**REGOLAMENTO DELEGATO (UE) 2018/389 DELLA COMMISSIONE**

**del 27 novembre 2017**

**che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri**

**(Testo rilevante ai fini del SEE)**

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE ([1]), in particolare l'articolo 98, paragrafo 4, secondo comma,

considerando quanto segue:

(1) I servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera sicura, ricorrendo a tecnologie in grado di garantire l'autenticazione sicura dell'utente e di ridurre il più possibile il rischio di frode. La procedura di autenticazione dovrebbe includere, in generale, meccanismi di monitoraggio delle operazioni al fine di rilevare i tentativi di utilizzo delle credenziali di sicurezza personalizzate di un utente dei servizi di pagamento che sono state perse, rubate o oggetto di appropriazione indebita e dovrebbe altresì garantire che l'utente dei servizi di pagamento sia l'utente legittimo, che pertanto acconsente al trasferimento di fondi e all'accesso alle informazioni sul suo conto attraverso un utilizzo normale delle credenziali di sicurezza personalizzate. Inoltre, è necessario specificare i requisiti dell'autenticazione forte del cliente che dovrebbero essere applicati ogni volta che un pagatore accede al suo conto di pagamento online, dispone un'operazione di pagamento elettronico o effettua qualsiasi azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi, imponendo la generazione di un codice di autenticazione che sia difficile da falsificare nella sua interezza o mediante la divulgazione di uno degli elementi sulla base dei quali il codice è stato generato.

(2) Poiché i metodi utilizzati per commettere frodi sono in continua evoluzione, i requisiti dell'autenticazione forte del cliente dovrebbero consentire soluzioni tecniche innovative per fronteggiare l'emergere di nuove minacce per la sicurezza dei pagamenti elettronici. Al fine di garantire che i requisiti stabiliti siano effettivamente attuati su base continuativa, è inoltre opportuno richiedere che le misure di sicurezza per l'applicazione dell'autenticazione forte del cliente e le sue esenzioni, le misure volte a tutelare la riservatezza e l'integrità delle credenziali di sicurezza personalizzate e le misure che stabiliscono standard aperti di comunicazione comuni e sicuri siano documentate, sottoposte a prove periodiche, valutate e controllate da revisori con competenze in materia di sicurezza informatica e pagamenti e indipendenti dal punto di vista operativo. Per consentire alle autorità competenti di monitorare la qualità del riesame di dette misure, tali riesami dovrebbero essere resi disponibili su loro richiesta.

(3) Poiché le operazioni di pagamento elettronico a distanza sono maggiormente esposte al rischio di frode, è necessario introdurre requisiti aggiuntivi per l'autenticazione forte del cliente per tali operazioni, al fine di assicurare che gli elementi colleghino in modo dinamico l'operazione all'importo e al beneficiario specificati dal pagatore al momento di disporre l'operazione.

(4) Il collegamento dinamico è possibile attraverso la generazione di codici di autenticazione soggetti a una serie di rigorosi requisiti di sicurezza. Per mantenere un approccio neutro dal punto di vista tecnologico, è opportuno che non venga richiesta una tecnologia specifica per l'attuazione dei codici di autenticazione. Pertanto, tali codici dovrebbero essere basati su soluzioni quali la generazione e la convalida di password monouso, firme elettroniche o altre conferme della validità basate sulla crittografia che utilizzano chiavi o materiale crittografico contenuto negli elementi di autenticazione, purché siano rispettati i requisiti di sicurezza.

([1]) GU L 337 del 23.12.2015, pag. 35.