Методы двухфакторной аутентификации – позиция Европейской службы банковского надзора

21 июня 2019 г. Европейская служба банковского надзора опубликовала позицию по использованию двухфакторной аутентификации при совершении безналичных платежей.

Двухфакторная аутентификация предполагает подтверждение операций с помощью двух из трех факторов: свойства субъекта, владения и знания. Или, говоря проще, «что есть клиент», «что есть у клиента» и «что знает клиент».

Согласно Второй платежной Директиве, двухфакторная аутентификация должна использоваться при совершении платежей, удаленном доступе к счету или иных действиях, когда есть риски мошенничества[1].

Исключение – небольшие платежи (например, до 50 евро), переводы в пользу доверенных получателей, в терминалах самообслуживания, до пяти последовательных бесконтактных платежей, операции низкого риска[2].

Ниже – таблица допустимых и недопустимых факторов аутентификации, на основе позиции Европейской службы банковского надзора. Из интересного: EBA считает, что ввод данных карты на сайте и подтверждение одноразовым паролем из SMS соответствует требованиям двухфакторной аутентификации – данные, нанесенные на карту, могут быть легко скопированы, а поэтому ненадежны.

Свойство субъекта (Inherence)	**Владение (Possession)**	**Знание (Knowledge)**
Допустимые факторы		
Отпечаток пальца	Владение устройством, подтвержденное путем получения или генерации одноразового пароля на этом устройстве (токены, SMS)	Пароль
Голос	Владение устройством, подтвержденное подписью, сгенерированной устройством (аппаратные или программные ключи)	Пин-код
Рисунок вен	Владение картой или устройством, подтвержденное QR-кодом (когда QR-код сгенерирован на этом устройстве или уникальный	Секретные вопросы

[1] Article 97. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC // Official Journal of the European Union. L 337.

[2] Chapter III. COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication // Official Journal of the European Union. L 69. 13.03.2018.

Свойство субъекта (Inherence)	**Владение (Possession)**	**Знание (Knowledge)**
	код сканируется с помощью этого устройства)	
Лицо или форма кисти	Владение устройством или доступ к браузеру, подтвержденные чипом, интегрированным в устройство, секретным ключом, связывающим устройство и приложение, или привязка браузера к конкретному устройству	Ключевые слова
Паттерн нажатия на клавиши	Владение картой, подтвержденное через считыватель карт	Графический пароль
Пульс или иные биологические паттерны, характерные для клиента (например, фиксируемые с использованием носимых устройств)	Владение картой, подтвержденное динамическим кодом, сгенерированным на карте (Dynamic Security Code)	
Угол, под которым клиент держит устройство		
Недопустимые факторы		
Информация, переданная по сетям связи, например по протоколу EMV 3-D Secure	Установленное на телефоне приложение	Адрес электронной почты или имя пользователя
Графические пароли (swiping path)	Владение картой, подтвержденное данными, нанесенными на карту	Данные, нанесенные на карту
	Владение картой, подтвержденное распечатанными данными (например, список одноразовых паролей)	Одноразовый пароль, сгенерированный или полученный с использованием устройства (аппаратные или программные генераторы токенов, пароли в SMS)
		Список одноразовых паролей

Ассоциация участников рынка электронных денег и денежных переводов "АЭД" - отраслевая ассоциация, созданная в 2010 году. Она объединяет крупнейших игроков российского рынка электронных денег и безналичных переводов.

Ассоциация является широко признанным центром компетенции по платежам, специализированному финансовому регулированию, повышению доступности финансовых услуг и финансовым инновациям как в России, так и за рубежом. Основные задачи АЭД - устойчивое развитие отрасли, распространение лучших деловых практик и оказание экспертной поддержки для государственных органов и частного сектора.

Для получения дополнительной информации, посетите наш сайт www.npaed.ru.

Или свяжитесь с нами по адресу npaed@npaed.ru, либо по телефону 8 (906) 271-04-50.

@npaed http://fb.me/emoney.russia