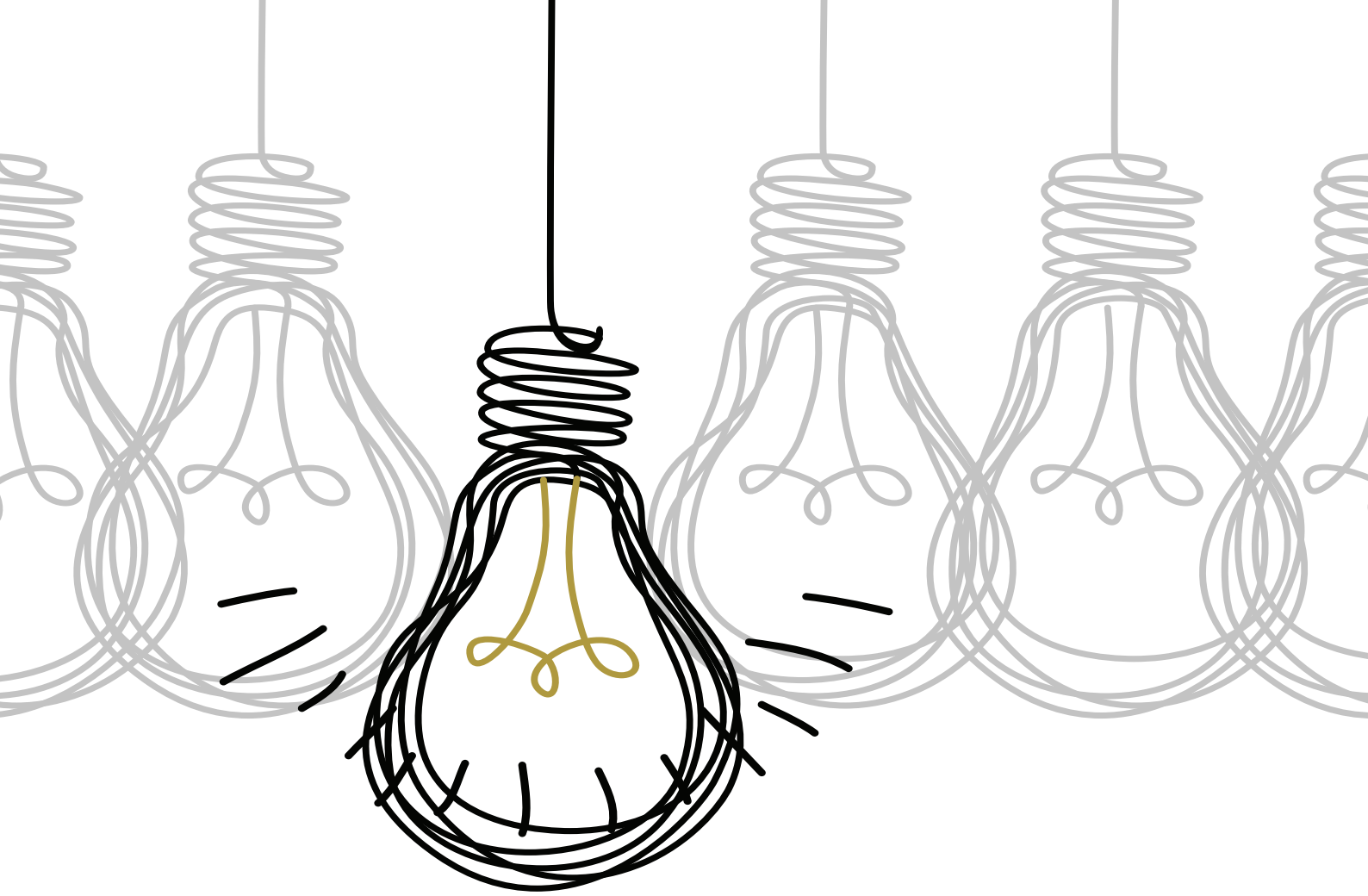

# PSD2 – KIHIRDETTÉK AZ ERŐS ÜGYFÉL-HITELESÍTÉSRŐL SZÓLÓ TECHNIKAI SZTENDERDET!

## MIT KELL ÁTGONDOLNUNK?

November 27-én az Európai Bizottság a végleges változatát publikálta annak a technikai sztenderdnek (regulatory technical standard – RTS), amely az erős ügyfél-hitelesítésre és a biztonságos kommunikációra vonatkozó szabályozást tartalmazza. A hivatalos publikáció itt elérhető. Az összes RTS közül ez az egyik legfontosabb a számlavezető pénzforgalmi szolgáltatók (Account Servicing Payment Service Provider – ASPSP), egyszerűbben fogalmazva a bankok, valamint a FinTech cégek számára. Az Európai Parlament és a Tanács számára 3 hónap áll rendelkezésre arra, hogy elfogadja vagy visszautasítsa a dokumentumot, és amennyiben nincs változás, akkor 2019 szeptemberétől kötelező lesz az Unióban. Magyarországon a hatályos törvény értelmében ez a dátum 2019. január 1-je.

Online BUSINESS TECHNOLOGIES

www.online.hu/kapcsolat

# TÖRTÉNETE

Az RTS elkészítése az Európai Bankfelügyelet (European Bank Authority – EBA) hatáskörébe tartozik. A nagy érdeklődésre és a rekordszámú visszajelzésre tekintettel a kiadással kapcsolatos konzultáció az eredetileg tervezetthez képest elhúzódott, így az EBA csak 2017 februárjában adta ki az RTS véglegesnek szánt változatát. A Bizottság számos ponton javaslatot tett az RTS megváltoztatására, azonban a Bizottság javaslatait az EBA, részletes indoklás mellett, többségében elutasította. Most, 2018 novemberében úgy tűnik, hogy a végső döntésnél a Bizottság, álláspontjához ragaszkodva, több ponton mégis kiegészítette az RTS-t, fontos kérdésekben egyet nem értve az EBA állásfoglalásaival. De mi is változott a februári változathoz képest?

