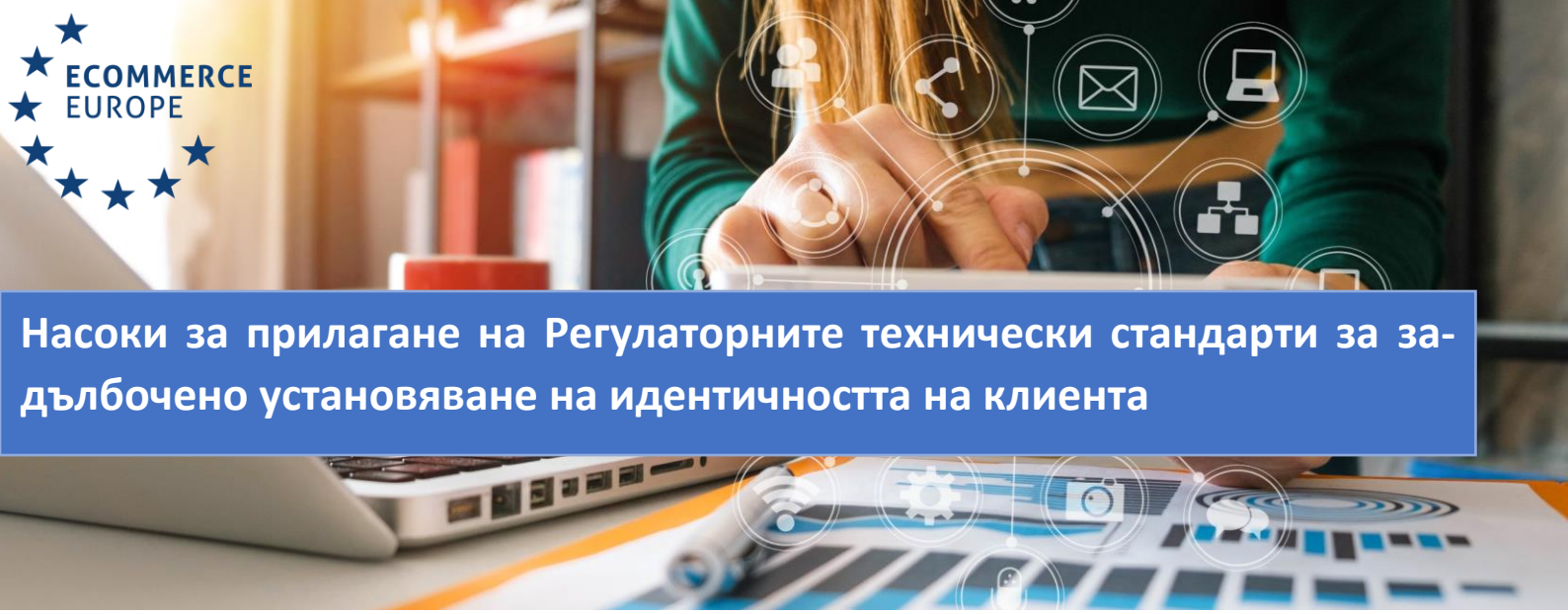

Насоки за прилагане на Регулаторните технически стандарти за задълбочено установяване на идентичността на клиента

Какво представляват регулаторните технически стандарти за задълбочено установяване на идентичността на клиента (RTS SCA)?

От 14 септември 2019 г. в ЕС ще се прилагат нови регулаторни технически стандарти (RTS [1]) за задълбочено установяване на идентичността на клиента (SCA[2]). Те определят специфични изисквания за сигурно установяване на идентичността и комуникация между отделните участници в платежната екосистема.

Задълбоченото установяване на идентичността (SCA) има за цел да повиши нивото на сигурност на електронните плащания, за да се гарантира защитата на потребителите срещу измами. Регулаторните технически стандарти покриват обхвата, имплементацията, както и възможностите за освобождаване от прилагане на SCA.

Информацията, представена в настоящия документ не следва да се приема като правен съвет. Тълкуването на регулаторните технически стандарти за задълбочено установяване на идентичността на клиента може да варира в различните държави-членки.

Защо това засяга онлайн търговците?

Ако търговците не са подготвени, въвеждането на новите стандарти на 14 септември може да доведе до голям брой отказани трансакции. SCA влияе върху начина, по който потребителите удостоверяват идентичността си и следователно върху тяхното потребителско изживяване при онлайн пазаруване.

