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.

(5) È necessario stabilire requisiti specifici per i casi in cui l'importo definitivo non è noto nel momento in cui il pagatore dispone un'operazione di pagamento elettronico a distanza, al fine di garantire che l'autenticazione forte del cliente sia specifica per l'importo massimo per il quale il pagatore ha prestato il consenso, come previsto dalla direttiva (UE) 2015/2366.

(6) Al fine di garantire l'applicazione dell'autenticazione forte del cliente, è altresì necessario imporre adeguate caratteristiche di sicurezza per gli elementi dell'autenticazione forte del cliente classificati nella categoria della conoscenza (qualcosa che solo l'utente conosce), come ad esempio la lunghezza o la complessità, per gli elementi classificati nella categoria del possesso (qualcosa che solo l'utente possiede), come ad esempio le specifiche dell'algoritmo, la lunghezza della chiave e l'entropia delle informazioni, e per i dispositivi e il software che leggono gli elementi classificati nella categoria dell'inerenza (qualcosa che caratterizza l'utente), come ad esempio le specifiche dell'algoritmo, il sensore biometrico e le funzioni di protezione del modello, in particolare per attenuare il rischio che tali elementi siano scoperti o svelati a soggetti non autorizzati e utilizzati da questi ultimi. È inoltre necessario stabilire i requisiti volti a garantire che tali elementi siano indipendenti, in modo tale che la violazione di uno di essi non comprometta l'affidabilità degli altri, in particolare quando uno qualsiasi di questi elementi è utilizzato mediante un dispositivo multifunzione, vale a dire un dispositivo come un tablet o un telefono cellulare che può essere utilizzato sia per disporre l'esecuzione del pagamento sia nel processo di autenticazione.

(7) I requisiti dell'autenticazione forte del cliente si applicano ai pagamenti disposti dal pagatore, indipendentemente dal fatto che questo sia una persona fisica o una persona giuridica.

(8) Per la loro stessa natura, i pagamenti effettuati attraverso strumenti di pagamento anonimi non sono soggetti all'obbligo dell'autenticazione forte del cliente. Qualora l'anonimato di tali strumenti sia rimosso per motivi contrattuali o legislativi, i pagamenti sono soggetti ai requisiti di sicurezza imposti dalla direttiva (UE) 2015/2366 e dalle norme tecniche di regolamentazione.

(9) A norma della direttiva (UE) 2015/2366, le deroghe al principio dell'autenticazione forte del cliente sono state definite in base al livello di rischio, all'importo, alla frequenza dell'operazione e al canale di pagamento utilizzato per l'esecuzione dell'operazione di pagamento.

(10) Le azioni che comportano l'accesso al saldo e alle operazioni recenti di un conto di pagamento senza la divulgazione dei dati sensibili relativi ai pagamenti, i pagamenti ricorrenti a favore dello stesso beneficiario precedentemente impostati o confermati dal pagatore attraverso il ricorso all'autenticazione forte del cliente e i pagamenti da e verso la stessa persona fisica o giuridica con conti presso lo stesso prestatore di servizi di pagamento presentano un basso livello di rischio, il che permette ai prestatori di servizi di pagamento di non applicare l'autenticazione forte del cliente. Ciò non tiene conto del fatto che a norma degli articoli 65, 66 e 67 della direttiva (UE) 2015/2366, i prestatori di servizi di disposizione di ordine di pagamento, i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta e i prestatori di servizi di informazione sui conti dovrebbero richiedere al prestatore di servizi di pagamento di radicamento del conto le informazioni necessarie ed essenziali per la fornitura di un determinato servizio di pagamento, e ottenerle dallo stesso, solo con il consenso dell'utente del servizio di pagamento. Tale consenso può essere fornito singolarmente per ogni richiesta di informazioni o per ogni pagamento da disporre o, per i prestatori di servizi di informazione sui conti, sotto forma di mandato per i conti di pagamento designati e le operazioni di pagamento associate, come stabilito nell'accordo contrattuale con l'utente del servizio di pagamento.

(11) Le esenzioni per i pagamenti di importo ridotto senza contatto fisico al punto vendita, che sono condizionate anche ad un numero massimo di operazioni consecutive o di un determinato valore massimo fisso delle operazioni consecutive senza applicazione dell'autenticazione forte del cliente, consentono lo sviluppo di servizi di pagamento intuitivi e a basso rischio e dovrebbero pertanto essere previste. È altresì opportuno prevedere un'esenzione per le operazioni di pagamento elettronico disposte da terminali incustoditi, nel cui caso l'autenticazione forte del cliente non sempre è facilmente applicabile per ragioni operative (ad esempio, per evitare code e potenziali incidenti ai caselli o altri rischi per la sicurezza).

(12) Come nel caso dell'esenzione per i pagamenti di importo ridotto senza contatto fisico al punto vendita, occorre trovare il giusto equilibrio tra l'interesse a una maggiore sicurezza nei pagamenti a distanza e le esigenze di facilità di utilizzo e accessibilità dei pagamenti nel settore del commercio elettronico. In linea con tali principi, le soglie al di sotto delle quali non occorre applicare l'autenticazione forte del cliente dovrebbero essere fissate con prudenza, in modo da limitarle unicamente agli acquisti online di importo ridotto. Le soglie per gli acquisti online dovrebbero essere stabilite con maggiore prudenza, in quanto il fatto che la persona non sia fisicamente presente al momento dell'acquisto pone un rischio leggermente più elevato per la sicurezza.

(13) I requisiti dell'autenticazione forte del cliente si applicano ai pagamenti disposti dal pagatore, indipendentemente dal fatto che questo sia una persona fisica o una persona giuridica. Molti pagamenti per le imprese sono disposti mediante appositi processi o protocolli che garantiscono gli elevati livelli di sicurezza dei pagamenti che la direttiva (UE) 2015/2366 mira a conseguire attraverso l'autenticazione forte del cliente. Se le autorità competenti constatano che i processi e i protocolli di pagamento resi disponibili unicamente ai pagatori che non sono consumatori consentono di conseguire gli obiettivi della direttiva (UE) 2015/2366 in termini di sicurezza, i prestatori di servizi di pagamento possono essere esentati dai requisiti relativi all'autenticazione forte del cliente in relazione a detti processi o protocolli.

(14) Nel caso di analisi dei rischi connessi all'operazione in tempo reale che classifichino un'operazione di pagamento come a basso rischio, è opportuno prevedere un'esenzione per i prestatori di servizi di pagamento che non intendono applicare l'autenticazione forte del cliente mediante l'adozione di requisiti efficaci e basati sul rischio che garantiscano la sicurezza dei fondi e dei dati personali dell'utente del servizio di pagamento. Tali requisiti basati sul rischio dovrebbero combinare i risultati dell'analisi dei rischi, che confermino che non sono stati rilevati schemi di spesa o di comportamento anomali del pagatore, tenendo conto di altri fattori di rischio come le informazioni sulla localizzazione del pagatore e del beneficiario, con soglie monetarie basate sui tassi di frode calcolati per i pagamenti a distanza. Qualora, sulla base dell'analisi dei rischi connessi alle operazioni in tempo reale, un pagamento non possa essere considerato a basso rischio, il prestatore di servizi di pagamento dovrebbe tornare ad applicare l'autenticazione forte del cliente. Il valore massimo di tale esenzione basata sul rischio dovrebbe essere fissato in modo da corrispondere a un tasso di frode molto basso, anche facendo un raffronto con i tassi di frode di tutte le operazioni di pagamento del prestatore di servizi di pagamento, comprese quelle per le quali è stata utilizzata l'autenticazione forte del cliente, in un determinato periodo di tempo e su base continuativa.

(15) Ai fini di un'attuazione efficace, i prestatori di servizi di pagamento che desiderano beneficiare delle esenzioni dall'autenticazione forte del cliente dovrebbero monitorare regolarmente e comunicare alle autorità competenti e all'Autorità bancaria europea (ABE), su loro richiesta, per ogni tipo di operazione di pagamento, il valore delle operazioni di pagamento fraudolente o non autorizzate e i tassi di frode osservati per l'insieme delle loro operazioni di pagamento, siano esse effettuate ricorrendo all'autenticazione forte del cliente o disposte in regime di esenzione da tale autorizzazione.

