GAZDASÁG ÉS PÉNZÜGY • 11. ÉVF. 3. SZ. • 2024. SZEPT. • DOI: 10.33926/GP.2024.3.5

AZONNALI FIZETÉSI KÖZPONTI INFRASTRUKTÚRA KONTRA FIZETÉSI MEGOLDÁS[1]

Czímer József – Kiszely Róbert – Biró-Lebovits Máté[2]

ABSZTRAKT

Az utóbbi években az azonnali fizetés bevezetése lett az egyik uralkodó tendencia a pénzforgalmi szolgáltatások terén. E rendszerek közös tulajdonsága: mindegyik azt az igen nehéz feladatot oldja meg, hogy egy pénzösszeget az egyik bankból a másik bankba átutaljon pár másodperc alatt folyamatosan, a nap 24 órájában. Minden létrehozott rendszer egy bankok közötti, központi infrastruktúrát tartalmaz, amelynek az a feladata, hogy lehetőséget nyújtson a tranzakciók gyors és biztonságos lebonyolítására. Az új rendszerek bevezetése ugyanakkor nem eredményezte azt, hogy azok kiszorítsák a korábbi fizetési megoldásokat. Mi lehet ennek az oka? A rövid válasz erre a kérdésre az, hogy az azonnali fizetési infrastruktúrák a bankokat kötik össze egymással, míg a fizetési megoldások a fizetési tranzakciók két végpontja, a fizető fél és a kedvezményezett között létesítenek kapcsolatot. A cikk ezt a témát járja körül azzal, hogy megvizsgálja, hogyan lehet egy azonnali fizetési központi infrastruktúrából egy komplex fizetési megoldást létrehozni. A cikk szerzői a Capsys Informatikai Kft. munkatársaiként részt vettek a társaság által lebonyolított Kutatási és Fejlesztési (K+F) projektben, amelynek célja ennek a kérdésnek a megválaszolása volt. A szerzők részesei voltak továbbá a Magyar Nemzeti Bank által kezdeményezett „Azonnali fizetés 2.0" projektnek is. Ezt azért hozták létre, hogy a magyar központi azonnali fizetési infrastruktúrát egy nemzeti fizetési megoldássá változtassa az újonnan bevezetett „qvik" brand alatt.

JEL-kódok: E42, O32

Kulcsszavak: azonnali fizetés, EAM, digitális aláírás, csalásmonitorozás

1 Összeférhetetlenség: A szerzők kijelentik, hogy a cikk megírásával kapcsolatban nem áll fenn semmiféle összeférhetetlenségük.

2 *Czímer József* London Office vezető, Capsys Informatikai Kft. E-mail: jozsef.czimer@capsys.hu.
Kiszely Róbert levelező szerző, igazgató, Professional Services, Capsys Informatikai Kft. E-mail: robert.kiszely@capsys.hu.
Biró-Lebovits Máté, Sales Representative, Capsys Informatikai Kft. E-mail: mate.biro-lebovits@capsys.hu.

1. AZONNALI FIZETÉSI KÖZPONTI INFRASTRUKTÚRÁBÓL FIZETÉSI MEGOLDÁS

Amint az azonnali fizetési rendszer 2020 márciusában sikeresen elindult Magyarországon, a Capsys szinte azonnal a következő kérdés megválaszolását tűzte ki célul: hogyan hozható létre egy olyan fizetési megoldás, amelynek a természetes alapja egy azonnali fizetési tranzakció? Ennek a kérdésnek a megvizsgálására a társaság által lebonyolított kutatási és fejlesztési (K+F) projekt keretében több olyan megoldást is megvizsgáltak, amelyek az azonnali fizetést próbálták alapul venni részben empirikus, részben tudományos módszerekkel. Minden olyan kritériumot megvizsgáltak, amelynek egy ilyen megoldásnak meg kell felelnie, valamint figyelembe vették az összes megkerülhetetlen körülményt és természetesen az is, hogy milyen lehetőségeket ad a technológiai fejlődése. A kutatás egyik fő eredménye annak a megállapítása volt, hogy egy életképes fizetési megoldásnak a következő hat feltételnek kell megfelelnie:

a) Legyen könnyű a használata – úgy a fizető, mint a kedvezményezetti oldalon könnyen kezelhetőnek kell lennie a rendszernek, ellenkező esetben a tömeges elterjedés nem biztosítható.

b) Legyen olcsó (alacsony díjak) – a könnyű megfizethetőség minden ágazatban fontos, főként egy olyanban, amelyben a piac tradicionális szolgáltatói már alacsonyra tették a szintet.

c) Legyen gyors – a fizetési tranzakciót a két végpont között pár másodperc alatt kell lebonyolítani.

d) Legyen megbízható – amennyiben a rendszer használói problémákkal találkoznak és azokra nem kapnak gyors választ, nem fogják azt használni.

e) Legyen biztonságos – csalások, visszaélések azóta léteznek, amióta az emberek fizetési műveleteket végeznek. A fizetési megoldásnak a csalások lehetőségét az elérhető minimumra kell csökkentenie.

f) Legyen széles körben elérhető – az olyan fizetési megoldás, ami csak kevés helyzetben használható, vagy nem ér el elég ügyfelet, elszigetelt megoldásokat eredményez, összezavarja és frusztrálja a felhasználókat.

Következő lépésként összegyűjtötték azokat a fizetési helyzeteket, amelyekben az azonnali fizetés is alkalmazható lehet. Igen sok ilyen van, például a bolti fizetés, szolgáltatói számlák kifizetése, szállítói számla kifizetése küldemény átvételekor, online fizetés, postai fizetés stb. Fontos volt biztosítani, hogy a lista teljes legyen, így a teljes képre lehetett később összpontosítani, és nemcsak valamelyik elemére.

Egy jó fizetési megoldás megtalálásához az adat- és információátvételi technológiák minden szóba jöhető fajtáját meg kellett vizsgálni. Ilyenek a QR-kód, az NFC, a deep link, a bluetooth (BLE), de idetartoznak a fizetési kérelem és más

egzotikus megoldások is. Amikor a fizetési helyzeteket és a szóba jöhető technológiákat összepárosították, kialakult az az általánosan elfogadható megközelítés, amely minden fizetési helyzetet lefed.

2. A FELTÉTELEK ELEMZÉSE

2.1. Könnyű használhatóság

Egy fizetési megoldás akkor tud elterjedni, ha az azt használók kényelmesnek találják az alkalmazását. Az egyik jó példa a „kényelem" illusztrálására az online kereskedelemben történő kártyás fizetés – be kell ütni a számítógépbe a bankkártya 16 karakterből álló számát, lejárati idejét, ami további négy leütés, és jön még három leütés, ami a biztonsági kód. Miután ezek az adatok a kártyán olvashatóak, ezért a szabályozás – és a józan ész – alapján egy második, független azonosítás is szükséges. Ez az azonosítás történhet oly módon, hogy a rendszer egy pushüzenettel megkéri a felhasználót, hogy hagyja jóvá a tranzakciót a bankja által szolgáltatott applikáció használatával. Ez az eljárás nehezen nevezhető kényelmesnek. Vannak ettől eltérő módszerek, például a kártyaadatokat egy harmadik fél tárolja, bár ezt a módszert a biztonsági szakértők nagyon ellenzik. Hogyan lehet tehát a fizetést kényelmesebbé tenni az ügyfél számára? Vizsgáljuk meg először azokat az adatátviteli technológiákat, amiket fizetési tranzakció kezdeményezésére alkalmazhatunk.

