Deloitte.

Je řešení 3D Secure 2 u card-not-present transakcí v souladu se směrnicí PSD2 a regulačními technickými normami (RTS)?

10. září 2019

Co je řešení 3DS 2.0

Řešení 3D Secure 2.0 („3DS2") označuje online ověření zavedené organizací EMVCo, která je řízena šesti nejvýznamnějšími karetními schématy (American Express, Discover, JCB, Mastercard, UnionPay a VISA). Toto řešení přináší nový přístup k ověření (autentizaci), neboť umožňuje ověření vycházející z rizik, nabízí možnost ověření pomocí biometrických údajů, zlepšuje zkušenost online uživatelů a zároveň řeší řadu problémů souvisejících s 3DS 1.0.

Hlavním důvodem ke změně stávajícího platebního procesu, jakož i procesu ověření/autorizace plateb, jsou regulační požadavky definované v Regulačních technických normách týkajících se silného ověření klienta a bezpečných standardů komunikace („RTS"),[1] které vstoupí v účinnost dne 14. září 2019. Normy RTS specifikují vybrané povinnosti vyplývající ze směrnice PSD2 v kontextu silného ověření klienta (anglicky strong customer authentication, „SCA").

V této souvislosti karetní schémata doporučují a rovněž nařizují používat řešení 3DS2, jež by mělo odpovídat regulačním požadavkům na SCA. Pro zajištění souladu s normami RTS musí dotčené subjekty zajistit, aby SCA bylo součástí všech card-not-present („CNP") transakcí (tj. transakcí, nichž není platební karta fyzicky přítomna). Z tohoto pohledu 3DS2 představuje průmyslový standard autentizačního protokolu, jenž je v souladu s normami RTS.

V rámci SCA existují výjimky v závislosti na typu transakce. Požadavek na provedení SCA se nevztahuje na transakce iniciované obchodníkem („MIT"), objednávky provedené poštovní cestou nebo telefonicky, jakož i na transakce typu business-to-business provedené v rámci přímých kanálů nebo transakce, u nichž se vydavatel karty nebo zpracovatel transakce nachází mimo Evropský hospodářský prostor.

RTS dále umožňuje SCA neprovést, pokud lze uplatnit výjimku z SCA. Pokud jde o CNP transakce v rámci e-commerce, existuje pět druhů možných výjimek – seznam důvěryhodných obchodníků (merchant whitelisting), opakované transakce (tj. transakce se stejným příjemcem a stejnou částkou, ovšem neplést s tzv. transakcemi iniciovanými obchodníkem, tedy merchant-initiated transactions), transakce týkající se malých částek, zabezpečené platební procesy a protokoly společností a výjimka spočívající v analýze transakčních rizik („TRA"), jíž je možné uplatnit u transakcí s nízkým rizikem podvodu. Příjemce však nikdy nemůže rozhodnout, zda výjimku aplikuje či nikoliv – toto rozhodnutí činí vždy poskytovatel platebních služeb plátci (tj. vydavatel) nebo poskytovatel platebních služeb příjemci (tj. zpracovatel). V této souvislosti je nutné zmínit, že konečné rozhodnutí, zda výjimku udělit nebo přijmout, vždy činí poskytovatel platebních služeb plátci, přičemž poskytovatel platebních služeb příjemci může znovu začít aplikovat SCA nebo odmítnout danou transakci provést. V daných případech není použití výjimek povinné, avšak pozitivně ovlivňuje zákaznickou zkušenost.

[1] Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017 (EU), kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

Deloitte.

Výjimka udělovaná různými zpracovateli plateb

V následující tabulce je uveden seznam možných výjimek z SCA, jejich popis a informace, zda hlavní zpracovatelé karetní transakce (acquirers) / zpracovatelé plateb tyto výjimky povolují.

Výjimka	Popis	Adyen	Worldpay	PayPal	Global Payments Europe
		Podporováno ANO/NE/VYDAVATEL			
Malé částky	Poskytovatelům platebních služeb je umožněno, aby neuplatňovali SCA, pokud plátce iniciuje elektronickou platební transakci na dálku za předpokladu, že byly splněny následující podmínky: • částka elektronické platební transakce na dálku nepřevyšuje 30 EUR a • kumulativní částka předchozích elektronických platebních transakcí na dálku iniciovaných plátcem ode dne posledního uplatnění SCA nepřevyšuje částku 100 EUR bez jakéhokoliv časového omezení, nebo • počet předchozích elektronických platebních transakcí na dálku iniciovaných plátcem od posledního uplatnění SCA nepřesáhne pět po sobě následujících jednotlivých elektronických platebních transakcí na dálku.	ANO	ANO	ANO	ANO
TRA (nízké riziko)	Aby platební transakce naplnila definici nízkorizikové transakce pro udělení výjimky z SCA, musí splňovat několik podmínek (kumulativně): • Celková míra podvodů u daného typu transakce, počítáno čtvrtletně od daného data na úrovni poskytovatele platebních služeb, nesmí převýšit referenční míru podvodů pro stejný typ platebních transakcí, jak jsou definovány v normách RTS. • Částka relevantní platební transakce nepřesahuje příslušnou prahovou hodnotu pro výjimku stanovenou	ANO	ANO	ANO	ANO