# VÁLTOZÁSOK

## A „TARTALÉK MECHANIZMUS" (FALLBACK)

A legtöbbet hivatkozott változtatás a screen scraping tiltása, amely immár hivatalossá vált, és ennek a bankok igazán örülhetnek. Azonban ha jobban belemélyedünk a szöveg értelmezésébe, akkor találunk előírást un. „tartalék mechanizmus" kialakítására, amit kötelező biztosítani abban az esetben is, ha dedikált interfész megvalósítása mellett dönt a bank. Ez több dolgot is jelent:

- Ha az ASPSP-nek nincs dedikált interfésze, akkor meg kell engednie külső szolgáltatók (Third Party Provider – TPP), azaz gyakorlatilag a FinTech vállalkozások számára, hogy a banki ügyfelek rendelkezésére álló felületet (interfészt) használják. Ezen a csatornán történő hozzáférés során is azonosítani kell a TPP-ket és biztosítani kell, hogy csak azokhoz az adatokhoz férjenek hozzá, amelyekre van felhatalmazásuk. (31. cikk).
- Ha egy ASPSP úgy dönt, hogy dedikált interfészt használ, akkor a fenti működést mint vészmegoldást kell biztosítania a TPP-k számára (33. cikk).

Meglátásunk szerint az említett megoldás alapvetően maga a screen scraping kiegészítve a TPP azonosításával. Azonban ASPSP-ként felmentést lehet kapni ilyen hozzáférési mechanizmus megvalósítása alól, ha a nemzeti felelős hatóság az EBA-val egyeztetve úgy dönt, hogy a dedikált interfész megfelel az előírt követelményeknek. Ez a felmentés visszavonható, amennyiben két egymást követő naptári héten a dedikált interfészekre vonatkozó előírások nem teljesülnek. A követelmények közül néhánynak elég ködös a megfogalmazása, így a tagállamok között eltérések lehetnek, például:

- "it has been designed and tested in accordance with Article 30(5) to the satisfaction of the payment service providers referred to therein" azaz az interfészt a 30. cikk 5-ös pontjával összhangban, az ott meghatározott pénzforgalmi szolgáltatók megelégedésére alakították ki és tesztelték.