(16) La raccolta di questi nuovi dati storici sui tassi di frode delle operazioni di pagamento elettronico contribuirà anche ad un efficace riesame da parte dell'ABE delle soglie applicabili per un'esenzione dall'autenticazione forte del cliente sulla base dell'analisi dei rischi connessi alle operazioni in tempo reale. A norma dell'articolo 98, paragrafo 5, della direttiva (UE) 2015/2366 e dell'articolo 10 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio [1], l'ABE dovrebbe rivedere le norme tecniche di regolamentazione e, se del caso, trasmettere i progetti di aggiornamento delle stesse alla Commissione, presentando nuovi progetti di soglie e di tassi di frode corrispondenti, allo scopo di migliorare la sicurezza dei pagamenti elettronici a distanza.

(17) Ai prestatori di servizi di pagamento che si avvalgono di una qualsiasi delle esenzioni previste dovrebbe essere consentito in qualsiasi momento di scegliere di applicare l'autenticazione forte del cliente alle azioni e alle operazioni di pagamento di cui alle suddette disposizioni.

(18) Le misure che tutelano la riservatezza e l'integrità delle credenziali di sicurezza personalizzate, come pure i dispositivi e il software per l'autenticazione, dovrebbero limitare i rischi di frode attraverso l'uso non autorizzato o fraudolento degli strumenti di pagamento e l'accesso non autorizzato ai conti di pagamento. A tal fine è necessario introdurre requisiti relativi alla creazione e alla consegna sicure delle credenziali di sicurezza personalizzate e alla loro associazione all'utente dei servizi di pagamento, nonché creare le condizioni necessarie per il rinnovo e la disattivazione di tali credenziali.

(19) Al fine di assicurare una comunicazione efficace e sicura tra i soggetti interessati nel contesto dei servizi di informazione sui conti, dei servizi di disposizione di ordine di pagamento e della conferma della disponibilità dei fondi, è necessario specificare i requisiti relativi agli standard aperti di comunicazione comuni e sicuri ai quali tutti i prestatori di servizi di pagamento interessati sono tenuti a conformarsi. La direttiva (UE) 2015/2366 prevede l'accesso e l'utilizzo delle informazioni sui conti di pagamento da parte dei prestatori di servizi di informazione sui conti. Il presente regolamento pertanto non modifica le norme sull'accesso ai conti diversi dai conti di pagamento.

---

[1] Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12).

(20) Tutti i prestatori di servizi di pagamento di radicamento del conto con conti di pagamento accessibili online dovrebbero offrire almeno un'interfaccia di accesso che consenta la comunicazione sicura con i prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta. L'interfaccia dovrebbe consentire ai prestatori di servizi di informazione sui conti, ai prestatori di servizi di disposizione di ordine di pagamento e ai prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta di identificarsi presso il prestatore di servizi di pagamento di radicamento del conto. Essa dovrebbe inoltre consentire ai prestatori di servizi di informazione sui conti e ai prestatori di servizi di disposizione di ordine di pagamento di avvalersi delle procedure di autenticazione fornite dal prestatore di servizi di pagamento di radicamento del conto all'utente dei servizi di pagamento. Per assicurare la neutralità dal punto di vista tecnologico e del modello di attività, i prestatori di servizi di pagamento di radicamento del conto dovrebbero essere liberi di decidere se offrire un'interfaccia dedicata per la comunicazione con i prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta o se consentire, ai fini di tale comunicazione, l'uso dell'interfaccia per l'identificazione e la comunicazione con gli utenti dei servizi di pagamento dei prestatori di servizi di pagamento di radicamento del conto.

(21) Per consentire ai prestatori di servizi di informazione sui conti, ai prestatori di servizi di disposizione di ordine di pagamento e ai prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta di sviluppare le loro soluzioni tecniche, le specifiche tecniche dell'interfaccia dovrebbero essere adeguatamente documentate e messe a disposizione del pubblico. Inoltre, il prestatore di servizi di pagamento di radicamento del conto dovrebbe offrire un meccanismo che consenta ai prestatori di servizi di pagamento di provare le soluzioni tecniche almeno sei mesi prima della data di applicazione delle norme di regolamentazione oppure, se il lancio avviene dopo la data di applicazione di tali norme, prima della data di immissione sul mercato dell'interfaccia. Per assicurare l'interoperabilità delle diverse soluzioni tecnologiche di comunicazione, l'interfaccia dovrebbe utilizzare standard di comunicazione sviluppati da organismi di normazione internazionali o europei.

(22) La qualità dei servizi forniti dai prestatori di servizi di informazione sui conti e dai prestatori di servizi di disposizione di ordine di pagamento dipenderà dal corretto funzionamento delle interfacce predisposte o adattate dai prestatori di servizi di pagamento di radicamento del conto. È quindi importante che, nel caso in cui tali interfacce non siano conformi alle disposizioni contenute nelle norme tecniche, siano adottate misure atte a garantire la continuità operativa a vantaggio degli utenti di detti servizi. Spetta alle autorità nazionali competenti provvedere affinché i prestatori di servizi di informazione sui conti e i prestatori di servizi di disposizione di ordine di pagamento non siano bloccati o ostacolati nella fornitura dei loro servizi.

(23) Qualora l'accesso ai conti di pagamento sia offerto tramite un'interfaccia dedicata, al fine di garantire il diritto degli utenti dei servizi di pagamento di avvalersi dei prestatori di servizi di disposizione di ordine di pagamento e dei servizi che consentono l'accesso alle informazioni sui conti, come previsto dalla direttiva (UE) 2015/2366, è necessario prescrivere che le interfacce dedicate presentino lo stesso livello di disponibilità e di prestazioni dell'interfaccia disponibile per l'utente dei servizi di pagamento. I prestatori di servizi di pagamento di radicamento del conto dovrebbero inoltre definire indicatori chiave di prestazione e obiettivi in materia di livello del servizio trasparenti per la disponibilità e le prestazioni delle interfacce dedicate che siano almeno altrettanto rigorosi di quelli definiti per l'interfaccia utilizzata dagli utenti dei servizi di pagamento. Tali interfacce dovrebbero essere provate dai prestatori di servizi di pagamento che le utilizzeranno e dovrebbero altresì essere sottoposte a prove di stress e monitorate dalle autorità competenti.

(24) Affinché i prestatori di servizi di pagamento che si avvalgono dell'interfaccia dedicata possano continuare a prestare i propri servizi in caso di problemi di disponibilità o di prestazioni inadeguate, è necessario prevedere, a condizioni rigorose, un meccanismo alternativo che consenta loro di utilizzare l'interfaccia predisposta dal prestatore di servizi di pagamento di radicamento del conto per identificare i propri utenti dei servizi di pagamento e comunicare con loro. Determinati prestatori di servizi di pagamento di radicamento del conto saranno esentati dall'obbligo di fornire tale meccanismo alternativo attraverso le loro interfacce per l'interazione con i clienti qualora le autorità competenti constatino che le interfacce dedicate soddisfano le condizioni specifiche atte ad assicurare una concorrenza senza ostacoli. Nel caso in cui le interfacce dedicate esentate non soddisfino le condizioni previste, le autorità competenti devono revocare le esenzioni concesse.

(25) Al fine di consentire alle autorità competenti di sorvegliare e monitorare in modo efficace l'attuazione e la gestione delle interfacce di comunicazione, i prestatori di servizi di pagamento di radicamento del conto dovrebbero pubblicare una sintesi della documentazione pertinente disponibile sul proprio sito web e fornire, su richiesta, alle autorità competenti la documentazione delle soluzioni in caso di emergenza. I prestatori di servizi di pagamento di radicamento del conto dovrebbero inoltre rendere accessibili al pubblico le statistiche sulla disponibilità e le prestazioni di detta interfaccia.

