Az RTS SCA követelményeinek

mélyére merültünk jogi szakértőkkel

Október 2-án részt vettünk a PSD2 szabályozás részleteit meghatározó ún. RTS SCA követelményeit részletesen elemző workshopon (Dive deep into PSD2). A workshopot a CREOBIS szervezte, a workshop szakmai munkáját a Bird&Bird vezető fizetési jogászai, Scott McInnes és Adrián Calvo irányították. A jelen dokumentumban összefoglaljuk a workshop legfontosabb megállapításait.

Online BUSINESS TECHNOLOGIES

DIGITIE

Bevezetés

Október 2-án részt vettünk a PSD2 szabályozás részleteit meghatározó ún. RTS SCA követelményeit részletesen elemző workshopon (Dive deep into PSD2). A PSD2 (Payment Service Directive Revised) az Európai Parlament és Tanács 2366/2015-ös számú direktívája a pénzforgalmi szolgáltatások szabályozásáról. Az RTS SCA a Bizottság (EU) 2018/389 felhatalmazáson alapuló rendelete, amely a PSD2 direktíva erős ügyfél-hitelesítésre, valamint a közös és biztonságos nyílt kommunikációs standardokra vonatkozó részletszabályait határozza meg (a rendeletre a továbbiakban az egyszerűség kedvéért RTS-ként hivatkozunk).

A workshopot a CREOBIS szervezte, a workshop szakmai munkáját a Bird&Bird vezető fizetési jogászai, Scott McInnes és Adrián Calvo irányították. A workshopon a követelmények elemzéséhez felhasználtuk magát az RTS SCA-t, az Európai Bankfelügyelet által 2018. június 13-án közzétett véleményt az RTS SCA-nak történő megfelelés megvalósításáról (Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC), valamint a brit pénzügyi felügyelet (FCA) által 2018 szeptemberében kibocsátott konzultációs dokumentumot (Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive (PSD2)).

A jelen dokumentumban összefoglaljuk a workshop legfontosabb megállapításait.

Erős ügyfél-hitelesítés - SCA

Első témaként az SCA-val foglalkozunk, vagyis az RTS által leírt erős ügyfél-hitelesítéssel. A beszélgetés alapjaként a PSD2 direktíva 97-es cikkéhez nyúltunk vissza, ami meghatározza, hogy milyen esetekben kell az SCA-t alkalmazni. Ezen cikk szerint SCA-t kell alkalmazni, ha a fizető fél:

- online fér hozzá a fizetési számlájához;
- elektronikus fizetési műveletet kezdeményez;
- a műveleteket távoli csatornán keresztül hajtja végre, ami fizetéssel kapcsolatos csalásokra és más visszaélésekre adhat módot.

A fentiekből fontos kiemelni, hogy csak olyan esetben kell alkalmazni SCA-t, ha a fizető fél kezdeményezi a műveletet, illetve hogy akkor is elvárás ha általánosságban csalásra, visszaélésre okot adó tevékenységre irányul a művelet, így például ha egy pénzforgalmi szolgáltató (PSP) közvetítésével beadott csoportos beszedési megbízásról, vagy egy fizetési kérelem elfogadásáról van szó. SCA-t kell alkalmazni akkor is, ha a kártyás fizetést a fizető fél indítja el a kedvezményezetten keresztül. Nem kell azonban SCA-t alkalmazni, ha a kártya alapú fizetést ténylegesen a kedvezményezett indítja, pl. egy Netflix előfizetés havi engedélyezett 9,99 €-s kártya-terhelése esetén. További kivételt képeznek a PSD2 preambulumának 95-ös bekezdése szerinti ún. MO/TO (Mail Order/Telephone Order) műveletek, azaz papíralapú fizetési műveletek, vagy a postai és a telefonon történő rendelések, amelyek esetében nem szükséges az SCA alkalmazása.