След септември правилното управление на процеса по установяване на идентичността и по прилагането на изключенията от изискванията за SCA с цел да се предложи безпроблемно и сигурно плащане на клиентите ще бъде един от ключовите двигатели за растежа на електронната търговия в Европа.

Изброените в регулаторните технически стандарти изключения и бързото развитие на технологиите за установяване на идентичността като биометричните данни, ще спомогнат за подобряване на потребителското изживяване, като същевременно ще гарантират сигурността на трансакциите. Степента на готовност на отделните държави в Европа няма да бъде еднаква до влизането в сила на регулаторните технически стандарти.

Какви са следващите ключови стъпки за търговците?

1. Търговците трябва да са запознати с предстоящите промени и да са обърнат към другите страни, отговорни за имплементацията на SCA. На първо време това е тяхната приемаща институция или доставчик на платежни услуги. Търговците трябва да проучат, обсъдят възможните решения и да се запознаят с подготвителните стъпки, които трябва да предприемат, за да гарантират, че клиентите им ще продължават да пазаруват лесно и безпроблемно.
2. В случай, че още не са го направили, търговците трябва се обърнат към своя доставчик на платежни услуги, за да обсъдят MPI решението и да интегрират EMV 3D Secure (3DS). В противен случай има вероятност процентът отказани

[1] RTS – Regulatory Technical Standards / Регулаторни технически стандарти

[2] SCA – Strong Customer Authentication / Задълбочено установяване на идентичността

трансакции да се увеличи. Съществува риск някои банки издатели системно да не одобряват трансакции, при които не се използва 3DS поради опасения, че не са спазени изискванията на регулаторните технически стандарти.

3. В случай че приемащата институция или доставчика на платежни услуги е поискал изключение от прилагането на 3DS за определена трансакция и издателят откаже да авторизира плащането поради липсата на такъв, MPI (Merchant Payment Interface) трябва незабавно да предостави възможност за въвеждането на 3DS.
4. Ако банката издател все още не поддържа EMV 3DS, то търговците трябва да имат възможността да използват 3DS v1.0 (версията, предхождаща EMV 3DS), за да постигнат по-висок процент одобрени трансакциите.
5. Търговците трябва да се уверят, че приемащата институция или доставчика на платежни услуги разполага с точното име на марката или търговското наименование на търговеца (разпознаваеми от потребителите), за да се избегнат недоразумения от страна на потребителите и евентуалното оспорване на покупки. Най-добри резултати се постигат, когато името на търговеца съответства с името на търговската марка, с която е запознат потребителят. За да могат да се възползват максимално от изключението от прилагане на SCA, известно като white listing, търговците трябва да съществуват под едно, уникално име.

Какъв е обхватът на регулаторните технически стандарти за задълбочено установяване на идентичността на клиента?

Задълбоченото установяване на идентичността на клиента трябва да се прилага в 3 случая:

1. Когато потребителят получава достъп до своята платежна сметка онлайн
2. Когато потребителят извършва електронно плащане
3. Когато потребителят извършва каквото и да било дистанционно действие, което би могло да е свързано с риск от измама.

Изискванията се прилагат за плащания, **инициирани от потребителя (платеца)**. Плащания, инициирани от търговеца не попадат в обхвата на стандартите.

Как стои въпросът с „операциите, инициирани от търговеца“?

Електронни плащания, които са инициирани от търговеца (получателя на плащането) въз основа на (1) първоначален мандат от потребителя (платеца), даващ право на търговеца да инициира периодични плащания **и** (2) предварително споразумение между потребителя и търговеца за предоставяне на продукти или услуги, **не попадат в обхвата на изискванията за задълбочено установяване на идентичността на клиента.** (*Забележка: първоначалният мандат подлежи на задълбочено установяване на идентичността на клиента)

Според Европейския банков орган (ЕБО) всички плащания, които се базират на съществуващо споразумение между потребителя и търговеца и при които потребителят вече е дал разрешение на търговеца да инициира последващи операции във връзка с уговореното предоставяне на стоки или услуги, **може да се считат за операции, инициирани от търговеца, при условие, че тези плащания не зависят от конкретно действие на потребителя, което да предизвика иницииране на плащането от търговеца**.

В случаите обаче, в които съществуващо споразумение между потребител и търговец води до последващо таксуване от търговеца, **без** той да е получил мандат за него, то тези плащания не могат да се считат за плащания, инициирани от търговеца и попадат в обхвата на регулаторните технически стандарти.