Itt felmerül néhány érdekes kérdés, például hogy mit is jelent pontosan, hogy „megelégedésére"…

Emellett érdekes az is, hogyan fognak a nemzeti hatóságok dönteni a felmentésektől, illetve milyen eszközöket és módszereket fognak és tudnak alkalmazni arra, hogy az összes ASPSP-nél elérhető dedikált interfészt monitorozzák és azokon stressz-tesztet hajtsanak végre. Fontos észben tartani, hogy a PSD2 egy EUszintű szabályozás, aminek fontos eleme a „passporting", azaz a szolgáltatások tagállamokban történő egyszerű honosítása, tehát a tagországok szabályozásának kompatibilisnek kell egymással lennie.

## ÁTIRÁNYÍTÁS AZ API-BAN ÉS EGYÉB AKADÁLYOK

A bankok és FinTech cégek közötti sztenderd interfészekre (Application Programming Interface – API) vonatkozó legelterjedtebb standardok (például NextGenPSD2, Open Banking UK, STET) az OAuth szabványra épülnek, ami az átirányítás koncepciójára épül. Ezt a szabványt használja a Google és a Facebook is, amikor Google és Facebook fiókjainkkal egyéb szolgáltatásokba jelentkezünk be, így ez volt a legkézenfekvőbb választás a PSD2 esetében is, amikor a TPP-k az ügyfelek banki azonosítóját használják a banki szolgáltatások eléréséhez. Ezt a típusú hozzáférést kérdőjelezik meg a dedikált interfészekre vonatkozó legújabb változások, amelyek az RTS 32-es cikkében találhatóak.

Ha egy bank az RTS szabályainak megfelelő interfészt akar létrehozni, akkor tilos akadályt állítania a megbízásos online átutalási és számlaösszesítő szolgáltatások útjába. Felmerülhet a kérdés, hogy vajon mit is értünk akadály alatt. Itt az RTS egyértelműbben fogalmaz, mint máshol, bár a szövegezésben a „lehet" (may) szócska használata elgondolkodtató, felvetve a kérdést, hogy ezek a tiltások mennyire szigorúak valójában, és vajon érvényesek-e minden esetben. Az egyik ilyen „nem-nem-nem"-et az authentikáció vagy egyéb funkciók kapcsán az ASPSP felületeire történő átirányítás kapta, pedig a bankok alapkoncepciója éppen az volt, hogy mivel a felelősség többségében rajtuk van a szabályozás szerint,

ezért szeretnék a hitelesítést a saját berkeiken belül tartani. Nem teljesen egyértelmű és számos spekuláció tárgya, hogy mit is jelent pontosan ez a tiltás, vajon engedélyezett-e bizonyos esetekben, míg máskor nem. Meglátjuk, mit hoz a jövő, jelenleg nagyon bizonytalan, hogy a TPP-k számára a PSD2-vel összhangban hogyan lehetséges és hogyan engedélyezett az ügyfelek erős ügyfél-hitelesítése az ASPSP-knél.

**Az átirányítás mellett az RTS a következő akadályokat nevesíti:**

- "preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers," – azaz a bankok nem tilthatják meg, hogy a bank által kiadott azonosító adatokat a TTP a szolgáltatásaihoz felhasználja,
- „requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366," – azaz tilos további autorizációt és regisztrációt elvárni a TPP-ktől a direktíva 11, 14 és 15-ös cikkeiben foglaltakon túl,
- „or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services" – azaz tilos a TPP által felmutatott ügyfél-hozzájáruláson túl az ügyfél-hozzájárulásra vonatkozó további vizsgálatot folytatni.