A PSD2 direktíva 4. cikkének 30. meghatározása szerint az „erős ügyfél-hitelesítés" olyan hitelesítés, amely legalább két olyan elem felhasználásával történik, amely elemek az ismeret (csak a szolgáltatást igénybe vevő által ismert információ), a birtoklás (csak a szolgáltatást igénybe vevő által birtokolt dolog) és a biológiai tulajdonság (a szolgáltatást igénybe vevő jellemzője) kategóriákba sorolhatók. Az EBA a véleményében kifejtette (33. pont), hogy az RTS-ben meghatározott SCA definíció azon része, amely szerint a két faktornak a három kategória egyikéből kell kikerülnie, az EBA értelmezése szerint azt jelenti, hogy a két faktor két külön kategóriába kell, hogy tartozzon. A workshopon megállapítottuk, hogy az RTS szövegezéséből ez az értelmezés nem következik, és mivel az EBA véleménye nem rendelkezik joghatással, ezért akár egy olyan SCA is jogszerű lehet, ami két azonos kategóriába tartozó elemen alapszik, ha a hitelesítés az RTS minden további feltételének megfelel. Az ilyen jellegű hitelesítési kombináció alkalmazását azonban érdemes átgondolni, mert például az FCA is az EBA véleményét osztja, tehát az ilyen hitelesítési eljárások használatát a helyi felügyelet egy audit során kifogásolhatja!

Több fórumon felmerült már, hogy megfelelő lesz-e az erős ügyfél-hitelesítés szempontjából az SMS-ben küldött dinamikus jelszó. Ebben a kérdésben mind az EBA (http://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039), mind az FCA egyértelműen nyilatkozott: a 20.19-es pontban leírtak szerint egy eszköz akkor használható, mint a birtoklás kategóriájába tartozó hitelesítési faktor, ha az eszközt például token generálásra, vagy egyszeri jelszó fogadására használják. Ilyen egyszeri jelszó fogadásának minősül az SMS-ben fogadott dinamikus jelszó.

Az SCA alkalmazása alóli kivételek

Fontos kitétele az RTS-nek és az irányelvnek is (98-as cikk), hogy az SCA-t bizonyos esetekben nem kötelező alkalmazni. A kivétel alkalmazásáról mindig az a szolgáltató dönt, aki az adott folyamatban az SCA elvégzésére vagy elhagyására jogosult, ami eltérő lehet kártyás vagy TPP-n keresztüli fizetések esetén. A kivétel alkalmazása esetén a teljes felelősség a kivétel alkalmazásáról döntő szolgáltatót terheli, azaz mint „leggyengébb láncszem" viseli pl. az esetleges visszatérítési kötelezettséget.

10-es cikk - Fizetési számlára vonatkozó információk

Ezen kivétel kapcsán megállapítottuk, hogy a fizetési számla definíciója nem minden ország esetében egységes, ezért elképzelhető, hogy van olyan ország, ahol egy megtakarítási számla is fizetési számlának minősül. Ezt erősítette meg Az Európai Unió Bírósága október 4-i döntése, mely úgy fogalmazta meg, hogy az a számla fizetési számla, amely közvetlenül használható fizetés indítására vagy fogadására harmadik féle irányába/ból.

Az RTS 10. cikkének 2. bekezdése szerint a pénzforgalmi szolgáltatók számára nem biztosítható kivétel az erős ügyfélhitelesítés alkalmazása alól, ha több mint 90 nap eltelt azóta, hogy a pénzforgalmi szolgáltatást igénybe vevő utoljára online hozzáfért a számlájához kapcsolódó

információkhoz. Az EBA véleménye alapján a kivétel 90 napos számlálója külön vezetendő szolgáltatónként, azaz minden számlainformációs szolgáltató (AISP) és a bank online csatornái külön számlálóval kell, hogy rendelkezzenek. A számlainformációs számlálót más okból végrehajtott (pl. fizetés-kezdeményezés) SCA nem indíthatja újra.

