ČESKÁ BANKOVNÍ ASOCIACE

PSD 2 jako inovace i jako pojítko

Pavel Štěpánek Česká bankovní asociace

Konference *Rozvoj a inovace finančních produktů* 2018

ČESKÁ BANKOVNÍ ASOCIACE

O čem jsem tu hovořil loni

- Technologická inovace nestojí **mimo** ani **proti** tradičním poskytovatelům …
- Do technologické inovace investují i tradiční poskytovatelé
- Je tu prostor pro kooperaci a synergii mezi tradičními a novými hráči, např.:
  - Řízení rizik
  - Analýza klientských dat a customizace vztahu s klienty
  - Rozvoj distribučních kanálů
  - Platební služby a jejich infrastruktura
  - Zpracování a archivace dat
  - Datová bezpečnost, KYC,AML, prevence fraudu

Výhody vyplývají pro obě strany

- Pro banky je technologická inovace klíčem k tomu, aby dále plnily svou nezastupitelnou úlohu v ekonomice…

- Pro fintech firmy je mnohem snadnější s nimi spolupracovat, než jim být soupeřem. Banky mají ke spolupráci předpoklady a navíc mají něco, co se těžko prodává nebo převádí – důvěru veřejnosti

ČESKÁ BANKOVNÍ ASOCIACE

Směrnice PSD 2 - základní fakta

- Revidovaná směrnice o platebních službách

  (Payment Services Directive 2, PSD 2)
- 13. ledna 2018: členské státy EU měly povinnost implementovat směrnici PSD2 (ne všude splněno)
- Situace v ČR
  - Zcela nový zákon o platebním styku
  - Legislativní proces ukončen, zákon č. 370/2017 Sb.
- Cíle
  - Standardizace pravidel pro poskytovatele platebních služeb (vedle bank i nebankovní, ovšem licencované subjekty)
  - Pravidla pro nové hráče na trhu, kteří nebyli dosud regulováni
  - Posílení bezpečnosti celé oblasti platebních služeb

ČESKÁ BANKOVNÍ ASOCIACE

Zákon o platebním styku

- Většina dosavadních ustanovení zůstává v platnosti
- Snížení „spoluúčasti“ klienta na škodě při ztrátě, odcizení platební karty do okamžiku nahlášení (150 => 50 €)
- Blokace částek (hotely apod.)
  - Jen se souhlasem klienta
  - Okamžité uvolnění v okamžiku platby
- Zákaz surcharchingu (znevýhodnění plateb kartou, příplatky)
- Nové typy poskytovatelů platebních služeb
- Povinnost bank jim zpřístupnit data klientů, kteří s tím vysloví souhlas

Co PSD2 a Zákon o platebním styku přinášejí

Pro banky:

- Banky budou muset zpřístupnit data svých klientů dalším poskytovatelům platebních služeb
- Předpokládaná cesta prostřednictvím API
- Technologické zabezpečení dat (vyšší nákladovost), mimo své IT prostředí nad nimi ztrácejí kontrolu.

Pro třetí strany:

- Regulace, nutnost licence, pojištění či kapitál, dohled
- Při souhlasu klienta přístup k platebním informacím
- Rozsah informací podle typu poskytovatele a podle způsobu získání dat (API x screen scraping)

Pro spotřebitele / klienta banky:

- Vyjádřením souhlasu umožní přístup ke svým platebním údajům, ke kterým dnes přistupují prostřednictvím internetového bankovnictví
- Rozsah opět podle způsobu získání dat (API x screen scraping)
- Možnost využívat benefity Fintech společností

ČESKÁ BANKOVNÍ ASOCIACE

Hodnocení a co chybí

Stav

Sice existuje směrnice, máme i nový a účinný Zákon o platebním styku, ale zatím chybí některé evropské guidelines a regulatorní technické standardy (RTS)

Chybí např.

- Guidelines on procedures set by CAs for complaints and infringements
- Guidelines on security measures for operational and security risks
- RTS on Strong Customer Authentication and Secure Communication (!)
- RTS on electronic central register
- Guidelines on home-host cooperation

Schvalování Evropským parlamentem a Radou

- Proces trvá 3 měsíce
- Konzultace s národními regulátory (ne všude kladná stanoviska)
- Účinnost RTS: 18 měsíců po schválení
- Vznik minimálně rok a půl trvajícího právního vakua!

EBA doporučuje kompetentním autoritám, aby se řídily nejposlednějším textem návrhů (dosud neschválených) RTS (sic!)