(26) Al fine di preservare la riservatezza e l'integrità dei dati, è necessario garantire la sicurezza delle sessioni di comunicazione tra i prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di

pagamento che emettono strumenti di pagamento basati su carta. È necessario in particolare imporre l'utilizzo della crittografia sicura nello scambio dei dati tra prestatori di servizi di informazione sui conti, prestatori di servizi di disposizione di ordine di pagamento, prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta e prestatori di servizi di pagamento di radicamento del conto.

(27) Al fine di rafforzare la fiducia degli utenti e garantire l'autenticazione forte del cliente, è opportuno prendere in considerazione l'utilizzo dei mezzi di identificazione elettronica e dei servizi fiduciari, come previsto dal regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([1]), in particolare per quanto riguarda i regimi di identificazione elettronica notificati.

(28) Al fine di allineare le date di applicazione, il presente regolamento dovrebbe essere applicabile a decorrere dalla stessa data a partire dalla quale gli Stati membri devono provvedere all'applicazione delle misure di sicurezza di cui agli articoli 65, 66, 67 e 97 della direttiva (UE) 2015/2366.

(29) Il presente regolamento si basa sui progetti di norme tecniche di regolamentazione che l'Autorità bancaria europea (ABE) ha presentato alla Commissione.

(30) L'ABE ha svolto consultazioni pubbliche aperte e trasparenti sul progetto di norme tecniche di regolamentazione su cui si basa il presente regolamento, ne ha analizzato i potenziali costi e benefici e ha richiesto il parere del gruppo delle parti interessate nel settore bancario, istituito dall'articolo 37 del regolamento (UE) n. 1093/2010,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Il presente regolamento stabilisce i requisiti cui devono conformarsi i prestatori di servizi di pagamento ai fini dell'attuazione di misure di sicurezza che consentano loro di:

a) applicare la procedura dell'autenticazione forte del cliente conformemente all'articolo 97 della direttiva (UE) 2015/2366;

b) esonerare dall'applicazione dei requisiti di sicurezza dell'autenticazione forte del cliente, a condizioni specifiche e limitate, sulla base del livello di rischio, dell'importo e della frequenza dell'operazione di pagamento e del canale di pagamento utilizzato per l'esecuzione dell'operazione;

c) proteggere la riservatezza e l'integrità delle credenziali di sicurezza personalizzate dell'utente dei servizi di pagamento;

d) stabilire standard aperti comuni e sicuri per la comunicazione tra i prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di disposizione di ordine di pagamento, i prestatori di servizi di informazione sui conti, i pagatori, i beneficiari e altri prestatori di servizi di pagamento in relazione alla prestazione e all'uso dei servizi di pagamento in applicazione del titolo IV della direttiva (UE) 2015/2366.

Articolo 2

Obblighi generali di autenticazione

1. I prestatori di servizi di pagamento dispongono di meccanismi di monitoraggio delle operazioni che consentono loro di rilevare le operazioni di pagamento non autorizzate o fraudolente ai fini dell'attuazione delle misure di sicurezza di cui all'articolo 1, lettere a) e b).

([1]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 53).

Detti meccanismi si basano sull'analisi delle operazioni di pagamento, tenendo conto di elementi che sono tipici dell'utente dei servizi di pagamento in condizioni di normale utilizzo delle credenziali di sicurezza personalizzate.

2. I prestatori di servizi di pagamento provvedono affinché i meccanismi di monitoraggio delle operazioni tengano conto, come minimo, dei seguenti fattori di rischio:

a) gli elenchi degli elementi di autenticazione compromessi o rubati;

b) l'importo di ciascuna operazione di pagamento;

c) gli scenari di frode noti nella prestazione dei servizi di pagamento;

d) i segnali della presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione;

e) se il dispositivo o il software di accesso sono forniti dal prestatore di servizi di pagamento, un registro dell'utilizzo del dispositivo o del software di accesso forniti all'utente del servizio di pagamento e l'utilizzo anomalo degli stessi.

Articolo 3

Riesame delle misure di sicurezza

1. L'attuazione delle misure di sicurezza di cui all'articolo 1 è documentata, sottoposta a prove periodiche, valutata e controllata in conformità con il quadro giuridico applicabile del prestatore di servizi di pagamento da revisori con competenze in materia di sicurezza informatica e pagamenti e indipendenti dal punto di vista operativo nell'ambito o nei confronti del prestatore di servizi di pagamento.

2. Il periodo tra i controlli di cui al paragrafo 1 è stabilito tenendo conto del pertinente quadro in materia di contabilità e revisione legale applicabile al prestatore di servizi di pagamento.

Tuttavia, i prestatori di servizi di pagamento che si avvalgono dell'esenzione di cui all'articolo 18 sono soggetti a un controllo della metodologia, del modello e dei tassi di frode riferiti come minimo ogni anno. Il revisore che svolge il controllo dispone di competenze in materia di sicurezza informatica e di pagamenti ed è indipendente dal punto di vista operativo nell'ambito o nei confronti del prestatore di servizi di pagamento. Durante il primo anno di applicazione dell'esenzione di cui all'articolo 18, e in seguito almeno ogni tre anni, o più frequentemente su richiesta dell'autorità competente, detto controllo è effettuato da un revisore esterno indipendente e qualificato.

3. Detto controllo valuta la conformità delle misure di sicurezza del prestatore di servizi di pagamento ai requisiti di cui al presente regolamento e riferisce in merito.

L'intera relazione è resa disponibile alle autorità competenti su loro richiesta.

CAPO II

MISURE DI SICUREZZA PER L'APPLICAZIONE DELL'AUTENTICAZIONE FORTE DEL CLIENTE

Articolo 4

Codice di autenticazione

1. Se i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente conformemente all'articolo 97, paragrafo 1, della direttiva (UE) 2015/2366, l'autenticazione si basa su due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza e comporta la generazione di un codice di autenticazione.

Il codice di autenticazione è accettato solo una volta dal prestatore di servizi di pagamento quando il pagatore lo utilizza per accedere al suo conto di pagamento online, disporre un'operazione di pagamento elettronico o effettuare qualsiasi azione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento adottano misure di sicurezza al fine di garantire il soddisfacimento di tutti i requisiti elencati di seguito:

a) nessuna informazione su uno qualsiasi degli elementi di cui al paragrafo 1 può essere ricavata dalla comunicazione del codice di autenticazione;

b) non è possibile generare un nuovo codice di autenticazione sulla base della conoscenza di un altro codice di autenticazione generato in precedenza;

c) il codice di autenticazione non può essere contraffatto.

3. I prestatori di servizi di pagamento provvedono affinché l'autenticazione mediante generazione di un codice di autenticazione comprenda le seguenti misure:

a) se l'autenticazione per l'accesso a distanza, i pagamenti elettronici a distanza e qualsiasi altra azione effettuata tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi non è riuscita a generare un codice di autenticazione per i fini di cui al paragrafo 1, non è possibile stabilire quali elementi di cui al predetto paragrafo non sono corretti;

b) il numero di tentativi di autenticazione non riusciti che possono essere effettuati consecutivamente, dopo i quali le azioni di cui all'articolo 97, paragrafo 1, della direttiva (UE) 2015/2366 sono temporaneamente o permanentemente bloccate, non è superiore a cinque entro un determinato intervallo di tempo;

c) le sessioni di comunicazione sono protette contro l'acquisizione dei dati di autenticazione trasmessi durante l'autenticazione e contro la manipolazione da parte di soggetti non autorizzati in conformità con gli obblighi di cui al capo V;

d) il tempo massimo di inattività del pagatore in seguito all'autenticazione per l'accesso al conto di pagamento online non è superiore a cinque minuti.

4. Quando il blocco di cui al paragrafo 3, lettera b), è temporaneo, la durata del blocco e il numero di nuovi tentativi sono stabiliti in base alle caratteristiche del servizio fornito al pagatore e a tutti i rischi connessi, tenendo conto almeno dei fattori di cui all'articolo 2, paragrafo 2.