A workshopon megállapítottuk, hogy amikor az ügyfél egy TPP-n keresztül első alkalommal fér hozzá a számlájához, akkor az ügyfél a hozzáférésre vonatkozó hozzájárulását a TPP-nek és nem a számlavezető bankjának adja meg. A számlavezető banknak ebben az esetben nincs lehetősége a hozzájárulást felülbírálni (pl. a hozzáférést egyoldalúan elutasítani), a számlavezető banknak a hozzájárulás erős ügyfél hitelesítéssel történő megerősítését kell kérnie az ügyfelétől, amely végső megerősítést vagy megadja vagy elutasítja az ügyfél. A szabályozás értelmezése alapján kijelenthető, hogy a számlavezető banknál végrehajtott erős ügyfél hitelesítés az ügyfél részéről egyértelmű beleegyezésnek (explicit consent) minősül. Azt is kijelenthetjük továbbá, hogy ha az ügyfél a számlavezető banknál több számlát vezet és az ügyfél a TPP hozzáférésének engedélyezése során nem adta meg, hogy a hozzájárulása pontosan melyik számlájára vonatkozik, akkor nem számít az RTS szerinti ún. folyamatba épített akadálynak (RTS 32.(3) szerinti akadály), ha a számlavezető bank a hitelesítési folyamatban rákérdez arra, hogy melyik számlára vonatkozik az ügyfél hozzájárulása. A számla hozzáférés megadása mellett pontosan ezt az elvet lehet követni az átutalások esetében is. (ld. FCA 7.136).

A szabályozás rögzíti, hogy a fizetési számlák esetében a PSD2 API-n keresztül az ügyfelek számára ugyanazt az adatkört kell elérhetővé tenni, amely adatkört az ügyfelek a számlavezető bank által biztosított elektronikus csatornákon elérnek, de ez a kör bankonként akár nagyon eltérő is lehet. Amennyiben egy bank úgy dönt, hogy a PSD2 elvárásainak minimális megfelelést biztosító API-kat alakít ki, kiteszi magát annak a veszélynek, hogy azok a TPP-k, akik ennél szélesebb adatkört szeretnének elérni, azok a jelenleg alkalmazott screen scraping vagy reverse engineeringgel fognak ezekhez az adatokhoz hozzáférni, mivel a PSD2 keretein túlmutató adatkörök elérése esetében nem kell az RTS elvárásainak megfelelni!

A számlainformációs szolgáltatáshoz kapcsolódóan az SCA alkalmazásától csak akkor lehet eltekinteni (RTS 10. cikk), ha az ügyfél a számlája egyenlegét vagy a 90 napnál nem régebbi tranzakció-történetét, vagy esetlegesen mindkettőt szeretné lekérdezni. Minden ennél bővebb adatkörre vonatkozó lekérdezés esetében SCA-t kell alkalmazni. Így például internetbanki belépés esetén is csak akkor lehet eltekinteni az SCA-tól, ha az ügyfél az előzőekben ismertetett adatoknál bővebb adatkörhöz már csak SCA alkalmazását követően férhet hozzá.

13-as cikk - Megbízható kedvezményezettek

Az RTS 13. cikkének 2. bekezdése alapján a pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést, ha a fizető fél fizetési műveletet kezdeményez és a kedvezményezett szerepel a fizető által előzőleg összeállított, megbízható kedvezményezettek listáján.

A workshopon megállapítottuk, hogy megbízható kedvezményezettet kizárólag a számlavezető bankon keresztül lehet megadni, de a megbízható kedvezményezett esetében az SCA nem csak az online fizetések esetében hagyható el, hanem akkor is, ha a kedvezményezett személyesen fizet. Így például ha valaki megbízható kedvezményezettnek felveszi a Tesco-t, akkor akár a későbbiekben a bolti vásárlás során is SCA nélkül fizethet. A Tesco az SCA elhagyását további feltételekhez is kötheti, így például ha a Tesco kártyaelfogadóként dönt az említett SCA alóli kivétel alkalmazásáról, akkor az SCA elhagyását pl. a bankkártya és a törzsvásárlói kártya együttes jelenlétéhez kötheti. A számlavezető bank ilyen további feltételeket csak akkor írhat elő, ha ezen további feltételek teljesítését az összes fizetési csatornán egyformán előírja.