2.1.1. Adatátviteli technológiák

Folyamatos viták folynak a szakemberek között arról, hogy melyik a legjobb technológia egy fizetési művelet kezdeményezésére. Használjuk talán a kedvezményezett által megjelenített QR-kódot? Érintse a fizető fél mobiltelefonját a kedvezményezett eszközéhez? Esetleg a fizető fél azonosítsa magát elsőre, és utána kapjon egy fizetési kérelmet a mobiltelefonjára? Szóba jöhet-e, hogy a fizető fél adjon olyan adatot/információt magáról, aminek a használatával a kedvezményezett megterhelheti fizetési számláját?

A fizetési iparág területén a szakemberek évtizedek során számtalan új megoldást dolgoztak ki. Mint a legrégebb óta létező elektronikus fizetési megoldás, a bankkártya volt mindig a fejlődés motorja, ezért a később fejlesztők is a bankkártya rendszerek logikáját követték: a fizető felet azonosító információ a fizető féltől a kedvezményezetthez kerül, tőle az ő bankjához, majd a fizető fél bankjához annak a kártyatársaságnak a csatornáin keresztül, amelyiknek a neve a kártyán szerepel. Ez az elv kicsit úgy ivódott be a fizetési rendszerekbe, mint a nap a naprendszerbe; körülötte forog minden, ami létezik.

2.1.2. NFC

Az utóbbi évtizedek az NFC[3] – Near Field Communication, azaz magyarul az érintésmentes technológia elterjedését hozták. Az NFC technológiai standard leírása több változatot is tartalmaz, mégis az érintésmentes fizetési kártyák jutnak mindenki eszébe. Ezzel a megoldással egyszerűen lehet fizetni, a bank által kibocsájtott műanyag lapot csak oda kell érinteni egy eszközhöz. Tulajdonképpen a műanyag lapra sincs szükség, mivel a kártyaadatokat a mobiltelefonban, vagy akár egy karórában is lehet tárolni titkosított formában. A technológiai fejlődés egy kiemelkedő példáját jelenti az a megoldás: egy bizonyos mobiltelefon-gyártó a keresletet kielégítve megoldotta azt, hogy eszközeivel akkor is lehet tokenizált kártyát használni, amikor a telefon töltöttségi szintje más funkcióhoz nem elégséges. Egy élő példával illusztrálva a megoldás fontosságát: valaki a londoni metrón odaérinti a mobiltelefonját a kapunál az olvasóhoz, mivel ezzel akar fizetni, de az utazás során a telefon a töltöttségét a kitartó használatnak köszönhetően szinte elveszíti – ekkor egy speciális üzemmódba vált át, szinte kikapcsol. A metró szolgáltatási listáján nem szerepel az emberek fogva tartása, így a kijáratnál az utast mindenképp ki kell engedni. A telefon fent leírt funkciójának köszönhetően az utas akár a lemerült telefont használva is tud távozni.

Az NFC-technológia többet is tud, mint az EMV[4]-protokoll szerinti kártyaadatcsere támogatása. Az NFC olyan URL-adatok továbbítására is alkalmazható, amiket a modern okostelefonok kezelni tudnak. Egy ilyen URL átvezethet akár egy honlapra, akár pedig egy applikációra, vagy mindkettőre egy időben. Az URL-alapú universal linking technológia egy nagyon hatékony eszköz, mert ezzel a fizetés kezdeményezéséhez szükséges interakciók száma minimalizálható. Lényege, hogy egy applikáció egy honlaphoz kapcsolható ezzel a technológiával, így az okostelefon operációs rendszere feléleszti a kapott jelben szereplő honlaphoz kapcsolt applikációt a telefonon. Amennyiben a kereskedőnek van olyan eszköze, jellemzően egy POS-terminál, ami képes NFC-technológiával URL-jelet kibocsájtani, akkor a fizető félnek csak megfelelő közelségben kell tartania az okostelefonját, amelyik a kapott jel alapján azonosítja a megnyitandó applikációt, azt beindítja, és ezzel együtt továbbítja a fizetési művelet végrehajtásához szükséges adatokat is. Amennyiben az így felélesztett applikáció egy olyan mobilbanki applikáció, amelyik képes azonnali fizetéseket kezdeményezni, máris egy új, létező technológiai elemekből álló, azonnali fizetés kezdeményezésére alkalmas megoldást hozunk létre.

3 https://en.wikipedia.org/wiki/Near-field_communication

4 https://en.wikipedia.org/wiki/EMV

2.1.3. QR-kód

A fizetési adatok továbbításáról folytatott beszélgetések során a QR-kód lett a legmegosztóbb technológia. Ennek tulajdonképpen történelmi okai vannak, ugyanis vannak országok, ahol nagyon sok használati területen vezették be, míg máshol kevesebb esetben. Azokban az országokban, ahol a QR-kód az élet részéve vált, ahol az étlap olvasásától a WIFI-kapcsolat létesítésén keresztül a csomagok megcímzéséig használják, értelemszerűen az alkalmazása a fizetések területén is természetes. Ilyen országokban a pénzforgalmi szolgáltatók ezt használják a fizetések kérésére is.

A QR-kód előnye az egyszerűségében rejlik. A technológia egy igen egyszerű megoldás azzal, hogy a karakterek sorozatát fekete pontok sorozataként kódolja. Ezek a pontok egy képernyőn is megjeleníthetők, de nyomtathatók is. Ez a megoldás a QR-kódot széleskörűen alkalmazhatóvá teszi úgy, hogy maga a kódolás nem követel meg komoly technológiai szakértelmet.

A QR-kód URL-kódolására is alkalmazható, azaz ugyanaz a lehetőség rejlik benne, mint az NFC-technológiában. A mobiltelefonok túlnyomó többsége egyébként lehetővé teszi a QR-kódok olvasását és feldolgozását a beépített kamera segítségével.

2.1.4. Deep link

Az utóbbi idő egyik látványos trendje, hogy az okostelefonok elterjedése és a széleskörű internetlefedettség azt eredményezte, hogy az emberek egyre többször használják mobiltelefonjukat áruk és szolgáltatások kifizetésére. A fellelhető statisztikák szerint[5] az elektronikus vásárlások 73%-a okostelefonokon, nem pedig laptopokon vagy asztali számítógépen történik. Ez a jelenség egy új feladatot is ad: hogyan lehet NFC-jelet adni a fizetési művelethez ugyanannak az okostelefonnak, vagy hogy lehet a kamera számára olvasható QR-kódot mutatni? A válasz egyszerű: sehogy!

A megoldást a fenti problémára egy kevésbé ismert technológia, a deep link használata adja. Ez a technológia lehetőséget nyújt arra, hogy egy honlap vagy egy applikáció adatot adjon át egy másik honlapnak vagy applikációnak az okostelefonon. Az azonnali fizetés esetében az így továbbított adatcsomag a fizetési művelet végrehajtásához szükséges adatokat, információkat tartalmazza. Fontos megállapítani, hogy a deep link gyakorlatilag egy pontosan olyan URL, mint az NFC- és a QR-kód-alapú, titkosított adatátvitel esetében alkalmazott URL. Amikor az áruvásárláshoz használt honlapon/applikáción a felhasználó eljut oda, hogy fizetni kellene, a honlap/applikáció feléleszt egy deep linket, ami viszont elindítja a fizetéshez használt applikációt, végrehajtva ezzel egy azonnali fizetési műveletet.