Il pagatore è avvisato prima che il blocco venga reso permanente.

Una volta che il blocco è stato reso permanente, è definita una procedura protetta che consente al pagatore di ripristinare l'uso degli strumenti di pagamento elettronico bloccati.

Articolo 5

Collegamento dinamico

1. Se applicano l'autenticazione forte del cliente conformemente all'articolo 97, paragrafo 2, della direttiva (UE) 2015/2366, in aggiunta ai requisiti di cui all'articolo 4 del presente regolamento, i prestatori di servizi di pagamento adottano anche misure di sicurezza che soddisfano ciascuno dei seguenti requisiti:

a) il pagatore è informato dell'importo dell'operazione di pagamento e del beneficiario;

b) il codice di autenticazione generato è specifico per l'importo dell'operazione di pagamento e il beneficiario concordato dal pagatore al momento di disporre l'operazione;

c) il codice di autenticazione accettato dal prestatore di servizi di pagamento corrisponde all'importo specifico originario dell'operazione di pagamento e all'identità del beneficiario approvato dal pagatore;

d) qualsiasi modifica dell'importo o del beneficiario comporta l'invalidamento del codice di autenticazione generato.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento adottano misure di sicurezza che assicurano la riservatezza, l'autenticità e l'integrità di ognuno dei seguenti elementi:

a) l'importo dell'operazione e il beneficiario durante tutte le fasi dell'autenticazione;

b) le informazioni visualizzate al pagatore durante tutte le fasi dell'autenticazione, comprese la generazione, la trasmissione e l'utilizzo del codice di autenticazione.

3. Ai fini del paragrafo 1, lettera b, e se i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente in conformità dell'articolo 97, paragrafo 2, della direttiva (UE) 2015/2366, si applicano i seguenti requisiti per il codice di autenticazione:

a) in relazione a un'operazione di pagamento basata su carta per la quale il pagatore abbia approvato l'importo esatto dei fondi da bloccare a norma dell'articolo 75, paragrafo 1, di detta direttiva, il codice di autenticazione è specifico per l'importo che il pagatore ha acconsentito a bloccare e che ha approvato al momento di disporre l'operazione;

b) in relazione alle operazioni di pagamento per le quali il pagatore ha dato il consenso a eseguire una serie di operazioni di pagamento elettronico a distanza a favore di uno o più beneficiari, il codice di autenticazione è specifico per l'importo totale della serie di operazioni di pagamento e per i beneficiari specifici.

Articolo 6

Requisiti per gli elementi classificati come conoscenza

1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come conoscenza siano acquisiti da soggetti non autorizzati o divulgati a questi ultimi.

2. L'uso di detti elementi da parte del pagatore è soggetto a misure di attenuazione allo scopo di impedire che vengano divulgati a soggetti non autorizzati.

Articolo 7

Requisiti per gli elementi classificati come possesso

1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come possesso siano utilizzati da soggetti non autorizzati.

2. L'uso di detti elementi da parte del pagatore è soggetto a misure volte a impedirne la duplicazione.

Articolo 8

Requisiti dei dispositivi e del software connessi agli elementi classificati come inerenza

1. I prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi di autenticazione classificati come inerenza e letti dai dispositivi e dal software di accesso forniti al pagatore siano acquisiti da soggetti non autorizzati. Come minimo, i prestatori di servizi di pagamento garantiscono che la probabilità che soggetti non autorizzati effettuino l'autenticazione a nome del pagatore utilizzando detti dispositivi e software sia molto bassa.

2. L'utilizzo di detti elementi da parte del pagatore è soggetto a misure volte ad assicurare che detti dispositivi e software garantiscano la resistenza contro l'utilizzo non autorizzato degli elementi mediante l'accesso ai dispositivi e al software.

Articolo 9

Indipendenza degli elementi

1. I prestatori di servizi di pagamento assicurano che l'utilizzo degli elementi di autenticazione forte del cliente di cui agli articoli 6, 7 e 8 sia soggetto a misure volte a garantire che, in termini di tecnologia, algoritmi e parametri, la violazione di uno degli elementi non comprometta l'affidabilità degli altri elementi.

2. Se uno qualsiasi degli elementi di autenticazione forte del cliente o lo stesso codice di autenticazione sono utilizzati tramite un dispositivo multifunzione, i prestatori di servizi di pagamento adottano misure di sicurezza al fine di attenuare il rischio che deriverebbe dalla compromissione di tale dispositivo multifunzione.

3. Ai fini del paragrafo 2, le misure di attenuazione comprendono ognuno dei seguenti elementi:

a) utilizzo di ambienti di esecuzione protetti separati mediante il software installato nel dispositivo multifunzione;

b) meccanismi volti a garantire che il software o il dispositivo non siano stati alterati dal pagatore o da una terza parte;

c) nel caso in cui ci siano state alterazioni, meccanismi volti ad attenuarne le conseguenze.

CAPO III

ESENZIONI DALL'AUTENTICAZIONE FORTE DEL CLIENTE

Articolo 10

Informazioni sui conti di pagamento

1. I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare i requisiti di cui all'articolo 2 e al paragrafo 2 del presente articolo, se l'utente dei servizi di pagamento è limitato nell'accesso a uno dei seguenti elementi online o a entrambi senza che siano divulgati dati sensibili relativi ai pagamenti:

a) il saldo di uno o più conti di pagamento designati;

b) le operazioni di pagamento eseguite negli ultimi 90 giorni attraverso uno o più conti di pagamento designati.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento non sono esenti dall'applicazione dell'autenticazione forte del cliente se una delle seguenti condizioni è soddisfatta:

a) l'utente del servizio di pagamento accede online alle informazioni di cui al paragrafo 1 per la prima volta;

b) sono trascorsi più di 90 giorni dall'ultima volta che l'utente del servizio di pagamento ha avuto accesso online alle informazioni di cui al paragrafo 1, lettera b), ed è stata applicata l'autenticazione forte del cliente.

Articolo 11

Pagamenti senza contatto fisico al punto vendita

I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi di cui all'articolo 2, se il pagatore dispone un'operazione di pagamento elettronico senza contatto, purché siano soddisfatte le seguenti condizioni:

a) l'importo individuale dell'operazione di pagamento elettronico senza contatto non supera i 50 EUR; e

b) l'importo cumulativo delle precedenti operazioni di pagamento elettronico senza contatto disposte per mezzo di uno strumento di pagamento con una funzionalità senza contatto a partire dalla data dell'ultima applicazione dell'autenticazione forte del cliente non supera i 150 EUR; oppure

c) il numero di operazioni consecutive di pagamento elettronico senza contatto disposte per mezzo di uno strumento di pagamento con una funzionalità senza contatto a partire dalla data dell'ultima applicazione dell'autenticazione forte del cliente non è superiore a cinque.

Articolo 12

Terminali incustoditi per le tariffe di trasporto e le tariffe di parcheggio

I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi di cui all'articolo 2, se il pagatore dispone un'operazione di pagamento elettronico presso un terminale di pagamento incustodito allo scopo di pagare una tariffa di trasporto o di parcheggio.

Articolo 13

Beneficiari di fiducia

1. I prestatori di servizi di pagamento applicano l'autenticazione forte del cliente se un pagatore crea o modifica un elenco di beneficiari di fiducia attraverso il prestatore di servizi di pagamento di radicamento del conto.

2. I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi generali di autenticazione, se il pagatore dispone un'operazione di pagamento e il beneficiario è incluso in un elenco di beneficiari di fiducia precedentemente creato dal pagatore.

Articolo 14

Operazioni ricorrenti

1. I prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando un pagatore crea, modifica o dispone per la prima volta una serie di operazioni ricorrenti dello stesso importo e a favore dello stesso beneficiario.

2. I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi generali di autenticazione, per l'avvio di tutte le operazioni di pagamento successive incluse nella serie di operazioni di pagamento di cui al paragrafo 1.