Какво е задълбочено установяване на идентичността на клиента?

Регулаторните технически стандарти го определят като установяване на идентичността чрез поне два от следните три фактора:

1. **Знание** – Нещо, което само потребителят знае, като например ПИН или парола. (Забележка: Европейският банков орган счита, че номерът на картата с CVV и дата на валидност, както и потребителско име, не принадлежат към „категория знание“.)
2. **Принадлежност** – Нещо, което потребителят **е**, като например употребата на биометрия: пръстов отпечатък, разпознаване на лице, ирис или глас, включително поведенчески модели и др.
3. **Притежание** – Нещо, което само потребителят притежава като карта с чип, мобилен телефон или токен устройство. Според вижданията на ЕБО, за да се счита, че едно устройство отговаря на условията за притежание, трябва да са на лице надеждни средства за потвърждаване на действителното притежание, като например генериране на разписка за динамично валидиране. Еднократна парола (One-Time Password (OTP)), изпратена чрез СМС до мобилен номер се признава за фактор притежание.

Регулаторните технически стандарти изискват избраните фактори да бъдат независими един от друг като компрометирането на едния да не застрашава надеждността на другия. ЕБО също така пояснява, че тези два (от възможни три) фактора за установяване на идентичността трябва да принадлежат към **различни категории (знание, принадлежност и притежание)**.

Възможно ли е да се използва едно единствено устройство за установяване на идентичността?

Разрешено е използването на едно устройство за установяване на идентичността и за осъществяване на покупката. Това означава, например, че смартфон може да се използва едновременно за извършване на трансакцията и за установяване на идентичността на притежателя на картата.

Рискът, свързан с използването на многоцелеви устройства (например смартфони и таблети), трябва да бъде намален чрез използването на отделни среди за сигурно изпълнение (separated secure execution environments).

Трябва да съществуват механизми, които да гарантират, че софтуерът или устройството не са били променени (компрометирани) от получателя или от трета страна.

Какво е динамично свързване?

За онлайн платежни трансакции, всяко задълбочено установяване на идентичността на клиента трябва да бъде свързано с конкретна сума и получател. Това се нарича динамично свързване (dynamic linking).

Това изискване, което свързва установяване на идентичността с конкретен търговец и конкретна сума, цели да гарантира, че валидният код за установяване на идентичността се използва само един път и за конкретната операция, за която е било поискано потвърждението.

Търговци, използващи Card on File: Има ли изключения от RTS?

Търговците, които използват Card on File (CoF), осигуряват по-добро потребителско изживяване в момента на плащане, тъй като търговецът предлага потребителят да запази картовите си данни, като например номер на картата и адрес, така че тази информация да не трябва да бъде попълвана отново всеки път, когато потребителят реши да инициира плащане.

Регулаторните технически стандарти не съдържат конкретни изключения за CoF трансакции. За трансакции, които не попадат в изключенията за прилагане на SCA, задълбоченото установяване на идентичността на клиента се изисква за всяка CoF операция, при която картодържателят инициира плащане. **Включването на търговеца в т.нар. списък на доверени бенефициенти (white listing) би позволило иницирането на трансакции само с един клик в случаите на CoF.** Вижте точка 3 в раздел „Освобождаване от прилагане на задълбочено установяване на идентичността на клиента“, за да разберете повече за включването в този списък.

Позволена ли е делегирано установяване на идентичността със смартфон?

Има редица устройства (напр. смартфони), които предлагат Consumer Device Cardholder Verification Method (CDCVM) за осигуряване на достъп до устройството.

Това е чудесна възможност тези устройства да бъдат използвани от потребителите, за да удостоверят автентичността си при плащане, особено за мобилни NFC плащания, тъй като повечето от тях се случват чрез мобилни портфейли (напр. Apple Pay, Samsung Pay и др.).

Позволена ли е делегирано установяване на идентичността към търговец?

Издателите на карти могат да вземат под внимание средствата за сигурност (security credentials), издадени от търговеца за установяване на идентичността на картодържателя, стига те да отговарят на изискванията за SCA според регулаторните технически стандарти (например да позволяват сигурно биометрично удостоверяване).

За целта ще е необходимо SCA за средствата за сигурност, издадени от търговеца и изрично разрешение от банката издател. Делегираното установяване на идентичността към търговеца е позволено само за ниско рискови търговци и когато картовите данни са дигитализирани и токенизирани в Card on File (CoF) решението на търговеца.