5 https://marketing.dynamicyield.com/benchmarks/device-usage/

A felsorolt három technológia – NFC, QR-kód, deep link – valamelyike felhasználható tehát az egyes fizetési helyzeteknél, legyen az bolti fizetés, számlakifizetés, online fizetés vagy mobiltelefonos fizetés. Az URL formájában mindegyik technológia képes a szükséges adatsor továbbítására, ezért teljes mértékben interoperábilisak, így tehát a fizetési helyzettől függetlenül azonos ügyfélélményt biztosítanak. Az a megoldás, hogy a fizetési applikáció azonnal a jóváhagyási oldalra ugrik, jelentősen csökkenti a felhasználótól megkövetelt interakciók számát, javítva ezzel a felhasználói élményt.

2.2. Alacsony díjak

A díjnak egy fizetési megoldás esetében is több összetevője van. Ezek közül az egyik legérzékelhetőbb az a díj, amit a fizető fél fizet. A fizetési szolgáltatók tradicionálisan tranzakció alapon terhelik ki díjaikat. A bankkártyarendszerek nagyon magasra tették a lécet – vagy nagyon alacsonyra, attól függ, honnan nézzük –: ők ugyanis nem fizettetnek tranzakcióalapú díjat a fizető féllel. Éppen ezért bármilyen fizetési megoldás is csak akkor versenyképes, ha a fizető fél számára nem alkalmaz tranzakcióalapú díjat. Az emberek azért is használnak különféle megoldásokat, mert azok a kényelmen túl divatosak is, de végül is a fizetendő díj szintje diktálja a használatot.

A kedvezményezettek jobban elfogadják a tranzakcióalapú díjazást. A bankkártyarendszerek ezen az oldalon is meghatározták már a szintet, nem valószínű, hogy bármely kedvezményezett elfogadna a jelenlegi költségeinél magasabb díjakat.

A harmadik faktor az új rendszer bevezetésének költsége gyakorlatilag minden szereplőnél. A boltoknak olyan eszközöket kell beállítaniuk, amelyek kezelni tudják az új módszert, az online szolgáltatóknak módosítani kell a szoftvereiket, fizetéskezelési eljárásaikat, a szolgáltatóknak meg kell változtatni a számlázás, illetve a bejövő pénzforgalom kezelésnek a módját. Rövid távon tehát a legegyszerűbbnek és legolcsóbbnak részükről a jelenleg működő rendszerek módosítása tűnik. A tapasztalatok szerint a kedvezményezetteknek az a legegyszerűbb, ha mindent készen kapnak a pénzforgalmi szolgáltatóiktól.

Van mindamellett még egy költségfaktor, amelyet meg kell említeni, ez pedig a technológia komplexitása. Ez a faktor alapvetően a biztonsági követelmények függvénye. Ahogy azt már tárgyaltuk, a fizető felet azonosító információk több szereplőn és rendszeren mennek keresztül, ezért szigorúan védeni kell azokat. Ennek előírásait a PCI-DSS szabvány tartalmazza[6], ami az utóbbi évtizedekben

6 https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

folyamatosan fejlődő, nagyon széles körben elterjedt szabvány. Ez írja elő az érzékeny kártyaadatok továbbításának, kezelésének a módját. Egy lánc éppen olyan erős, amilyen erős a leggyengébb szeme, ezért ez a szabvány a rendszer legkisebb elemét is szabályozza. Jó példa erre: az is pontosan szabályozva van, hogy a POS-terminálától centiméterekre levő PIN-beütő készülékről az adatok milyen kódolással menjenek magához a POS-készülékhez. Világosan látható tehát, hogy ez jelentősen megnöveli az alkalmazott rendszerekhez tapadó költségeket. Azonnali fizetés esetében a fizető felet azonosító információk közvetlenül a bankhoz érkeznek, mivel a mobiltelefon applikációja a bankkal kommunikál. Éppen ezért az adatokat nem kell több szereplőn keresztül kommunikálni, ezért a bankkártyaadatok biztonságos továbbításának a költsége eltűnik a rendszerből.

2.3. Gyorsaság

Az első kérdés, ami az azonnali fizetés esetében rendszerint felmerül, az, hogy a tranzakció kezdeményezési műveletének a végrehajtása elég gyors-e ahhoz, hogy a bankkártyával versenyezzen. Egy bolt esetében nagyon fontos a fizetési művelet végrehajtásának gyorsasága a pénztárnál ahhoz, hogy elkerüljék a sorok feltorlódását. Az online boltok tapasztalata is az, hogy sok függ a vásárlói értékelésben attól, milyen gyors a vásárlás fizetési szakasza.

A korrekt választ erre a kérdésre a hivatalos statisztikák adják meg. A GIRO időről időre kibocsájtja a GIROInstant rendszer működését bemutató számokat:[7] 2024. márciusában az azonnali átutalások átlagos végrehajtási ideje 0,87 másodperc volt, míg a tranzakciók 97,55 %-a két másodpercnél gyorsabban teljesült. Hasonló adatokat láthatunk más hónapok vizsgálata esetében is. Az itt idézett tranzakciós idők ugyanakkor nem csak a bankok közötti átutalási időt tartalmazzák! Amikor az azonnali fizetési rendszert bevezették Magyarországon, a szabályozó a felhasználó szempontjából akarta mérni a rendszert, ezért a hivatalos tranzakciós idő mérése akkor indul, amikor a küldő fél jóváhagyta az utalást, és akkor ér véget, amikor az átutalt összeg odaért a fogadó bankba. Mindezek alapján nyugodtan ki lehet jelenteni, hogy a központi infrastruktúra műveleti sebessége megfelelő.

A teljes fizetési művelet természetesen nem annak a jóváhagyásával kezdődik, hanem figyelembe kell venni a jóváhagyáshoz szükséges lépéseket is. A kedvezményezettnek létre kell hoznia a fizetéshez szükséges adatokat, azokat továbbítania kell a fizető fél eszközére, a fizető fél applikációjának meg kell vizsgálnia az adatokat, fel kell azokat dolgoznia, és csak utána kérheti a művelet jóváhagyását.

7 https://penzforgalom.hu/eng/

Az azonnali fizetés bizonyos szempontból olyan, mint a Forma–1: az autó súlyát minimalizálni kell akár úgy is, hogy még a pedálokba is lyukakat fúrunk. Az azonnali fizetés esetében tehát az adatfolyamnak egyszerűnek, ugyanakkor mindent kielégítőnek kell lennie. A tapasztalatok azt mutatják, hogy a tranzakciós idő hosszúsága szempontjából a legnagyobb problémát a felhasználók interakciói és a rendszerkommunikáció jelentheti.