Articolo 15

Bonifici tra conti detenuti dalla stessa persona fisica o giuridica

I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, a condizione di rispettare gli obblighi di cui all'articolo 2, se il pagatore dispone un bonifico in circostanze in cui il pagatore e il beneficiario sono la stessa persona fisica o giuridica ed entrambi i conti di pagamento sono detenuti dallo stesso prestatore di servizi di pagamento di radicamento del conto.

Articolo 16

Operazioni di modesta entità

I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente se il pagatore dispone un'operazione di pagamento elettronico a distanza, purché siano soddisfatte le seguenti condizioni:

a) l'importo dell'operazione di pagamento elettronico a distanza non supera i 30 EUR; e

b) l'importo cumulativo delle precedenti operazioni di pagamento elettronico a distanza disposte dal pagatore dall'ultima applicazione dell'autenticazione forte del cliente non supera i 100 EUR; oppure

c) il numero delle precedenti operazioni di pagamento elettronico a distanza disposte dal pagatore dall'ultima applicazione dell'autenticazione forte del cliente non è superiore a cinque operazioni singole consecutive.

Articolo 17

Processi e protocolli di pagamento sicuri per le imprese

I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, per le persone giuridiche che dispongono operazioni di pagamento elettronico ricorrendo a processi o protocolli di pagamento dedicati resi disponibili unicamente ai pagatori che non sono consumatori, nel caso in cui le autorità competenti abbiano accertato che tali processi o protocolli garantiscono livelli di sicurezza almeno equivalenti a quelli previsti dalla direttiva (UE) 2015/2366.

Articolo 18

Analisi dei rischi connessi alle operazioni

1. I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente qualora abbiano determinato che l'operazione di pagamento elettronico a distanza disposta dal pagatore presenta un basso livello di rischio secondo i meccanismi di monitoraggio delle operazioni di cui all'articolo 2 e al paragrafo 2, lettera c), del presente articolo.

2. Le operazioni di pagamento elettronico di cui al paragrafo 1 sono considerate come aventi un basso livello di rischio se sono soddisfatte tutte le seguenti condizioni:

a) il tasso di frode per il tipo di operazione, riferito dal prestatore di servizi di pagamento e calcolato in conformità dell'articolo 19, è pari o inferiore ai tassi di frode di riferimento riportati nella tabella figurante nell'allegato rispettivamente per i «pagamenti elettronici a distanza basati su carta» e i «bonifici elettronici a distanza»;

b) l'importo dell'operazione non supera il pertinente valore della soglia di esenzione specificato nella tabella che figura nell'allegato;

c) i prestatori di servizi di pagamento non hanno rilevato uno dei seguenti elementi a seguito di un'analisi dei rischi eseguita in tempo reale:

   i) uno schema di spesa o di comportamento anomalo del pagatore;

   ii) informazioni insolite sull'utilizzo del dispositivo o del software del pagatore a fini di accesso;

   iii) la presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione;

   iv) uno scenario di frode noto nella prestazione dei servizi di pagamento;

   v) localizzazione anomala del pagatore;

   vi) localizzazione ad alto rischio del beneficiario.

3. I prestatori di servizi di pagamento che intendono esentare le operazioni di pagamento elettronico a distanza dall'autenticazione forte del cliente a motivo del fatto che presentano un basso rischio tengono conto almeno dei seguenti fattori di rischio:

a) i precedenti schemi di spesa del singolo utente di servizi di pagamento;

b) la cronologia delle operazioni di pagamento di ciascun utente dei servizi di pagamento del prestatore di servizi di pagamento;

c) la localizzazione del pagatore e del beneficiario al momento dell'operazione di pagamento nei casi in cui il dispositivo o il software di accesso è fornito dal prestatore di servizi di pagamento;

d) il rilevamento di schemi di pagamento anormali dell'utente dei servizi di pagamento rispetto alla sua cronologia delle operazioni di pagamento.

La valutazione effettuata dai prestatori di servizi di pagamento combina tutti questi fattori di rischio in una valutazione dei rischi per ogni singola operazione al fine di determinare se un determinato pagamento debba essere consentito senza l'autenticazione forte del cliente.

Articolo 19

Calcolo dei tassi di frode

1. Per ogni tipo di operazione di cui alla tabella figurante in allegato, il prestatore di servizi di pagamento garantisce che i tassi di frode complessivi concernenti sia le operazioni di pagamento per le quali è stata applicata l'autenticazione forte del cliente sia le operazioni di pagamento eseguite in forza delle esenzioni di cui agli articoli da 13 a 18 sono equivalenti o inferiori al tasso di frode di riferimento per lo stesso tipo di operazione di pagamento riportato nella tabella figurante nell'allegato.

Il tasso di frode complessivo per ciascun tipo di operazione è calcolato come il valore totale delle operazioni a distanza non autorizzate o fraudolente, indipendentemente dal fatto che i fondi siano stati recuperati, diviso per il valore totale di tutte le operazioni a distanza per lo stesso tipo di operazioni, siano esse autenticate mediante l'applicazione dell'autenticazione forte del cliente o eseguite in forza di una delle esenzioni di cui agli articoli da 13 a 18, in un periodo continuativo di tre mesi (90 giorni).

2. Il calcolo dei tassi di frode e i dati che ne risultano sono valutati nell'ambito del controllo di cui all'articolo 3, paragrafo 2, il quale accerta che siano esatti e completi.

3. La metodologia e l'eventuale modello utilizzato dal prestatore di servizi di pagamento per calcolare i tassi di frode, come pure gli stessi tassi di frode, sono adeguatamente documentati e resi pienamente disponibili alle autorità competenti e all'ABE, previa notifica alla o alle autorità competenti, su loro richiesta.

Articolo 20

Cessazione delle esenzioni sulla base dell'analisi dei rischi connessi alle operazioni

1. I prestatori di servizi di pagamento che si avvalgono dell'esenzione di cui all'articolo 18 segnalano immediatamente alle autorità competenti l'eventuale superamento del tasso di frode di riferimento applicabile da parte di uno dei tassi di frode monitorati, per qualsiasi tipo di operazione di pagamento riportato nella tabella figurante nell'allegato, e forniscono alle autorità competenti una descrizione delle misure che intendono adottare per ripristinare la conformità del tasso di frode monitorato con i tassi di frode di riferimento applicabili.

2. I prestatori di servizi di pagamento cessano immediatamente di avvalersi dell'esenzione di cui all'articolo 18 per qualsiasi tipo di operazione di pagamento riportato nella tabella figurante nell'allegato nello specifico intervallo di soglie di esenzione se il loro tasso di frode monitorato supera per due trimestri consecutivi il tasso di frode di riferimento applicabile per lo strumento di pagamento o il tipo di operazione di pagamento nell'intervallo di soglie di esenzione in questione.

3. In seguito alla cessazione dell'esenzione di cui all'articolo 18 conformemente al paragrafo 2 del presente articolo, i prestatori di servizi di pagamento utilizzano nuovamente tale esenzione solo quando il loro tasso di frode calcolato è pari o inferiore ai tassi di frode di riferimento applicabili per lo specifico tipo di operazione di pagamento nell'intervallo di soglie di esenzione per un trimestre.

4. Se intendono avvalersi nuovamente dell'esenzione di cui all'articolo 18, i prestatori di servizi di pagamento lo notificano alle autorità competenti entro un lasso di tempo ragionevole e, prima di riavvalersi dell'esenzione, dimostrano il ripristino della conformità del loro tasso di frode monitorato con il tasso di frode di riferimento applicabile per l'intervallo di soglie di esenzione in questione, conformemente al paragrafo 3 del presente articolo.