A workshopon felmerült, hogy a megbízható kedvezményezett megadása mikor tekinthető egyértelműnek, azaz a fenti példánál maradva például megadható-e egyszerűen névvel a Tesco, vagy egyértelmű megadásnak csak a név és a számlaszám, vagy egyéb jogszabályban meghatározott azonosító (pl. másodlagos azonosító) megadása minősül. A workshopon ezzel kapcsolatban nem alakult ki egységes álláspont, de a legvalószínűbb, hogy a megbízható kedvezményezetthez rögzítendő adatok körét a számlavezető bank határozhatja meg.

17-es cikk - Biztonságos vállalati fizetési folyamatok és protokollok

Az RTS 17. cikke szerint a pénzforgalmi szolgáltatók számára lehetővé kell tenni, hogy ne alkalmazzanak erős ügyfél-hitelesítést olyan jogi személyek kapcsán, amelyek erre a célra kijelölt, kizárólag nem fogyasztónak minősülő fizető felek rendelkezésére bocsátott fizetési folyamatok vagy protokollok használatával kezdeményeznek elektronikus fizetési műveleteket, amennyiben az illetékes hatóságok meggyőződtek arról, hogy a szóban forgó folyamatok vagy protokollok az (EU) 2015/2366 irányelvben előírtakkal legalább egyenértékű szintű biztonságot garantálnak.

A legtöbb tagállam még nem határozta meg, hogy ezen kivétel alkalmazása a helyi hatósági engedélyéhez kötött-e vagy sem, és ha engedélyköteles, akkor az erre vonatkozó engedély hogyan szerezhető meg. Az FCA álláspontja az, hogy a kivétel alkalmazásához nem szükséges az FCA engedélye, de ha egy szolgáltató alkalmazza ezt a kivételt, akkor ezt jelentenie kell az FCA-nak. Az FCA értelmezése szerint a kivétel csak akkor alkalmazható, ha a vállalati rendszer direktben a banki rendszerrel kommunikál, és nem alkalmazható a kivétel a vállalati online banking megoldások és a vállalati dolgozók számára kibocsátott fizikai kártyák esetében. (FCA 20.55-60)

18-as cikk - Műveletikockázat-elemzés

A PSD2 hatályba lépésével módosult a csalás eddigi fogalma, és a továbbiakban a csalás definíciójába a nem engedélyezett műveletek és a csalárd, azaz pl. a fogyasztó megtévesztésével végrehajtott műveleteket is beletartoznak. A változás miatt célszerű a csalásokra vonatkozó felügyeleti jelentéseket felülvizsgálni.

Amennyiben egy bank a kivétel alkalmazása mellett dönt, érdemes figyelemmel kísérni a jelenleg még vita tárgyát képező ún. ePrivacy szabályozást (EUR-Lex - 52017PC0010), amelynek tárgya az elektronikus hírközlés során a magánélet tiszteletben tartása és a személyes adatok védelme. Ez a jogszabály komoly hatást gyakorolhat arra, hogy a kockázat-elemzéshez milyen adatokat lehet felhasználni, összegyűjteni.

Számlahozzáférés az ügyfél jelenléte nélkül

Az RTS SCA 36 (5) cikke előírja, hogy a számlainformációs szolgáltatók részére 24 óránként négyszer hozzáférést kell biztosítani azokhoz a számlákhoz, amely számlákra vonatkozóan a számlainformációs szolgáltatók érvényes ügyfél-hozzájárulással rendelkeznek, anélkül, hogy ezt a hozzáférést az ügyfél aktívan kérnéó. Ettől a hozzáférési gyakoriságtól egyedi megállapodással felfelé el lehet térni. Mivel az előírás nem korlátozza a hozzáférés keretében elérhető adatok körét, így minden olyan adatot elérhetővé kell tenni, amely adatokat az ügyfél a banktól közvetlenül is megkaphatna. Ha egy AISP külön megállapodás hiányában 24 óránként négynél többször kezdeményez hozzáférést a számlához, akkor megszegi az RTS előírásait, mivel az RTS megfogalmazása alapján a naponta engedélyezett hozzáférések számának betartása az AISP felelőssége.