A felhasználói interakció komoly bizonytalansági tényező a tranzakciós idő tekintetében. Különbözik az ujjunk nagysága és a látásunk is, de mindenkinek különböző az applikációk kezelésében való gyakorlata, mások a szokásai. Mindegyikünk ismer legalább egy olyan valakit, aki a fotók megtekintéséhez megnyitja a kamera applikációt is, holott azok közvetlenül is nézegethetők. Ha sikerül a fizető fél szükséges interakcióinak a számát csökkenteni, az stabilizálja a folyamatot. Éppen ezért a megjelenített információnak mindig világosnak és érthetőnek kell lennie.

A rendszerkommunikáció gyakorlatilag akadálytalanul a háttérben történik. Az átlagos felhasználó ezt a folyamatot csak a homokóra ikon alapján észleli. Az esetek többségében, amikor a rendszer a felhasználó türelmét kéri, éppen egy másik rendszer vagy applikáció válaszára vár. Ezek az interakciók is sok kockázatot rejtenek magukban – nagy lehet az adatforgalom a két rendszer között, nagy lehet a másik rendszer leterheltsége, probléma lehet az alkalmazott eszközzel stb. Világosan látható, hogy ha ezek akár egyike is jelentkezik, megnőhet a tranzakciós idő. Minél többet kommunikálnak egymással a rendszerek, annál nagyobb a kockázat is.

A való életből vett példán keresztül szemléltethető a felhasználói és a rendszer-interakciók hatása. Következzen két lehetőség a fizetési folyamat implementálására egy banki mobil applikációban:

1) Az URL elindítja az applikációt, az applikáció megkéri a felhasználótól az azonosító adatokat (PIN, ujjlenyomat, arcfotó), validálja az adatokat, megjeleníti azokat, és jóváhagyást kér, majd a jóváhagyás után elindítja a fizetési tranzakciót. Ehhez a megoldáshoz két felhasználói interakció szükséges.
2) Az URL elindítja az applikációt, az applikáció megjeleníti az adatokat, és jóváhagyást kér, ami után elindítja a tranzakciót. Ehhez a megoldáshoz egy felhasználói interakció szükséges.

Az első megoldás biztonságosabbnak tűnik, de a második megoldás egyrészt gyorsabb, másrészt kisebb benne a hibázás lehetősége.

Ahhoz, hogy egy azonnali fizetéssel működő fizetési megoldás szülessen, a feldolgozási lánc minden elemének megtervezése, fejlesztése és tesztelése során mindig a gyorsaságot mint alapot figyelembe kell venni.

2.4. Megbízhatóság

Mai világunkban, amikor a számítástechnika óriási fejlődése tapasztalható, a felhasználók az applikációk megbízható működéséhez szoktak hozzá. A felmerülő hibák nemcsak zavarják őket, hanem reklamációra ösztönzik őket, esetleg arra is, hogy szolgáltatót váltsanak. Az, hogy fizessünk valamiért, nem egy alaptevékenység, hanem mindig velejárója annak, hogy egy árut vagy szolgáltatást megkapjunk. Ha csak azért nem kapunk meg egy árut vagy szolgáltatást, mert hiba van a fizetési rendszerben, az nagy felháborodást vált ki. A szolgáltatók ugyancsak a fizetési forgalom zavartalanságában (a folyamatos bevételben) érdekeltek.

Mit okozhat az, ha egy fizetési megoldás kevésbé megbízható? Feljebb már megvizsgáltuk a felhasználói interakció és a rendszerkommunikáció kérdését; mindkettő nemcsak késésekhez, hanem hibákhoz is vezethet. Van persze sok más tényező is, ami hibát eredményezhet. Az egyik ilyen ok annak a környezetnek a növekvő komplexitása, amelyben ezeknek a rendszereknek működniük kell. Ehhez jön még az is, hogy a szabályozói környezet évről évre bonyolultabb. Az üzleti szükségletek így folyamatos fejlesztési kötelezettséget indukálnak, ugyanakkor a költségvetési lehetőségek határokat szabnak az azonnali piacra jutás lehetőségeinek. A csalók egyre újabb lehetőségeket találnak az emberek átverésére, a lyukak megtalálására.

Vegyük példának az online bankkártyás fizetést. A bolti fizetésekhez alkalmazott, nagyon fejlett technológia az online fizetések esetében nem használható, ugyanis nincs a fizető félnél olyan validáló eszköz, amelyet a szolgáltató el tud fogadni. Az egyik módja az online bankkártyás fizetésnek tehát az, hogy a fizető fél beviszi a rendszerbe a bankkártya adatait – kártyaszám, lejárati dátum és biztonsági kód. Erről a megoldásról kiderült, hogy nem biztonságos, a kártyaadatok könnyen ellophatók így. Az egyik legelterjedtebb módja a kockázat csökkentésének a szabályozói nyomásra alkalmazott 3-D biztonsági protokoll.[8] Ez a megoldás egyrészt további interakciót követel meg a fizető féltől, másrészt egy további résztvevőt is bevon a műveletbe, mivel a jóváhagyás a mobilfizetési applikáción keresztül történik. Ez a komplexebb módszer az elkövetett hibák számának a növekedését vonja maga után. Megtörténhet, hogy a mobilapplikáció által használt infrastruktúra leterhelt, a kérés nem éri el a felhasználót, blokkolva ezzel a teljes fizetési folyamatot. Az a szabályozói követelmény tehát, hogy egy második, független azonosítót is alkalmazzanak a fizetéshez és a 3-D biztonsági elem bevezetése jelentősen megnövelte a bankkártyás online fizetés komplexitását. Vannak ter-

8 https://en.wikipedia.org/wiki/3-D_Secure

mészetesen alternatívái ennek a megoldásnak, de azok egyes vélemények szerint alacsonyabb biztonsági fokot biztosítanak.

A folyamatos fejlődés következménye, hogy egyre komplikáltabb megoldások születnek a meglévők helyett. Az elvégzett kutatások eredménye azt mutatta, hogy az azonnali fizetés területén van lehetőség a komplexitás csökkentésére. Az az alapelv, hogy a fizető fél applikációja követlenül kommunikáljon a fizető fél bankjával, egy sor kockázati tényezét kiküszöböl. Természetesen más tényezőket is figyelembe kell benni. Az egyik legkomolyabb aggodalom az, hogy vajon a fizető fél mobiltelefonja rendelkezik-e minden esetben internetkapcsolattal. A globális mobillefedettség 2020-ra elérte a 95%-ot[9], és a fejlődés nem állt le. Nagyon sok esetben a kereskedők is nyújtanak WIFI-kapcsolatot a vásárlóknak. A számlabefizetések és az online vásárlások túlnyomó részét az emberek az otthonukban végzik, ahol az internetkapcsolat az alap infrastruktúra része. Biztosak lehetünk abban, hogy az internetkapcsolat az esetek túlnyomú részében nem jelent problémát.