Articolo 21

Monitoraggio

1. Al fine di avvalersi delle esenzioni di cui agli articoli da 10 a 18, i prestatori di servizi di pagamento registrano e monitorano i seguenti dati per ogni tipo di operazione di pagamento, disaggregandoli per le operazioni di pagamento a distanza e per quelle non a distanza, almeno ogni trimestre:

a) il valore complessivo delle operazioni di pagamento non autorizzate o fraudolente in conformità dell'articolo 64, paragrafo 2, della direttiva (UE) 2015/2366, il valore complessivo di tutte le operazioni di pagamento e il conseguente tasso di frode, compresa la disaggregazione dei dati per le operazioni di pagamento disposte tramite l'autenticazione forte del cliente e nell'ambito di ciascuna esenzione;

b) il valore medio delle operazioni, compresa la disaggregazione dei dati per le operazioni di pagamento disposte tramite l'autenticazione forte del cliente e nell'ambito di ciascuna esenzione;

c) il numero di operazioni di pagamento per le quali ciascuna esenzione è stata applicata e la loro percentuale in relazione al numero complessivo di operazioni di pagamento.

2. I prestatori di servizi di pagamento rendono disponibili i risultati del monitoraggio di cui al paragrafo 1 alle autorità competenti e all'ABE, previa notifica alla o alle autorità competenti, su loro richiesta.

CAPO IV

RISERVATEZZA E INTEGRITÀ DELLE CREDENZIALI DI SICUREZZA PERSONALIZZATE DEGLI UTENTI DEI SERVIZI DI PAGAMENTO

Articolo 22

Obblighi generali

1. I prestatori di servizi di pagamento assicurano la riservatezza e l'integrità delle credenziali di sicurezza personalizzate dell'utente dei servizi di pagamento, compresi i codici di autenticazione, durante tutte le fasi del processo di autenticazione.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento assicurano il soddisfacimento di tutte le condizioni riportate di seguito:

a) le credenziali di sicurezza personalizzate sono mascherate quando vengono visualizzate e non sono leggibili nella loro interezza quando sono inserite dall'utente dei servizi di pagamento durante l'autenticazione;

b) le credenziali di sicurezza personalizzate nel formato dati e il materiale crittografico relativo alla crittografia delle credenziali di sicurezza personalizzate non sono conservati come testo in chiaro;

c) il materiale crittografico segreto è protetto dalla divulgazione non autorizzata.

3. I prestatori di servizi di pagamento documentano in maniera esauriente il processo relativo alla gestione del materiale crittografico utilizzato per crittografare o rendere altrimenti illeggibili le credenziali di sicurezza personalizzate.

4. I prestatori di servizi di pagamento assicurano che il trattamento e l'instradamento delle credenziali di sicurezza personalizzate e dei codici di autenticazione generati conformemente al capo II avvengano in ambienti protetti secondo standard settoriali rigorosi e ampiamente riconosciuti.

Articolo 23

Creazione e trasmissione delle credenziali

I prestatori di servizi di pagamento provvedono affinché la creazione delle credenziali di sicurezza personalizzate avvenga in un ambiente protetto.

Essi attenuano i rischi di utilizzo non autorizzato delle credenziali di sicurezza personalizzate e dei dispositivi e dei software di autenticazione in seguito a perdita, furto o copia degli stessi prima della consegna al pagatore.

Articolo 24

Associazione all'utente dei servizi di pagamento

1. I prestatori di servizi di pagamento assicurano che solo l'utente dei servizi di pagamento sia associato, in modo sicuro, alle credenziali di sicurezza personalizzate, ai dispositivi e al software di autenticazione.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento assicurano il soddisfacimento di tutte le condizioni riportate di seguito:

a) l'associazione dell'identità dell'utente dei servizi di pagamento alle credenziali di sicurezza personalizzate, ai dispositivi e al software di autenticazione avviene, sotto la responsabilità del prestatore di servizi di pagamento, in ambienti protetti che comprendono almeno i locali del prestatore di servizi di pagamento, l'ambiente Internet fornito da quest'ultimo o altri siti web protetti analoghi utilizzati dal prestatore di servizi di pagamento e dai suoi servizi di sportello automatico, e tenendo conto dei rischi connessi ai dispositivi e ai componenti sottostanti utilizzati durante il processo di associazione che non sono sotto la responsabilità del prestatore di servizi di pagamento;

b) l'associazione tramite un canale a distanza dell'identità dell'utente dei servizi di pagamento alle credenziali di sicurezza personalizzate e ai dispositivi o al software di autenticazione è effettuata ricorrendo all'autenticazione forte del cliente.

Articolo 25

Consegna delle credenziali, dei dispositivi e del software di autenticazione

1. I prestatori di servizi di pagamento provvedono affinché le credenziali di sicurezza personalizzate, i dispositivi e il software di autenticazione siano consegnati all'utente dei servizi di pagamento in un modo sicuro volto a far fronte ai rischi connessi al loro utilizzo non autorizzato conseguente a perdita, furto o copia.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento come minimo applicano tutte le misure elencate di seguito:

a) meccanismi di consegna efficaci e sicuri volti a garantire che le credenziali di sicurezza personalizzate, i dispositivi e il software di autenticazione siano consegnati al legittimo utente dei servizi di pagamento;

b) meccanismi che consentano al prestatore di servizi di pagamento di verificare l'autenticità del software di autenticazione fornito all'utente dei servizi di pagamento tramite Internet;

c) quando la consegna delle credenziali di sicurezza personalizzate avviene al di fuori dei locali del fornitore dei servizi di pagamento o tramite un canale a distanza, misure volte a garantire che:

   i) nessuna parte non autorizzata possa ottenere più di un elemento delle credenziali di sicurezza personalizzate, dei dispositivi o del software di autenticazione quando questi sono forniti attraverso lo stesso canale;

   ii) le credenziali di sicurezza personalizzate, i dispositivi o il software di autenticazione forniti debbano essere attivati prima del loro utilizzo;

d) nei casi in cui sia necessario attivare le credenziali di sicurezza personalizzate, i dispositivi o il software di autenticazione prima del primo utilizzo, misure volte a garantire che l'attivazione abbia luogo in un ambiente protetto nel rispetto delle procedure di associazione di cui all'articolo 24.

Articolo 26

Rinnovo delle credenziali di sicurezza personalizzate

I prestatori di servizi di pagamento provvedono affinché il rinnovo o la riattivazione delle credenziali di sicurezza personalizzate avvengano nel rispetto delle procedure per la creazione, l'associazione e la consegna delle credenziali e dei dispositivi di autenticazione, in conformità degli articoli 23, 24 e 25.

Articolo 27

Distruzione, disattivazione e revoca

I prestatori di servizi di pagamento provvedono a predisporre procedure efficaci per applicare tutte le misure di sicurezza elencate di seguito:

a) la distruzione, la disattivazione o la revoca secondo modalità sicure delle credenziali di sicurezza personalizzate, dei dispositivi e del software di autenticazione;

b) se il prestatore di servizi di pagamento distribuisce dispositivi e software di autenticazione riutilizzabili, prima che il dispositivo o il software siano resi disponibili a un altro utente dei servizi di pagamento, ne viene stabilito, documentato e attuato il loro riutilizzo secondo modalità sicure;

c) la disattivazione o la revoca delle informazioni relative alle credenziali di sicurezza personalizzate memorizzate nei sistemi e nelle banche dati del prestatore di servizi di pagamento e, se del caso, negli archivi pubblici.

CAPO V

STANDARD APERTI DI COMUNICAZIONE COMUNI E SICURI

Sezione 1

Obblighi generali per la comunicazione

Articolo 28

Obblighi relativi all'identificazione

1. I prestatori di servizi di pagamento garantiscono l'identificazione protetta nella comunicazione tra il dispositivo del pagatore e i dispositivi di accettazione del beneficiario per i pagamenti elettronici, inclusi tra gli altri i terminali di pagamento.

2. I prestatori di servizi di pagamento provvedono all'effettiva attenuazione del rischio che la comunicazione sia deviata verso soggetti non autorizzati nelle applicazioni mobili e in altre interfacce per gli utenti dei servizi di pagamento che offrono servizi di pagamento elettronico.

Articolo 29

Tracciabilità

1. I prestatori di servizi di pagamento predispongono procedure volte a garantire che tutte le operazioni di pagamento e altre interazioni con l'utente dei servizi di pagamento, con altri prestatori di servizi di pagamento e con altri soggetti, compresi i commercianti, nel contesto di una prestazione di servizi di pagamento, siano tracciabili, assicurando la conoscenza a posteriori di tutti gli eventi rilevanti per l'operazione elettronica in tutte le varie fasi.