Предстои в най-скоро време картовите схеми да обявят програми за делегиране. Търговците, които имат интерес да се включат в тях, трябва да се свържат със своята приемаща институция или доставчика си на платежни услуги.

Освобождаване от изискването за задълбочено установяване на идентичността на клиента

Регулаторните технически стандарти включват изключения от задължението за задълбочено установяване на идентичността на клиента.

При наличие на едно от по-долу изброените хипотези, търговецът може да не прилага изискванията за SCA. Прилагането на изключението обаче зависи в голяма степен от преценката на банката издател на картата.

Търговците се насърчават да се възползват от изключенията и по-специално от възможността да НЕ се прилага SCA за трансакции с ниска стойност или с малък риск.

1. Повтарящи се операции

Доставчиците на платежни услуги прилагат задълбочено установяване на идентичността на клиента, когато картодържателят създава, изменя или инициира за пръв път редица повтарящи се операции **със същия размер и със същия получател.**

На доставчиците на платежни услуги е разрешено да не прилагат SCA при иницииране на всички последващи платежни операции, включени в поредица от платежни операции.

2. Операции с ниска стойност

Дистанционни електронни платежни операции, които отговарят на следните условия, също могат да бъдат освободени от SCA:

- Размерът на индивидуалната трансакция не надвишава 30 евро и
- Общата сума на трансакциите след последното прилагане на SCA не надвишава 100 евро или броят на трансакциите от последното прилагане на SCA не надвишава 5 броя.

3. Доверени бенефициенти (списък на доверени бенефициенти)

SCA не се прилага когато търговецът (получателят) е включен в списък с доверени бенефициенти. SCA се прилага само при създаването или изменението на списъка. Само издателят на картата на потребителя може да приложи това освобождаване. **За съжаление е вероятно издателите да не са в състояние да предложат прилагането на това изключение от м. септември 2019 г. Ето защо е препоръчително търговците да помислят за някой от другите варианти за освобождаване от изискването за SCA.**

4. Анализ на риска от операциите

За трансакции, за които се счита, че има ниско ниво на риск от измама, не е необходимо доставчикът на платежни услуги да прилага SCA. Условията за това освобождаване са посочени в регулаторните технически стандарти и засягат операции до 500 евро.

Търговците не могат да прилагат директно това освобождаване, а трябва да се обърнат към тяхната приемаща институция или към доставчика на платежни услуги. Ако приемащата институция приложи освобождаването, тя носи отговорност за трансакцията и плащането е гарантирано за търговеца.

5. Други изключения

Регулаторните технически стандарти предвиждат и други изключения като например безконтактни плащания на ПОС, сигурни корпоративни процеси и протоколи на плащане, достъп до информация за платежна сметка, или превод към друга сметка, която се държи от същото лице със същия доставчик на платежни услуги.

EMV3-D Secure (EMV 3DS)

EMV 3DS е еволюцията на текущия интерфейс за установяване на идентичността (3DS v1.0) в индустриален стандарт, който:

- Дава възможност за обмен на транзакционни и потребителски данни (напр. данни за устройства, адрес за доставка и фактуриране), което улеснява вземането на решения и позволява на издателя да прилага освобождаване от SCA.
- Поддържа нови форми на плащане, като например плащания в приложение и мобилни плащания (in app & mobile payments).
- Поддържа допълнителни начини на употреба, като:
    - Credential-on-file (COF): няма нужда клиентите да въвеждат данни за картата в уебсайта или приложението на търговеца за всяка покупка, ако картата е предварително регистрирана.
    - Портфейли като тези на Google и Samsung
    - Токенизация: токен замества реалния номер на картата, който се съхранява, избягвайки компрометирането на пълните данни на картата.

Регулаторните технически стандарти към Втората директивата за платежните услуги (ДПУ2) изискват считано от 14 септември 2019 г. да се прилага SCA за всички дистанционни електронни операции, включително електронната търговия, освен в случаите на прилагане на някое от изключенията (моля, вижте по-долу за повече информация). **Поради това на търговците се препоръчва техния Merchant Payment Interface да има техническата възможност да изпраща заявки за установяване на идентичността чрез EMV 3D Secure (EMV 3DS) протокол, за да се сведе до минимум възможността издателите на карти да откажат онлайн трансакции поради съмнение за измама.**