RTS pro silnou autentizaci a bezpečnou komunikaci

- Evropská komise zveřejnila 27.11.17 návrh RTS pro silnou autentizaci a bezpečnou komunikaci
- EBA se 26.1.18 ohradila, že text, zveřejněný Komisí obsahuje ustanovení, která nebyla v předchozích podkladech EBA obsažena a která s ní nebyla řádně projednána
- Předmětem sporu je, jak se postavit k API, které banky vyvíjejí pro komunikaci se třetími stranami
- Podle Komise musí třetí strany povinně komunikovat prostřednictvím API, pokud je otestoval a schválil regulátor. Pokud API nebudou stabilní, bude nutné náhradní řešení (fall-back solution)
- Definice stability a fall-back solution však chybí. Jedna z možností řešení je i screen scraping (!)
- Implikace dle EBA – regulatorní orgán by měl schvalovat každý jednotlivý interface, to bude při 6000 bankách v EU obtížné …
- Navíc bude regulatorní orgán muset vzít v úvahu, zda daný interface vyhovuje třetím stranám, což narušuje rovnost podmínek. Na druhou stranu třetí strany argumentují, že úplný zákaz screen scrapingu také vytváří nerovné konkurenční prostředí …

Čerstvé signály z Evropského parlamentu spíše indikují, že návrh RTS bude schválen v textaci Evropské komise (nelze jej totiž již měnit, pouze schválit či zamítnout)

Řešení: ČOBS – základní charakteristiky

- Snaha o řešení v ČR: **Český Standard pro Open Banking** https://www.czech-ba.cz/sites/default/files/cesky-standard-pro-open-banking/ceskystandardproopenbankingv011.pdf

- Nepovinný standard, jeho využití však pro kteroukoliv banku přináší následující výhody:
  - Splňuje zákonem a RTS definované požadavky
  - Zavádí moderní technologie API používané v současných řešeních
  - Neřeší pouze potřeby služeb PSD2, ale definuje principy Open Bankingu
  - Přináší podrobné vzorové řešení pro banky
  - Informuje třetí strany o způsobu řešení bank, které ke standardu přistoupí
  - Přináší volitelné varianty vzhledem k rozdílným charakterům produktů bank

Sdělení MF a ČNB z 1. prosince 2017 …

- Rozhodne-li se poskytovatel, který vede uživateli platební účet, využít jako způsob zajištění přístupu třetích stran k účtu API, musí zajistit, aby toto API splňovalo základní zákonné podmínky.
- Přístup k tomuto API musí být založen na zásadě rovnosti a nediskriminace.
- V ČR i v zahraničí vznikly standardizační iniciativy, které si kladou za cíl vyvinout specifikaci pro API splňující výše uvedené požadavky (např. Czech Open Banking Standard vytvořený ČBA, …). Využívání těchto standardů snižuje náklady poskytovatelům, kteří vedou uživateli platební účet, i třetím stranám, a je proto doporučeníhodné.

Jak komunikujeme s třetími stranami

- ČOBS jsme po jeho dokončení prezentovali Fintech asociaci
- I když Standard již byl dokončen a zveřejněn, dohodli jsme se s Fintech asociací, že pokud budou ze strany jejich členů podněty, dotazy či připomínky, budeme připraveni to s nimi probrat a diskutovat.

Zpět na začátek – z dialogu vyplývají výhody pro obě strany

- Pro banky je technologická inovace klíčem k tomu, aby dále plnily svou nezastupitelnou úlohu v ekonomice…
- Pro Fintech firmy je mnohem snadnější s nimi spolupracovat, než jim být soupeřem. Banky mají ke spolupráci předpoklady a navíc mají něco, co se těžko prodává nebo převádí – důvěru veřejnosti …

ČESKÁ BANKOVNÍ ASOCIACE

Okamžité platby

- Společný projekt bank a České národní banky
  - Důvod zapojení ČNB zřejmý: nutnost zajistit mezibankovní převody, vazba na CERTIS
- Standardem dostupnost 365 / 7 / 24
- Limit 400.000 Kč (vychází ze standardu v EU)
  - Příjemci budou prostředky k dispozici v řádu jednotek vteřin
  - Využití: další okamžitá platba, výběr z ATM, platba kartou
- Dokončena „základní pravidla“, popis služeb, rolí, chybových stavů, technická specifikace, principy zúčtování
- 13 bank participuje na realizaci (všechny, které v ČR poskytují retailové služby)
- Termíny
  - Testování: 3. Q 2018
  - Pilotní provoz 4. Q 2018
  - Rutinní zpracování 1. Q 2019

Otázka z loňské konference – regulovat či neregulovat?