2.5. Biztonság

A biztonság a fizetések világában mindig is kiemelten fontos kérdés volt, csak korábban ezzel a témával kizárólag a szakértők egy zárt csoportja foglalkozott. Valamelyest most is ez a helyzet: egy nagyobb konferencián a központi teremben mintegy 300 fő vett részt az MI megbeszélésén, míg a fizetési csalások problematikájával 40 ember foglalkozott egy kisebb teremben. Ugyanakkor a biztonság kérdése nagyságrenddel nagyobb figyelmet kapott az elmúlt években, amit a szinte mindenhol megjelenő statisztikák is mutatnak. A csalások technikája, „technológiája" is folyamatosan változik; a csalók mindig más és más módszert alkalmaznak. A statisztikák szerint 2023-ra az elektronikus kereskedelem vesztesége a csalások következtében globálisan elérte a 48 milliárd dollárt.[10]

Minden fizetési megoldásnak kezelnie kell a biztonság kérdését. A korábban bemutatott kártyarendszerek kiforrott megoldásokkal rendelkeznek ebből a szempontból is. Egy új megoldás felhasználhatja ezeket az elemeket abban az esetben, ha a technológiák átfedik egymást, de új biztonsági megoldásokat is kell találni. A mobilbanki applikáció használata a fizető fél és bankja közötti kapcsolat viszonylatában csökkenti a biztonsági kockázatot. A csalók persze nem dőlnek hát-

9 https://en.wikipedia.org/wiki/3-D_Secure

10 https://b2b.mastercard.com/news-and-insights/blog/ecommerce-fraud-trends-and-statistics-merchants-need-to-know-in-2024/

ra, hanem azt próbálják elérni, hogy a fizető fél maga kezdeményezze azt a fizetési műveletet, amit ők szeretnének csinálni.

A QR-kódok legfőbb gyengeségét is az egyszerűségük jelenti. Nagyon egyszerű a QR-kód tartalmát megváltoztatni úgy, hogy azt az emberi szem nem érzékeli. További kockázat, hogy a fizetések számlaszámra történnek, de név is szerepelhet a megbízáson. A fizető fél természetes módon a nevet nézi, de nem tudhatja, hogy az adott számlaszám a névhez tartozik-e. A probléma megoldását a „kedvezményezett igazolása"[11] jelentheti, azaz a pénzforgalmi szolgáltatók egy olyan adatbázist érhetnek el, amelyben ellenőrizhetik egy adott számlaszám tulajdonosát, és fordítva. Ez a megoldás még fejlesztés alatt van, gyakorlati tapasztalatok nincsenek róla. Egy gond lehet a használatával, ez a megoldás megnövelheti a tranzakció komplexitását, a végrehajtás idejét és a lehetséges hibák számát is. A jelen cikkben bemutatott K+F projekt máshogy közelítette meg a kedvezményezett és a hozzá tartozó számlaszám integritásának biztosítását. Nem a kerék újbóli feltalálásáról van szó, sokkal inkább egy széles körben elterjedt technológiáról: amennyiben egy adatsort valaki digitálisan aláír, az adatsor sértetlenségének ellenőrzéséhez nem szükséges rendszerkapcsolat, ugyanakkor a biztonság szavatolható.

2.5.1. Digitális aláírás

Első látásra az adatbiztonság és az azt támogató kriptográfia tudománya nagyon komplikáltnak és ijesztőnek tűnhet. Kétségtelen, hogy a mély megértéséhez komoly matematikai ismeretek szükségesek. Mindamellett a kriptográfia sok-sok eredménye a mindennapok részét képezi – használjuk, amikor megnyitunk egy honlapot (a böngésző, aminek segítségével ezt a cikket egy távoli szerveren írom, jelzi nekem, hogy a kapcsolat biztonságos), illetve amikor egy PIN-t ütünk be egy bankkártyás fizetésnél (egy érdekesség: a „PIN-kód" fogalom nem ugyanaz, mint a „PIN", hanem a titkosított változata a négy számjegyből álló Personal Identification Numbernek (PIN), amit mindannyian az eszünkben, vagy őszintén szólva, valamilyen biztonságosnak vélt helyen tartunk). Nagyon sok választható kriptográfiai módszer van egy-egy probléma megoldásához. Csak korlátozott számú szereplő fogja használni a megoldást, vagy az egész világ részt fog venni benne? Van a megoldás során adatmennyiségi korlát, vagy ezzel nem kell foglalkozni? Mennyire biztonságosnak kell lenni-e a megoldásnak, azaz más szóval, milyen sok idő kell a kód feltöréséhez számítástechnikai kapacitásban kifejezve? Hány évig kell a technológiának biztonságosnak maradnia?

11 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400886

Nemcsak a kriptográfiai módszer kiválasztása fontos, meghatározó paraméter az ún. kulcsméret (keysize) is. A kulcsméret meghatározza a digitális aláírás méretét, illetve ez mondja meg azt is, milyen nehéz azt feltörni – minél nagyobb a kulcs, annál nehezebb. Ha sokan használják a megoldást, széles körben elterjedt módszert kell alkalmaznunk, olyat, amit több operációs rendszer is támogat (mobiltelefonok, tabletek, laptopok és PC-k rendszerei), ráadásul több programozói nyelvben is alkalmazható azért, hogy a fejlesztők könnyen használhassák azt. Ugyanakkor nem minden kulcsméret használható minden alkalmazásban ugyanazzal a megoldással, tehát nagyon figyelni kell arra, milyen kulcsméretet választunk.

A K+F projekt egyik megfigyelése, hogy a QR-kód használata korlátozza a továbbítható adatmennyiséget. Ilyen esetben tehát a digitális aláírás mérete meghatározó tényező, persze úgy, hogy a biztonság szintjét nem veszélyeztethetjük.

A kriptográfia gyorsan és folyamatosan fejlődik. Ez persze nemcsak a módszerekre és a kulcsméretre vonatkozik, hanem a feltörési kísérletekre is. Az alkalmazott módszereket és variációs lehetőségeket tehát folyamatosan ellenőrizni kell a családi technológiák szempontjából is. A kriptográfiának az egyik legnagyobb kihívást a kvantum-számítástechnika várt elterjedése jelenti. A kvantum-számítástechnika lényege, hogy szakít a bitalapú számítási módszerekkel, a kvantummechanika tudományos eredményeit felhasználva, bizonyos problématípusokra várhatóan nagyságrendekkel gyorsabban fogja tudni megtalálni a megoldást a Neumann-architektúrájú számítógépeknél. Az egyik ilyen problématípus a számok prímtényezős felbontása, amelynek számításigényessége a jelenleg legelterjedtebb titkosítási algoritmusok magas biztonsági fokának alapja. A kvantum-számítástechnika még nem érte el azt a szintet, hogy a kriptográfiát veszélyeztesse[12], mégis figyelembe kell venni ezt veszélyt, ha egy módszert évek múlva is szeretnénk alkalmazni. Vannak szervezetek, mint például az ECRYPT[13], a NIST[14], a BSI[15] vagy az NSA, amelyek a módszer és a kulcsméret kiválasztását segítő anyagokat bocsájtanak ki, meghatározva azt az időtartamot, amíg egy kulcsméret használható.

Van egy általánosan elfogadott alapelv: mindig hivatalosan elfogadott szabványt kell alkalmazni. Ezeket a szabványokat kiváló szakemberek fejlesztették ki, a kriptográfia sok ezer szakértője ellenőrizte azokat, a világon sok milliárd eszkö-

12 https://www.etsi.org/technologies/quantum-safe-cryptography#:~:text=Quantum%2Dsafe%20cryptography%20refers%20to,quantum%20computer%20has%20been%20built

13 https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

14 https://doi.org/10.6028/NIST.SP.800-57pt1r5

15 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile

zön használják és folyamatosan ellenőrzik abból a szempontból, hogy a technológiai fejlődés nem fogja-e hamarosan annullálni ezeket a szabványokat.