С внедряването на EMV 3DS се очаква онлайн търговците да постигнат по-високи нива на одобрение на трансакциите, сходни с тези на търговците във физически магазини. Това може да се постигне като се позволи на издателите да прилагат SCA за всяка онлайн покупка, като същевременно им бъдат предоставени достатъчно данни, които да им позволят да я освободят от SCA, за да се гарантира, че трансакциите се осъществяват безпроблемно. **Поради това онлайн търговците трябва да поддържат EMV 3DS.**

Удостоверяването на автентичността с EMV 3DS е и препоръчителният метод, чрез който търговецът да уведоми банката издател за изключението от SCA, което се прилага от приемащата институция. Това обикновено не представлява допълнително усложнение за картодържателя (например, няма да доведе до отказ от поръчката), но позволява на издателя да контролира риска, и съответно ще доведе до увеличаване на процента одобрени трансакции.

EMV 3DS става задължителен за европейските търговци на дребно от септември 2019 г.

Какви действия е добре да предприемат търговците?

1. Търговците трябва да изберат доставчик на платежни услуги, който поддържа EMV 3DS и да направят необходимите имплементации и настройки, за да управлява от тяхно име интерфейса за установяване на идентичността чрез EMV 3DS и 3DS v1.0 (като резервен вариант, когато издателят не поддържа EMV 3DS).
2. Търговците трябва да могат да улавят транзакционните и потребителските данни (напр. адрес за фактуриране и доставка, електронна поща, номер на мобилен телефон или идентификационен номер на устройство) и да ги изпращат до доставчика на платежни услуги, което може да изисква създаването на нов API (приложно-програмен интерфейс).
3. Търговците следва да гарантират, че техните общи условия са съобразени с изискванията за събирането и споделянето на потребителски данни (например в съобщението за поверителност) на Общия регламент за защита на данните (GDPR).
4. Търговците трябва да въведат политика за установяване на идентичността, която да е съгласувана с техния доставчик на платежни услуги или приемаща институция в съответствие с RTS и изключенията от тях, и по-специално в случаите, свързани с изключенията на база анализ на риска от трансакции (TRA) и приложимите допустими нива на измами.
5. Търговците трябва да поискат от своята обслужваща банка да ги регистрира за EMV 3DS с картовите схеми.
6. Търговците трябва да въведат промени на уебсайтове си, така че да отразяват изискванията за EMV 3DS и RTS.

7. В случай че търговец поиска освобождаване от SCA от страна на приемащата банка без искане за установяване на идентичността и операцията е отхвърлена от издателя (особено по причини, различни от финансови или технически откази), то тогава трябва да има механизъм, който автоматично да изпраща искане за EMV 3DS установяване на идентичността. Ако то е одобрено от банката издател, трансакцията ще бъде разрешена. По подобен начин, ако издател все още не поддържа EMV 3DS, търговецът трябва да използва текущата версия 3DS 1.0.2 като резервен вариант.
8. За да предлагат оптимално изживяване за крайния потребител, търговците трябва да интегрират EMV 3DS. Те трябва да работят с доставчика на MPI, приемащата институция за обновяването на частта на приложението за установяване на идентичността със собствен потребителски интерфейс (UI), за да осигурят на клиента същото усещане.
9. Търговците трябва да прилагат SCA към първото периодично плащане. За да се увеличи процента на одобрение, се препоръчва за всяко следващо плащане да се изпраща заявка за EMV 3DS на издателя с позоваване на първоначалния SCA, за да се избегне необходимостта от това, картодържателят отново да бъде помолен да се идентифицира.
10. В случаите на периодични плащания за променливи суми или плащания, за които крайната сума не е известна, търговецът следва ясно да информира потребителя за причините, поради които сумата, за която е приложено SCA, може да бъде различна от окончателната сума на трансакцията.
11. Търговците трябва да се уверят, че размерът на трансакцията, която подлежи на SCA, е равна или по-голяма от сумата, която в последствие ще бъде платена. В противен случай издателят може да откаже трансакцията, а при иницииране на chargeback отговорността се поема от търговеца.
12. Препоръчва се търговците винаги да изпращат заявка за SCA, предвид че издателите на карти могат да откажат авторизация на трансакции, за които няма предварително установяване на идентичността.

Ecommerce Europe

Rue d'Arlon, 69-71

B-1040 Brussel - Belgium

T. +32 (0) 2 502 31 34

info@ecommerce-europe.eu

www.ecommerce-europe.eu

www.ecommercetrustmark.eu

@Ecommerce_EU

Създадено в сътрудничество с Mastercard