionalitás sérül, hiszen a felhasználók nem képesek minden tényezőt számba venni, amely az adott eszköz vagy szolgáltatás előnyeihez, illetve hátrányaihoz kapcsolódik.

Az egyének bizonyos mértékű kockázattal szembesülnek, ha egy adott döntés társadalmi és gazdasági következményekkel járhat valamilyen bizonytalanságból fakadóan. A felhasználói kockázatészleléssel több tudományterület foglalkozik, pl. a közgazdaságtan, a pszichológia, a menedzsment, a kockázat- és biztosítási diszciplínák, a közpolitika és a pénzügyek. Az elmúlt években az észlelt kockázatelméletet széles körben alkalmazták a kereskedelemmel kapcsolatos informatikai innovációkra is,

amelyekben a fogyasztók magatartása az informatikai technológiák használatában a kockázatvállalás példájának tekinthető. A fogyasztók észlelt kockázatát széles körben egyfajta többdimenziós konstrukciónak tekintik. Az észlelt kockázatnak öt részdimenzióját különíthetjük el az internetes banki műveletek során, ezek sorban: a teljesítmény-, a társadalmi, az idő-, a pénzügyi és a biztonsági kockázatok (Liu et al. 2013).

## Irodalomjegyzék

Bermejo, C., Flores, H. and Hui, P.: "Notice of Retraction: Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags," *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Austin, TX, USA, 2020, pp. 1-6, doi: 10.1109/PerComWorkshops48775.2020.9156089.

Cavoukian, A.: Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private. 2011

Chattha, N. A.: NFC – Vulnerabilities and defense. *2014 Conference on Information Assurance and Cyber Security (CIACS)*, 2014, pp. 35–38. OI: 10.1109/CIACS.2014.6861328.

Curran, K., Millar, A., Mc Garvey, C.: Near Field Communication. *International Journal of Electrical and Computer Engineering*, Vol.2, No.3, June 2012, pp. 371–382. ISSN: 2088-8708

Gummeson, J., Priyantha, B., Ganesan, D., Thrasher, D., Zhang, P.: EnGarde: protecting the mobile phone from malicious NFC interactions. *Proceeding of the 11th annual international conference on Mobile systems, applications, and services* (*MobiSys '13*). Association for Computing Machinery, 2013, New York, NY, USA,
pp. 445–458. DOI: https://doi.org/10.1145/2462456.2464455

Haselsteiner, E., Breitfuß, K.: Security in Near Field Communication (NFC). *Workshop on RFID Security*. 2006, Philips Semiconductors

ISO/IEC 14443-4:2018 „Cards and security devices for personal identification — Contactless proximity objects" (https://www.iso.org/standard/73599.html), utoljára megtekintve: 2020. 12. 05.

Liu, Y., Kostakos, V., Deng, S.: Risks of using NFC mobile payment: Investigating the moderating effect of demographic attributes. *In Proceedings of the 15th International Conference on Electronic Commerce*, 2013, pp. 125–134.

(http://nearfieldcommunication.org/technology.html), utoljára megtekintve: 2020. 12. 10.

Roland, M., Langer, J., Scharinger, J.: Security Vulnerabilities of the NDEF Signature Record Type. *2011 Third International Workshop on Near Field Communication*, Hagenberg, 2011, pp. 65–70, DOI: 10.1109/NFC.2011.9.

Trottmann U.: NFC – Possibilities and Risks, *Seminar Future Internet WS2012*, 2012, Fakultät für Informatik, Technische Universität München