A fentieket többféleképpen lehet értelmezni, egyesek úgy értelmezik, hogy az ASPSP-k nem írhatnak elő regisztrációt a szolgáltatásaik használatához, meg kell bízniuk az EIDAS tanúsítványokban (amelyekre vonatkozóan még nincsen egységes szabvány) és meg kell bízniuk a TPP által felmutatott ügyfél-hozzájárulásban is, habár az API megfelelő kiépítésével biztosítható lenne az utóbbi egyszerű és egyértelmű kezelése. Másfelől létezik olyan értelmezés is, hogy az ASPSP semmilyen módon nem tilthatja meg egy TPP számára, hogy a felhasználó belépési adatait ő küldje el az autentikációhoz, ami miatt néhány banki IT biztonsági szakember biztosan a szívéhez fog kapni.

## MEGVÁLASZOLATLAN KÉRDÉSEK

Az RTS – szabályozói technikai sztenderd – kezdeti verzióitól kezdve kérdéses, hogy mennyire is lesz végső soron „technikai" és „sztenderd", az már ma is látszik, hogy „szabályozó". Az is köztudott volt, hogy a szabályozó hatóság technológia-semleges szeretne lenni, de komoly kockázata van annak is, hogy semmilyen technológiai standard nem készül, és a bankok nincsenek is ehhez hozzászokva. Ebben a ködös környezetben sok kérdés merül fel a szövegezés kapcsán, amely szövegezés néhány helyen teljesen egyértelmű és igencsak megkérdőjelezhető máshol.

Az első és legfontosabb kérdés az erős ügyfél-hitelesítéssel (Strong Customer Authentication – SCA) kapcsolatban, hogy ki dönti el a kivételszabályok valamelyikének alkalmazását. Elsőre azt mondhatnánk a TPP, mivel az ügyfél közvetlenül vele van kapcsolatban, de van pár buktató ebben a gondolatmenetben. Az egyik ilyen buktató, hogy mi történik akkor, ha a TPP az ASPSP autentikációjára hagyatkozik, a másik, hogy mi van ha a TPP úgy dönt, hogy kivételt alkalmaz, de az ASPSP a belső mechanizmusai alapján arra a döntésre jut, hogy muszáj erős hitelesítést végeznie. Nem megoldhatatlan, de nem túl tiszta és nem nyilvánvaló.

A másik kérdés is a kivételekhez kapcsolódik: nem világos, hogy fraud rátát (csalások, csalárd tevékenységek vagy műveletek aránya) az ASPSP csak csatornánként számolhat, vagy lehetőség van tovább finomítani a kivételkezelést, és több csoportban, vagy elég kifinomult megoldás alkalmazása esetén akár szolgáltatónként egyedi rátákat alkalmazhat.

Ez természetesen csak egy szűk részhalmaza azoknak a kérdéseknek, amelyek EU szerte felmerülhetnek az egyeztetéseken. Meglátjuk, mi alakul ki ezekből.

# KONKLÚZIÓ ÉS ELŐRE TEKINTÉS

Ami biztos, a végleges RTS publikálásával még nem értünk az egyeztetések végére az erős ügyfél-hitelesítés és a biztonságos kommunikáció témakörében. Arra számítunk, hogy további tisztázó információk fognak megjelenni a szabályozó oldaláról ahol ez fontos és ott is, ahol akár kevéssé érezzük fontosnak, ezzel is támogatva a zökkenőmentes implementációt. A piac , ahogy eddig is, majd eldönti hogyan válaszol az új kihívásokra, az RTS és az API-k biztosan valósággá válnak, a változás hatalmas lesz és már zajlik, a játéktér át fog alakulni.

Online Business Technologies Ltd.
H-1032 Budapest, Vályog utca 3. | +36-1-437-0700 | www.online.hu/kapcsolat