A K+F projekt sok algoritmust és paramétert megvizsgált oly módon, hogy a hivatalosan elfogadott szabványok közül összehasonlította az ECDSA-, a Schnorr-, a Taproot- és a BLS-megoldásokat. A nyertes az ECDSA lett, mivel ez elég széles körben terjedt el, kis adatméret kell hozzá, megfelelő a biztonsága, ugyanakkor várhatóan még elég hosszú ideig biztonságos lesz.

2.5.2. Csalásmonitorozás

Ahhoz, hogy a csalások okozta veszteséget csökkentsük, azokat folyamatosan monitorozni kell, a felfedezett csalásokat pedig azonnal blokkolni szükséges. A hatóságok mindig figyelik azt, hogy vajon a bankok aktivitása megfelelő szintű-e a csalásmegelőzés területén azért, hogy az ügyfelek veszteségeit elkerüljék. A felelősséget a szabályozás a bankokra terelte azért, hogy motiválja őket a minél nagyobb aktivitásra e téren, megelőzve így a saját veszteségeiket is.

Sok intézmény azt a módszert használja, hogy minden tranzakciót ellenőriz úgy, hogy a csalás jeleit keresi benne. Ez a megoldás jelentősen növeli a komplexitást és a látenciát, ezért nagyon gyorsnak és robusztusnak kell lennie. Az az információmennyiség, ami a bankok rendelkezésére áll ügyfeleik szokásairól, valamint a rendelkezésre álló adatelemzési eszközök és módszerek együttesen nagyon hatékony eredményt tudnak produkálni. E módszerek használata ugyanakkor megköveteli a szakterület pontos ismeretét is. Az operátor nem veszhet el a rendelkezésre álló, óriási adatmennyiségben, a hasznos információt el kell tudni választani a „zajtól". A szakértőnek napi szinten kell ismernie a csalási trendeket, azok módszereit, illetve le kell fordítania az adatokból kinyerhető mutatókra. Mindezek közben a hibás jelzések számát, azaz a téves riasztásokét is csökkenteni kell.

Több intézmény is arra a következtetésre jutott, hogy a különféle forrásokból nyert adatokat kombinálni kell. A csalásmonitorozás fogalma a bankkártya-feldolgozásból ered, így az első módszereket a kártyatranzakciók elemzésére dolgozták ki. Az elektronikus csatornák térhódításával a bankoknak egyre több ügyfélkapcsolati rendszerük lett. Ugyanaz az ügyfél használja a mobilapplikációt, az internetbankot, fizethet plasztikkártyával, de virtuális kártyával is. Példaként említhető, hogy fontos információ lehet egy kártyahasználat esetében, hogy a kártya felhasználási helye és a felhasználó mobiltelefonja közel van-e egymáshoz. Ez csak egy kis adat a sok közül, azonban az eszközre, beállításra, fizetési helyre stb. adatok tucatjait azonosították minden fizetési helyzet esetében.

A csalások elleni harcban egy akadályt nagyon nehéz leküzdeni. Az adatvédelmi szabályozások előírják, hogy a bankok nem oszthatják meg egymással a csalásokban érintett ügyfelek adatait. Ez az előírás korlátozza a bankok lehetőségeit a

csalások elleni harcban. Vannak ugyanakkor kezdeményezések központi csalásmonitorozó megoldás létrehozására, amely lehetőséget adna a bankoknak arra, hogy a saját rendszerükön túl a központilag összegyűjtött adatokat is használják. A csalásmonitorozó rendszer fontos eleme az, hogy milyen válaszinformációkat kapunk a rendszertől. Egy egyszerű igen/nem válasz vagy egy kockázatbesorolási érték távolról sem elegendő. Meg kell érteni az eredmény mögötti tényezőket, valamint értékelni az eredményeket, továbbá döntéseket hozni ezek alapján, és ha szükséges, változtatásokat végrehajtani a rendszerben a különféle eredmények alapján. Mindezek szerint is a különféle MI-alapú megoldásokat óvatosan kell kezelni. Nem szabad elfogadni egy öntanuló fekete doboz döntését anélkül, hogy ismernénk a döntés mögötti tényezőket. Neurálishálózat-alapú rendszerek esetében például a „miért" kérdésre adott azon válasz, amely szerint „a kapott mintaparaméterek alapján képzett differenciálegyenletnek az adott döntés felel meg", helyesnek mondható, csak egyáltalán nem használható.

Amennyiben egy fizetési megoldást biztonsági szempontból nem megfelelően terveztek meg, a felhasználók veszteségeket fognak elszenvedni, aminek nemcsak az lesz az eredménye, hogy ők nem használják a megoldást tovább, hanem a hatóságok is lépni fognak. Több módszer is van a csalások észlelésére és megelőzésére, kezdve az adatátvitel biztonságának a növelésétől, a tranzakciófigyeléstől és -blokkolástól az előző kettő kombinálásáig.

2.6. Elterjedtség

Egy fizetési megoldás bevezetése során két kezelendő csoport van: a fizető fél és a kedvezményezettek csoportja. Kezdetben ez a két csoport egymásra vár. A fizető felek felteszik az egyszerű kérdést: „Hol tudok fizetni ezzel a megoldással?", a potenciális kedvezményezettek pedig azt kérdezik: „Ki fog fizetni ezzel a megoldással?" Egyik csoport sem fogja használni a megoldást, ha a kérdéseikre nem kapnak meggyőző választ. Éppen ezért az indulás mindig nagyon nehéz. Hogyan lehet mégis ösztönözni ezt az indulást?

Egy új fizetéskezdeményezéshez használandó fizikai eszköz elkészítése kockázatos dolog, ugyanis van egy határa annak, hogy hány ilyen eszközpéldányt lehet legyártani egyszerre. Lehet olyan eset is, hogy egyszerűen visszaküldik az eszközt, ami csökkentheti elfogadottságát. Az eszköznek természetesen kompatibilisnek kell lennie a kedvezményezettek már meglevő eszközeivel, azaz a gyártás előtt be kell szerezni minden kezdeményezetti eszközt, és ezekkel együtt tesztelni az újat. Az eszközök költsége természetesen terheli a megoldás nyereségességét is. Ez a megoldás tehát akkor működik, ha a megoldás elfogadottsága elég nagy, mivel a

fizető felek nem váltanak egyszerűen. Mindez a bevezetési költségek növekedését eredményezheti.

Egy másik lehetséges megoldás egy applikáció fejlesztése, amelynek a terjesztésébe a mobilgyártók is bevonhatók. Ez egy olcsó megoldásnak tűnik, bár az applikáció fejlesztésének is vannak költségei. Nem szabad ugyanakkor az applikációk közötti verseny hatásait sem lebecsülni. Ma mintegy 5 millió applikáció[16] vár letöltésre a piacon, ráadásul ezeket folyamatosan minden lehető csatornán reklámozzák. Ahhoz, hogy a potenciális ügyfél a mi applikációnkat töltse le, jelentős reklámköltségek szükségesek, vagy pedig más, komolyabb érvet kell bevetni ahhoz, hogy az ügyfél a mi applikációnkat részesítse előnyben.