2. Ai fini del paragrafo 1, i prestatori di servizi di pagamento provvedono affinché ciascuna sessione di comunicazione stabilita con l'utente dei servizi di pagamento, con gli altri prestatori di servizi di pagamento e con altri soggetti, compresi i commercianti, si basi sui seguenti elementi:

a) un identificatore univoco della sessione;

b) meccanismi di sicurezza per la registrazione dettagliata dell'operazione, compresi il numero dell'operazione, le marcature orarie e tutti i dati pertinenti relativi all'operazione;

c) le marcature orarie che sono basate su un sistema di riferimento orario unificato e sono sincronizzate in base a un segnale orario ufficiale.

Sezione 2

Obblighi specifici per gli standard aperti di comunicazione comuni e sicuri

Articolo 30

Obblighi generali per le interfacce di accesso

1. I prestatori di servizi di pagamento di radicamento del conto che offrono a un pagatore un conto di pagamento accessibile online dispongono di almeno un'interfaccia che soddisfa tutti i requisiti elencati di seguito:

a) i prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta possono identificarsi presso il prestatore di servizi di pagamento di radicamento del conto;

b) i prestatori di servizi di informazione sui conti possono comunicare in modo sicuro per chiedere e ricevere informazioni su uno o più conti di pagamento designati e sulle operazioni di pagamento associate;

c) i prestatori di servizi di disposizione di ordine di pagamento possono comunicare in modo sicuro per disporre un ordine di pagamento a partire dal conto di pagamento del pagatore e ricevere tutte le informazioni sulla disposizione dell'operazione di pagamento e tutte le informazioni accessibili ai prestatori di servizi di pagamento di radicamento del conto in merito all'esecuzione dell'operazione di pagamento.

2. Ai fini dell'autenticazione dell'utente dei servizi di pagamento, l'interfaccia di cui al paragrafo 1 consente ai prestatori di servizi di informazione sui conti e ai prestatori di servizi di disposizione di ordine di pagamento di avvalersi di tutte le procedure di autenticazione fornite dal prestatore di servizi di pagamento di radicamento del conto all'utente dei servizi di pagamento.

L'interfaccia soddisfa almeno tutti i seguenti requisiti:

a) i prestatori di servizi di disposizione di ordine di pagamento o i prestatori di servizi di informazione sui conti possono dare istruzioni al prestatore di servizi di pagamento di radicamento del conto affinché avvii l'autenticazione sulla base del consenso dell'utente dei servizi di pagamento;

b) le sessioni di comunicazione tra il prestatore di servizi di pagamento di radicamento del conto, il prestatore di servizi di informazione sui conti, il prestatore di servizi di disposizione di ordine di pagamento e l'utente dei servizi di pagamento interessati sono stabilite e mantenute durante l'intero processo di autenticazione;

c) sono assicurate l'integrità e la riservatezza delle credenziali di sicurezza personalizzate e dei codici di autenticazione trasmessi da o attraverso il prestatore di servizi di disposizione di ordine di pagamento o il prestatore di servizi di informazione sui conti.

3. I prestatori di servizi di pagamento di radicamento del conto provvedono affinché le loro interfacce siano conformi agli standard di comunicazione emessi dagli organismi di normazione internazionali o europei.

I prestatori di servizi di pagamento di radicamento del conto assicurano inoltre che le specifiche tecniche delle interfacce siano documentate specificando una serie di routine, protocolli e strumenti di cui necessitano i prestatori di servizi di disposizione di ordine di pagamento, i prestatori di servizi di informazione sui conti e i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta per consentire l'interoperabilità del loro software e delle loro applicazioni con i sistemi dei prestatori di servizi di pagamento di radicamento del conto.

Almeno sei mesi prima della data di applicazione di cui all'articolo 38, paragrafo 2, o prima della data prevista per il lancio sul mercato dell'interfaccia di accesso, quando il lancio avviene dopo la data di cui all'articolo 38, paragrafo 2, i prestatori di servizi di pagamento di radicamento del conto come minimo rendono disponibile la documentazione, a titolo gratuito, su richiesta dei prestatori autorizzati di servizi di disposizione di ordine di pagamento, di servizi di informazione sui conti e di servizi di pagamento che emettono strumenti di pagamento basati su carta o dei prestatori di servizi di pagamento che hanno chiesto l'autorizzazione alle autorità competenti, e pubblicano una sintesi della documentazione sul loro sito web.

4. Oltre a quanto disposto al paragrafo 3, i prestatori di servizi di pagamento di radicamento del conto provvedono affinché, fatta eccezione per le situazioni di emergenza, le eventuali modifiche alle specifiche tecniche delle loro interfacce siano rese preventivamente disponibili, il prima possibile e almeno tre mesi prima dell'attuazione della modifica, ai prestatori autorizzati di servizi di disposizione di ordine di pagamento, di servizi di informazione sui conti e di servizi di pagamento che emettono strumenti di pagamento basati su carta o ai prestatori di servizi di pagamento che hanno chiesto l'autorizzazione alle autorità competenti.

I prestatori di servizi di pagamento documentano le situazioni di emergenza in cui sono state apportate modifiche e rendono disponibile la documentazione alle autorità competenti su richiesta.

5. I prestatori di servizi di pagamento di radicamento del conto rendono disponibile un dispositivo di prova, che comprende l'assistenza, per la prova della connessione e del funzionamento al fine di consentire ai prestatori autorizzati di servizi di disposizione di ordine di pagamento, di servizi di pagamento che emettono strumenti di pagamento basati su carta e di servizi di informazione sui conti o ai prestatori di servizi di pagamento che hanno chiesto l'autorizzazione pertinente, di provare il software e le applicazioni utilizzati per offrire un servizio di pagamento agli utenti. Il dispositivo di prova è reso disponibile al più tardi sei mesi prima della data di applicazione di cui all'articolo 38, paragrafo 2, o prima della data prevista per il lancio sul mercato dell'interfaccia di accesso quando il lancio avviene dopo la data di cui all'articolo 38, paragrafo 2.

Nessuna informazione riservata è tuttavia condivisa attraverso il dispositivo di prova.

6. Le autorità competenti provvedono affinché i prestatori di servizi di pagamento di radicamento del conto rispettino in ogni momento gli obblighi previsti da detti standard in relazione alla o alle interfacce che hanno predisposto. Nel caso in cui un prestatore di servizi di pagamento di radicamento del conto non rispetti gli obblighi previsti per le interfacce in tali standard, le autorità competenti assicurano che la prestazione di servizi di ordine di pagamento e di servizi di informazione sui conti non sia impedita o ostacolata, nella misura in cui i prestatori dei servizi in questione soddisfano le condizioni di cui all'articolo 33, paragrafo 5.

Articolo 31

Opzioni delle interfacce di accesso

I prestatori di servizi di pagamento di radicamento del conto predispongono la o le interfacce di cui all'articolo 30 attraverso un'interfaccia dedicata o consentendo ai prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, di servirsi delle interfacce utilizzate per l'autenticazione e la comunicazione con gli utenti dei servizi di pagamento del prestatore di servizi di pagamento di radicamento del conto.

Articolo 32

Obblighi applicabili alle interfacce dedicate

1. Fatto salvo il rispetto degli articoli 30 e 31, i prestatori di servizi di pagamento di radicamento del conto che hanno predisposto un'interfaccia dedicata provvedono affinché tale interfaccia offra in qualsiasi momento lo stesso livello di disponibilità e di prestazione, anche in relazione all'assistenza, delle interfacce rese disponibili all'utente dei servizi di pagamento per accedere direttamente al suo conto di pagamento online.