	v příloze k RTS, tj. max. 500 EUR, nebo je nižší. • Po zohlednění specifických rizikových kritérií transakce nevykazuje znaky, které by naznačovaly vyšší riziko podvodu (jako např. abnormální chování plátce, nevšední lokalita plátce atd.).				
Opakovaná transakce	Poskytovatelé platebních služeb mohou provést SCA, pokud plátce poprvé vytvoří, pozmění nebo iniciuje sérii opakovaných transakcí se stejnou částkou a stejným příjemcem. Poskytovatelé platebních služeb by měli mít povoleno neprovést SCA, pokud to bude v souladu s obecnými požadavky na ověření, a to při iniciaci všech následných platebních transakcí v sérii platebních transakcí provedených za platnosti výše uvedené podmínky.	NE	NE	ANO	ANO
Whitelisting	Poskytovatelé platebních služeb musí provést SCA, pokud plátce vytvoří nebo pozmění seznam důvěryhodných příjemců, a to prostřednictvím poskytovatele platebních služeb, které vede účet plátce. Poskytovatelé platebních služeb by měli mít povoleno neprovádět SCA, pokud to bude v souladu s obecnými požadavky na ověření, jestliže plátce iniciuje platební transakci a příjemce je uveden na seznamu důvěryhodných příjemců, jenž byl v minulosti plátcem vytvořen.	VYDAVATEL	VYDAVATEL	VYDAVATEL	VYDAVATEL
Korporátní protokoly	Poskytovatelé platebních služeb by měli mít povoleno neprovést SCA v případě právnických osob, které iniciují elektronické platební transakce s využitím odpovídajících platebních procesů nebo protokolů, které jsou přístupné pouze plátcům, jež nejsou spotřebiteli, jestliže příslušné orgány budou mít dostatečnou jistotu, že dané procesy nebo protokoly zaručují alespoň ekvivalentní úrovně	VYDAVATEL	VYDAVATEL	VYDAVATEL	VYDAVATEL

	zabezpečení jako ty, jež jsou definovány v PSD2. Tuto výjimku lze aplikovat na elektronické platební transakce provedené platební kartou za předpokladu, že platba kartou je „umožněna pouze plátcům, kteří nejsou spotřebiteli" a že příslušný orgán (e.g. FCA) bude mít dostatečnou jistotu, že dané procesy nebo protokoly zaručují „alespoň ekvivalentní úrovně zabezpečení" jako ty, jež jsou definovány v PSD2, a to předtím, než poskytovatel platebních služeb výjimku aplikuje.				

Co to znamená pro obchodníky

Obchodníci musí zajistit, aby u transakcí bylo provedeno SCA, je-li to právními předpisy vyžadováno. Aby bylo možné aplikovat výjimku z SCA, obchodník musí poslat dodatečné údaje, které vydavateli nebo zpracovateli pomohou u cílové transakce určit nízké riziko. Obchodník by také měl zajistit tok plateb bez SCA v případě transakcí, které nejsou v rozsahu působnosti PSD2/RTS, aby se vyhnul poklesu úspěšnosti transakcí. Pokud je u transakce provedeno SCA nebo pokud vydávající banka aplikuje výjimku z SCA, vydávající banka odpovídá za ztrátu (tzv. chargeback) v případě podvodné transakce.

Přesun odpovědnosti

Následující tabulka popisuje, kdy dochází ve specifických situacích k přesunu odpovědnosti.

Situace	**Aktivita**	**Přesun odpovědnosti**	**Konečná odpovědnost**
Požaduje se SCA	Vydávající banka provede SCA (nebo 3DS), nebo dokonce 3DS neprovede	Ano	Vydavatel
Výjimka pro zpracovatele	Vydávající banka schválí výjimku	Ne	Obchodník
	Vydávající banka odmítne výjimku	Ano	Vydavatel
Výjimka pro vydavatele	X	Ano	Vydavatel
Mimo rozsah (např. MIT transakce)	X	Ne	Obchodník

Doba odkladu

Přestože nejzazší termín nabytí účinnosti RTS je stále 14. září 2019, příslušné vnitrostátní orgány v některých zemích (Velká Británie, Irsko, Německo, Itálie, Nizozemsko, Rakousko, Belgie, Malta, Polsko, Norsko a dle našeho očekávání ještě řada dalších včetně Francie a Španělska) se rozhodly udělit odklad vynucení příslušných povinností dle RTS, aby vydavatelům, zpracovatelům a obchodníkům poskytly více času přizpůsobit se těmto novým pravidlům. Tímto rovněž EMVCo získá čas k zavedení nových autentizačních metod na základě behaviorálních biometrických údajů, které

Deloitte.

by se považovaly za metody v souladu s požadavkem na SCA (tzv. ověření vycházející z rizik, které je součástí standardu 3DS2 organizace EMVCo, nebylo orgánem EBA uznáno jako faktor inherence, v důsledku čehož se na trhu nabízelo jediné řešení, jak splnit kritéria definovaná v RTS, pokud jde o ověření SCA, tj. tzv. out-of-band challenge flow).

Radek Musílek
Senior Managing Associate
Ambruz & Dark Deloitte Legal s.r.o., advokátní kancelář
rmusilek@deloittece.com

Tomáš Huml
Senior Manager | FSI Technology
Deloitte Advisory s.r.o.
thuml@deloittece.com

Jan Ševčík
Senior Consultant | FSI Technology
Deloitte Advisory s.r.o.
jsevcik@deloittece.com