A K+F projekt keretében lefolytatott kutatások nagyon fontos megállapítása az, hogy egy olyan applikációt kell használni, ami már biztosan ott van az ügyfél mobiltelefonján! Ez a banki mobilapplikáció, hiszen azt is lehet egy kis kiegészítéssel virtuális fizetési eszközként használni. Az ügyfelek elvárásainak megfelelően az utóbbi évtizedben szinte az összes bank kifejlesztett saját applikációt. Ezek az applikációk fizetéskezdeményezési művelet végrehajtására is képesek. Annak a változtatásnak a volumene, ami egy banki applikációhoz szükséges, elhanyagolható egy új eszköz vagy egy új applikáció kifejlesztéséhez képest.

Az elfogadottság növelésének igen egyszerű módja az, ha azt kötelezővé lehet tenni. Ez egy kicsit kemény megoldásnak tűnk, de hatásos. Nem kell a bevezetéshez gazdaságossági számításokat végezni, nem kell a várható profitot bemutatni a banki döntéshozóknak.

Több módszer van arra is, hogy a felhasználók motiváltak legyenek abban, hogy használják a fizetési megoldást. Amennyiben a fizető felek elkezdik alkalmazni a megoldást, a kedvezményezettek is be fogják azt vezetni. Ahogy korábban bemutattuk, az adatátvitelnek nincs univerzális technológiája. Amennyiben a fizetési megoldás több technológiát is használ, a fizető felek biztosan meg fogják találni a nekik legmegfelelőbbet. Arra is figyelni kell ugyanakkor, hogy a megoldás bevezetésekor az adatátviteli technológia már benne legyen az eszközben, elkerülendő az eszközcsere költségeit. Bizonyos esetekben az sem feltétlenül szükséges, hogy a fizető fél tudja egyáltalán, hogy új fizetési módot használ. Sok online kereskedő az ún. „VPOS" (virtuális POS) megoldást használja, amelyet részére egy pénzforgalmi szolgáltató biztosít. A VPOS nem képezi a kedvezményezett technológiájának a részét, éppen ezért az abban bevezetett változás nem indukál semmilyen változtatási kötelezettséget nála.

16 https://www.bankmycell.com/blog/number-of-mobile-apps-worldwide

3. CAPSYS SMART PAYMENT SOLUTION

A Capsys által végrehajtott K+F projekt eredménye egy azonnali fizetési ökoszisztéma tervezete lett. Egy ilyen ökoszisztémában a következő résztvevők vannak:

A központi szereplő, amely szabályozza a rendszert és támogatja az összes folyamatot. Ez a szerep több résztvevő között is szétoszthatóː a szabályozó, az elszámolóház, pénzforgalmi szolgáltató és autorizáló egység, de olyan döntés is hozható, hogy ezeket a szerepeket egy azonos szervezet tölti be.

A rendszert használó kedvezményezetteket regisztrálni kell éppen a csalások elkerülése miatt. A regisztrációt a központi szereplő is végezheti, de a feladatot a bankokhoz is lehet delegálni, az ő KYC-folyamataik megfelelőek ennek a feladatnak a végrehajtásához. A domainnév kezelése mindenképpen központi feladat. A fizető applikációkat a központi szereplő regisztrálja és kapcsolja össze a központi domainnel. A banki mobilapplikációk is regisztrálva vannak, de gyakorlatilag bármely olyan applikáció, amely azonnali fizetési tranzakció kezdeményezésére alkalmas – mint például egy open bank interfészt használó alkalmazás – regisztrálható.

A kedvezményezetteknek minden fizetés kérést a központi egységnél kell regisztrálniuk, amelyik erre egy, a fizetés adatait igazoló digitális aláírást bocsájt ki.

A megoldás a fizetési helyzetek nagyon széles körét fedi le. A fizetési tranzakció történhet fizikai boltban, online módon, számlák kifizetéseként, POS/VPOS terminálóknál, bolti kasszák igénybevételével vagy akár nyomtatott számlák kifizetéseként stb.

A kedvezményezettek a fizetési kérést megjeleníthetik egy képernyőn QR-kódként, de küldhetnek akár NFC-, akár deep link jelet is. Az adatátvételi technológiától függetlenül az adattartalom minden esetben ugyanaz, biztosítva így a teljes interoperabilitást. Az URL-alapú formátumot a központi szereplő szabályozza.

A továbbított adatok olvasására a fizető fél a mobiltelefonját használja. A mobiltelefonok a Universal Linking technológiát alkalmazzák az applikáció felélesztésére. Az applikáció ellenőrzi az adatokat, és megkéri a fizető fél hozzájárulását, természetesen az erős ügyfél-hitelesítési és kivételkezelési szabályokat alkalmazva, majd az adatok felhasználásával elindítja az azonnali fizetési tranzakciót. A bankok és a központi infrastruktúra visszaigazolást küld a központi szereplőnek a művelet végrehajtásáról. A visszaigazolás formátumát a központi szereplő szabályozza.

Amikor a K+F projekt lezárult, következett a legnehezebb feladat: nevet kellett adni a megoldásnak. A munka során a QR-kód volt az első szóba jöhető technológia. A QR-kód egy specifikus tranzakciós adatokat tartalmazó dinamikus megol-

dás volt, kényelmes is, mert nem kellett használatához külön ügyfél-interakció és megfelelően biztonságos is volt. A „Dinamikus, kényelmes, biztonságos QR-kód" elnevezés nem tűnt ugyanakkor túl vonzónak. A csapat tehát azt mondta: az új QR-kód megoldás okosabb (smart), mint a korábbiak, legyen a név tehát az alkotóra is utalva: Capsys Smart Payment Solution.

4. QVIK: AZONNALI FIZETÉS 2.0 – MAGYARORSZÁG AZ AZONNALI FIZETÉSI RENDSZEREK ÉLVONALÁBAN

Magyarország egy igazán különleges ország az azonnali fizetések világát illetően. A Magyar Nemzeti Bank 2017-ben[17] hozta meg döntését az azonnali fizetési rendszer bevezetéséről. Ennek a döntésnek volt egy különleges eleme: kötelezővé tette a rendszerhez való csatlakozást minden pénzforgalmi számlát vezető szolgáltatónak (hétköznapi meghatározással banknak). A bevezetett rendszeren a szolgáltatás 2020. március 2-án indult, és azóta is zavartalanul folyik. A rendszeren végrehajtott tranzakciók mennyisége folyamatosan növekszik, elérve a havi 14 milliós számot. Ezek a tények azt mutatják, hogy az azonnali fizetési rendszer bevezetése Magyarországon sikeres volt, és az az elképzelés, hogy a szolgáltatás bevezetése a bankoknak kötelező volt, olyan népszerű lett, hogy az EU meglépte ugyanezt az intézkedést a 2024-ben[18] elfogadott Azonnali Fizetési Szabályozás (Instant Payment Regulation) kibocsájtásával.

Az MNB 2022-ben a következő szabályozási csomag kibocsájtásakor ugyanezt az elvet követte. A projekt kódneve AFR 2.0, jelezve azt, hogy a kezdeményezett változás a már létező rendszer fejlesztését jelenti. A változtatások célja az, hogy az azonnali fizetési központi infrastruktúra egy fizetési megoldássá változzon, lehetővé téve azt, hogy olyan fizetési helyzetekben is lehessen azonnali fizetési tranzakciót kezdeményezni, amelyekben az AFR 1.0 nem teszi ezt lehetővé. A szélesebb körben történő használat támogatása érdekében az MNB a fizetési módhoz új brandet hozott létre, ez lett a qvik. A qvik márkanevű rendszer elemei a következők:

- Minden banknak kötelező bevezetnie a „fizetési kérelem" szolgáltatást legalább mint fogadó félnek.
- Bevezeti az „Egységes adatbeviteli megoldást" (EAM), ami egy biztonságos URL-alapú adatátviteli formátum NFC, QR-kód és deep link használatával.