Összegzés

A workshop egyértelműen rámutatott arra, hogy bár a PSD2 direktíva végleges szövegét már 2015-ben közzétették, és az RTS hivatalos, végleges szövege már 2018. március 13-ától ismert, de mind a mai napig felmerülnek olyan gyakorlati kérdések, amelyek megválaszolása komoly jogi elemzést és értelmezést igényel.

Cégünk számára azért fontosak a 2018. október 2-i workshophoz hasonló szakmai rendezvények, mert banki rendszerfejlesztőként a kezünk alatt a PSD2 és az RTS követelményeinek működő szoftverfunkciókká kell átalakulniuk, amely funkciók egyértelmű állásfoglalást és értelmezést követelnek meg.

A workshopon összegyűjtött ismereteket a DigiTie PSD2 szoftverünk fejlesztéséhez (ld. https://www.online.hu/megoldasok/digitie/digitie-psd2) használjuk fel, amely szoftver segítséget nyújt banki partnereinknek a PSD2 informatikai követelményeinek történő megfelelésben. Reméljük ez a tanulmány segíteni fog ebben az Olvasónak is.

Amennyiben a tanulmányban leírtakkal, vagy DigiTie PSD2 megoldásunkkal kapcsolatban további kérdés merülne fel, kérjük vegyék fel velünk a kapcsolatot!

Cégünkről

Az ONLINE ÜZLETI INFORMATIKA ZRT. az egyik legnagyobb hazai szoftverház, amely 1989 óta nyújt IT megoldásokat kereskedelmi bankok és pénzintézetek részére.

Megoldások széles és rugalmas skáláját kínáljuk, mely támogatja a bankok digitalizáció útjára történő áttérését, beleértve a csatlakozási lehetőséget FinTech ökoszisztémákhoz (pl. PSD2, nyílt API-k, azonnali fizetés), elektronikus csatornát érintő megoldásokat és a legkorszerűbb alapvető számlavezetési modulokat, melyek front- és back-office működést támogatja (beleértve a számlavezetést, hiteleket, letétet, GL-t stb.)

Moduljaink szabadon variálhatóak, akár önálló speciális megoldásként is bevezethetőek (például PSD2), vagy modulok olyan sorozataként, amelyek segítségével a teljes értéklánc lefedhető (például hitelezési folyamatok).

Tevékenységünk számokban:

- Közel 2500 emberévnyi banki, pénzügyi szoftverfejlesztési tapasztalattal rendelkezünk
- Megoldásainkat több, mint 8000 ügyintéző használja
- Megoldásainkat partnereink több, mint 1000 bankfiókban használják
- Megoldásainkkal partnereink több, mint 3 millió ügyfelet szolgálnak ki

ÉRTÉKEINK

EGYEDÜLÁLLÓ KOMPETENCIA A hitelintézeti, pénzügyi területen felhalmozott tapasztalatunk és szaktudásunk az IT szállítók között egyedülálló.

TESTRESZABOTT RENDSZEREK Egyedülálló fejlesztési és verzió-követési technológiánk segítségével moduljaink rövid idő alatt testre-szabhatók és bevezethetők, ugyanakkor nagy gyakorlatunk van egyedi funkciók hatékony megvalósításában is

MAGAS MINŐSÉG Minden tevékenységre kiterjedő minőségirányítási rendszerünknek, szabályozott fejlesztési folyamatainknak köszönhetően rendszereink magas minőségűek és üzembiztosak

GYORS MEGTÉRÜLÉS A megrendelői erőforrásokat kímélő, gyors bevezetés, hatékonyabb ügyvitel és a piaci trendekre való rugalmas reagálás révén ügyfeleink előnyre tehetnek szert a gyorsan változó pénzügyi piacon

További információért látogasson el weboldalunkra: www.online.hu

Online Üzleti Informatika Zrt.

H-1032 Budapest, Vályog street 3. | +36-1-437-0700 | https://www.online.hu/contact