FinTech Action plan: For a more competitive and innovative European financial sector

- Rétorika textu nestaví fintech proti tradičním poskytovatelům služeb, fintech považuje za nedílnou součást modernizace finančního odvětví
- Na prvním místě mezi výzvami fintechového fenoménu je kybernetická bezpečnost jako faktor důvěryhodnosti a stability finančního systému
- Souvislost s AML
- Varování před spekulativním charakterem virtuálních měn
- Důraz na GDPR a eiDAS jako nástroje prevence a bezpečného sdílení dat napříč jednotným trhem

EC je názoru, že t.č. není důvod iniciovat na úrovni celé EU rozsáhlou legislativní a regulatorní akci vůči fintechovému fenoménu

Záměrem je jít cestou více dílčích iniciativ:

- Sjednocení regulatorních přístupů vůči crowd-fundingovým platformám a vůči kryptoměnám
- Interface: vytvoření EU API standardu pro PSD2 a GDPR
- Doporučení pro jednotný přístup k rozvíjení nástrojů na podporu inovací (inovační huby, sandboxy …)
- Analýza finanční legislativy s cílem identifikovat prvky, které nejsou technologicky neutrální (umožnění přeshraniční akceptace e-identity, vzdáleného procesu KYC)
- Prověření možnosti vydat doporučení ke cloudovým službám (vzorová smluvní dokumentace, jejich reporting, kontrolování a auditování
- Definování ucelené strategie vůči blockchainům
- Odstraňování překážek při sdílení informací o kybernetických rizicích (případně vydat doporučení jak řešit regulatorně)

ČESKÁ BANKOVNÍ ASOCIACE

Děkuji za pozornost

Záložní slajdy

ČESKÁ BANKOVNÍ ASOCIACE

ČOBS – definované, popsané oblasti

- Technický standard
  - REST (Representational state transfer)
  - JSON (JavaScript Object Notation, JavaScriptový objektový zápis)
  - chybové stavy API
  - best practices
- Security standard
  - způsob autorizace requestů
  - API enrollment do COBS
  - API autorizaci iniciované platby
  - NE: autentizace klienta + práce s certifikáty
- Data - Obsah requestu a response jednotlivých API zpráv definovaný na úroveň jednotlivých elementů, které jsou charakterizovány:
  - popisem elementu
  - výskytem elementu
  - strukturou elementu
  - typem elementu

ČOBS – definované služby

- Informace o účtu (AIS)
  - pasivní operace pro náhled na informace o **platebním** účtu
- Přehled zdrojů:
  - GET seznam platebních účtů klienta
  - GET zůstatek na účtu
  - GET přehled transakcí

ČESKÁ BANKOVNÍ ASOCIACE

ČOBS – definované služby

- Iniciace platby (PIS)
  - **API** definuje jednotný resource pro více typů plateb
  - Primární popis vychází z rozdělení na domácí (v rámci ČR), SEPA, zahraniční v rámci EHP a mimo EHP
- Přehled zdrojů
  - POST dotaz na dostatek prostředků
  - POST nová platba
  - GET status založené/iniciované platby
  - DELETE smazání založené neautorizované platby
  - POST generování autorizačního ID
  - Autorizace platby a (iniciace platby)

Evropský a český registr platebních institucí

- EU: PSD 2 „neřeší“ – úkol pro EBA
- Veřejná konzultace
  - Preference manuálních updatů max 1 regulátor 1x denně
  - Možnost elektronického updatu (standardizovaný file)
  - Webové stránky
  - Řešení prostřednictvím webových služeb (API) odmítnuta jako nákladná a složitá
  - 2x denně bude možné stáhnou soubor s aktuálním stavem registru
- ČR – registr ČNB – JERRS
  - Jednotná evidence registrovaných a regulovaných subjektů
  - Současnost: web, změny max 1x za den
  - Budoucnost: web i webová aplikace (pro profesionály)
- Obavy bank…

Další povinnosti pro banky

- Hlášení tzv. závažných (major) incidentů
- Hlášení bezpečnostních a provozních rizik
  - 1x ročně do 30. 6.
  - Rizika, podvody…
  - ČNB pak bude informovat ECB, EBA
- Hlášení o neúspěšné spolupráci se třetími stranami
- Statistická hlášení
- Náprava neautorizovaných platebních transakcí
- Řešení reklamací (15 pracovních dnů, resp. 35)

Závažné incidenty

- Guideline on major incident reporting => vyhláška ČNB
- Kritéria
  - Počet dotčených položek
  - Počet zasažených uživatelů
  - Doba výpadku
  - Ekonomický dopad
  - Vnitřní eskalace problémů
  - Zasažení jiných poskytovatelů platebních služeb či relevantní infrastruktury
  - Reputace