17 https://www.mnb.hu/letoltes/decree-no-35-2017-xii-14.pdf

18 https://www.mnb.hu/letoltes/decree-no-35-2017-xii-14.pdf

- Az EAM-olvasás bevezetése kötelező minden olyan bank részére, amely mobilapplikációt üzemeltet ügyfeleinek.
- A fizető fél bankjának kötelező visszaigazolást küldenie az Azonnali Fizetés Rendszer Központi Infrastruktúra részére az EAM használatával kezdeményezett átutalások eredményéről.
- A brandhasználat bevezetése – kötelező a központilag meghatározott qvik név és piktogram használata.
- A fizető fél bankja nem alkalmazhat tranzakcióalapú díjazást az EAM és a fizetési kérelem alapján benyújtott utalási megbízás esetén.
- Központi panasz- és visszatérítés-kezelés.

Az EAM, valamint a feldolgozási folyamat technikai szabályozása a központi infrastruktúrát működtető vállalat, a GIRO Zrt. feladata lett.

4.1. Az Egységes Adatbeviteli Megoldás bevezetése

A qvik bevezetése előtt az azonnali fizetési műveleteket többnyire kézi adatbevitel útján kezdeményezték. Volt ugyan néhány próbálkozás adatátvitelen alapuló megoldása bevezetésére, de ezek lokális próbálkozások maradtak. Az ilyen megoldások korlátozott voltát felismerve a szabályzó hatóság egy egységes adatbeviteli rendszer bevezetése mellett döntött. A rendszer egységes részben abból a szempontból, hogy minden banknak ugyanazt a formátumot kell használnia, és egységes abból a szempontból is, hogy ugyanazt az URL-alapú megoldást kell használni a QR-kóddal, NFC-vel és deep link technológiával történő fizetés esetében is.

Az EAM minden, a fizetéshez szükséges adatot tartalmaz (név, kereskedelmi név, a kedvezményezett IBAN-száma, tranzakciós azonosító, összeg stb.), valamint egy sor „H-Data" néven ismert adatot (terminálazonosító, számlaszám stb.), és digitális aláírás formájában tartalmaz egy biztonsági kódot is. A bankok nemcsak hogy olvassák az EAM adatokat, hanem ellenőrizniük kell, hogy az adatokat validáló digitális aláírás nem lett-e meghamisítva.

4.2. Ki kicsoda az új rendszerben?

A qvik összeköti a jelenlegi fizetési rendszerek szereplőit az azonnali fizetési rendszer által létrehozandó új lehetőségekkel.

Az MNB az általa meghatározott stratégiai célokat az egész projektet átfogó szabályozási rendszerré alakítja át.

A GIRO működteti a központi infrastruktúrát, amelyik végrehajtja a bankközi átutalásokat, továbbítja a fizetésekhez tartozó értesítéseket és a privát kulcs rendszerének működtetésével központi szereplője az EAM-ban a digitális aláírások rendszerének is. A GIRO az ügyfélpanaszok kezelésének a rendszerében is központi szereplő azzal, hogy biztosítja a panaszok nyilvántartási rendszerét.

A fizető fél bankjának feladata az EAM-feldolgozás működtetése, valamint az azonnali átutalási tranzakciók indítása a mobilapplikációk útján.

Az aggregátor az EAM-alapú fizetések műszaki támogatásában működik közre, szoros együttműködésben a GIRO Zrt.-vel.

A sub-aggregátorok, amelyek közvetlen jogi és műszaki kapcsolatban vannak az aggregátorral, fizetéstámogatási rendszert működtetnek a kedvezményezettek részére. A sub-aggregátorok hasonló feladatokat végeznek ebben a rendszerben, mint az elfogadók a bankkártyás fizetési rendszerekben. Amennyiben valaki már működtet egy elfogadói szolgáltatást, az EAM-alapú szolgáltatást bekapcsolhatja a már létező szolgáltatás mellé. A sub-aggregátornak működéséhez pénzforgalmi szolgáltatói jogosítvánnyal kell rendelkeznie. A műszaki szolgáltatók a kedvezményezettekkel szállítói kapcsolatban levő vállalkozások, ők szállítják a fizetések lebonyolításához szükséges eszközöket és szoftvereket. Ezek az eszközök lehetnek POS-terminálok, kasszagépek, VPOS-megoldások, webshoprendszerek, számlázórendszerek stb.

4.3. Mi lehet később?

A qvik első nagy lépése az infrastruktúra felállítása minden szereplőnél, beleértve a bankokat, de főként a GIRO-t 2024. szeptember 1-ig. Az első időben valószínűleg csak korlátozott számú kedvezményezett csatlakozik a rendszerhez. Ahogy az új qvik fizetési megoldás működése stabilizálódik, várhatóan mind több résztvevője lesz a rendszernek. Most nézzünk néhány gyakorlati példát, mi történhet az egyes fizetési helyzetek esetében:

- Az egyik legkönnyebben megvalósítható lehetőség a **VPOS-szolgáltatók** előtt van, ők nagyon egyszerűen bevezethetik a qvik EAM-fizetést. A bevezetés itt követeli meg a legkevesebb műszaki változtatást úgy, hogy a kedvezményezettnek gyakorlatilag semmilyen változtatást nem kell végrehajtania.
- Az **online számlaszolgáltatók** is egyszerűen tudják alkalmazni a qvik EAM fizetési lehetőséget ügyfeleik részére akár nyomtatott, akár pedig digitális formátumban. A szükséges műszaki változtatás igények minimálisak, ugyanakkor e szolgáltatóknak ügyelniük kell arra, hogy ügyfeleik valóban legális vállalkozások legyenek.

- A **közüzemi szolgáltatók** szintén könnyen alkalmazhatják a qvik EAM-fizetést ügyfeleik részére akár a honlapjukon, akár pedig az applikációjukon keresztül.
- A **telekommunikációs cégek** egy sor qvik EAM-megoldást ajánlhatnak ügyfeleiknek akár nyomtatott számláikon, akár applikációjukon, de bármilyen más módon is.
- A **bolti kereskedők** a qvik EAM-alapú fizetési rendszert könnyen ajánlhatják akár QR-kóddal, akár a kasszába integrált POS-termináljaikon, de POS-szolgáltatójuktól is igénybe vehetik a qvik EAM-szolgáltatást. Azt is megtehetik, hogy a lojalitás rendszereikhez hozzáférést adó applikációjukba deep link megoldást építenek be.

Magyarország egy olyan útra lépett, amely elvezethet oda, hogy a központi azonnali fizetési infrastruktúra egy, a mindennapokban jelen levő fizetési megoldást biztosítson. Az egységes adatbeviteli megoldás és a mindent átfogó szabályozás együttesen minden ehhez szükséges lehetőséget biztosít. Ezért érdemes a qvik-et figyelemmel kísérni a következő években.