2. I prestatori di servizi di pagamento di radicamento del conto che abbiano predisposto un'interfaccia dedicata definiscono indicatori chiave di prestazione e obiettivi in materia di livello del servizio trasparenti e almeno altrettanto rigorosi di quelli stabiliti per l'interfaccia utilizzata dai loro utenti dei servizi di pagamento, in termini sia di disponibilità che di dati forniti, conformemente all'articolo 36. Le interfacce, gli indicatori e gli obiettivi di cui sopra sono monitorati dalle autorità competenti e sottoposti a prove di stress.

3. I prestatori di servizi di pagamento di radicamento del conto che abbiano predisposto un'interfaccia dedicata provvedono affinché tale interfaccia non crei ostacoli alla prestazione dei servizi di disposizione di ordine di pagamento e di informazione sui conti. Detti ostacoli possono consistere, tra l'altro, nell'impedire l'utilizzo da parte dei prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, delle credenziali rilasciate dai prestatori di servizi di pagamento di radicamento del conto ai loro clienti, nell'imporre il reindirizzamento verso l'autenticazione o altre funzioni del prestatore di servizi di pagamento di radicamento del conto, nel richiedere autorizzazioni e registrazioni aggiuntive rispetto a quelle previste dagli articoli 11, 14 e 15 della direttiva (UE) 2015/2366 o nel richiedere ulteriori verifiche del consenso dato dagli utenti dei servizi di pagamento ai prestatori di servizi di disposizione di ordine di pagamento e di servizi di informazione sui conti.

4. Ai fini dei paragrafi 1 e 2, i prestatori di servizi di pagamento di radicamento del conto monitorano la disponibilità e le prestazioni dell'interfaccia dedicata. I prestatori di servizi di pagamento di radicamento del conto pubblicano sul proprio sito web le statistiche trimestrali sulla disponibilità e sulle prestazioni dell'interfaccia dedicata e dell'interfaccia utilizzata dai propri utenti dei servizi di pagamento.

Articolo 33

Misure di emergenza per le interfacce dedicate

1. I prestatori di servizi di pagamento di radicamento del conto includono, nella progettazione dell'interfaccia dedicata, una strategia e piani per le misure di emergenza da applicare in caso di prestazioni dell'interfaccia non conformi all'articolo 32, indisponibilità non programmata dell'interfaccia e guasto dei sistemi. Si può presumere un'indisponibilità non programmata o un guasto dei sistemi quando non viene dato seguito entro 30 secondi a cinque richieste consecutive di accesso alle informazioni per la fornitura dei servizi di disposizione di ordine di pagamento o dei servizi di informazione sui conti.

2. Le misure di emergenza comprendono piani di comunicazione per informare i prestatori di servizi di pagamento che utilizzano l'interfaccia dedicata circa le misure per il ripristino del sistema e una descrizione delle opzioni alternative immediatamente disponibili di cui i prestatori di servizi di pagamento potrebbero avvalersi in questo periodo.

3. Il prestatore di servizi di pagamento di radicamento del conto e i prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, segnalano senza indugio alle rispettive autorità nazionali competenti i problemi con le interfacce dedicate di cui al paragrafo 1.

4. Nell'ambito di un meccanismo di emergenza, i prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, sono autorizzati a utilizzare le interfacce messe a disposizione degli utenti dei servizi di pagamento per l'autenticazione e la comunicazione con il prestatore di servizi di pagamento di radicamento del conto, finché per l'interfaccia dedicata non viene ripristinato il livello di disponibilità e di prestazioni previsto dall'articolo 32.

5. A tal fine, i prestatori di servizi di pagamento di radicamento del conto provvedono affinché i prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1, possano essere identificati e possano avvalersi delle procedure di autenticazione fornite dal prestatore di servizi di pagamento di radicamento del conto all'utente dei servizi di pagamento. Se utilizzano l'interfaccia di cui al paragrafo 4, i prestatori di servizi di pagamento di cui all'articolo 30, paragrafo 1:

a) adottano le misure necessarie per evitare di accedere, memorizzare o trattare i dati per fini diversi dalla prestazione del servizio richiesto dall'utente dei servizi di pagamento;

b) continuano a rispettare gli obblighi derivanti dall'articolo 66, paragrafo 3, e dall'articolo 67, paragrafo 2, della direttiva (UE) 2015/2366;

c) registrano i dati accessibili mediante l'interfaccia gestita dal prestatore di servizi di pagamento di radicamento del conto per i suoi utenti dei servizi di pagamento e forniscono, su richiesta e senza indebiti ritardi, i file di registro all'autorità nazionale competente;

d) giustificano debitamente presso l'autorità nazionale competente, su richiesta e senza indebiti ritardi, l'uso dell'interfaccia resa disponibile agli utenti dei servizi di pagamento per l'accesso diretto al loro conto di pagamento online;

e) informano di conseguenza il prestatore dei servizi di pagamento di radicamento del conto.

6. Le autorità competenti, dopo aver consultato l'ABE per assicurare un'applicazione coerente delle condizioni elencate di seguito, esonerano i prestatori di servizi di pagamento di radicamento del conto che hanno optato per un'interfaccia dedicata dall'obbligo di predisporre il meccanismo di emergenza di cui al paragrafo 4 nel caso in cui l'interfaccia dedicata soddisfi tutte le condizioni seguenti:

a) rispetta gli obblighi applicabili alle interfacce dedicate di cui all'articolo 32;

b) è stata progettata e testata conformemente all'articolo 30, paragrafo 5, con soddisfazione dei prestatori di servizi di pagamento di cui al medesimo articolo;

c) è stata ampiamente utilizzata per almeno tre mesi dai prestatori di servizi di pagamento per offrire servizi di informazione sui conti e servizi di disposizione di ordine di pagamento e per confermare la disponibilità di fondi per i pagamenti basati su carta;

d) gli eventuali problemi relativi all'interfaccia dedicata sono stati risolti senza indebiti ritardi.

7. Le autorità competenti revocano l'esenzione di cui al paragrafo 6 qualora le condizioni di cui alle lettere a) e d) non siano soddisfatte dai prestatori di servizi di pagamento di radicamento del conto per più di due settimane di calendario consecutive. Le autorità competenti informano l'ABE di detta revoca e provvedono affinché il prestatore di servizi di pagamento di radicamento del conto predisponga, nel più breve tempo possibile e al più tardi entro il termine di due mesi, il meccanismo di emergenza di cui al paragrafo 4.

Articolo 34

Certificati

1. Ai fini dell'identificazione di cui all'articolo 30, paragrafo 1, lettera a), i prestatori di servizi di pagamento si avvalgono dei certificati qualificati di sigillo elettronico di cui all'articolo 3, punto 30, del regolamento (UE) n. 910/2014 o di autenticazione di sito web di cui all'articolo 3, punto 39, del suddetto regolamento.

2. Ai fini del presente regolamento, il numero di registrazione quale riportato nei documenti ufficiali in conformità dell'allegato III, lettera c), o dell'allegato IV, lettera c), del regolamento (UE) n. 910/2014 è il numero di autorizzazione del prestatore di servizi di pagamento che emette strumenti di pagamento basati su carta, dei prestatori di servizi di informazione sui conti e dei prestatori di servizi di disposizione di ordine di pagamento, ivi inclusi i prestatori di servizi di pagamento di radicamento del conto che forniscono tali servizi, disponibile nel registro pubblico dello Stato membro di origine a norma dell'articolo 14 della direttiva (UE) 2015/2366 o risultante dalle notifiche di ciascuna autorizzazione concessa a norma dell'articolo 8 della direttiva 2013/36/UE del Parlamento europeo e del Consiglio ([1]) in conformità dell'articolo 20 della medesima direttiva.

3. Ai fini del presente regolamento, i certificati qualificati di sigillo elettronico o di autenticazione di sito web di cui al paragrafo 1 comprendono, in una lingua comunemente utilizzata negli ambienti della finanza internazionale, attributi specifici aggiuntivi in relazione a ciascuno dei seguenti aspetti:

a) il ruolo del prestatore di servizi di pagamento, che può essere uno o più ruoli tra quelli indicati di seguito:

   i) radicamento del conto;

   ii) disposizione di ordine di pagamento;

   iii) informazione sui conti;

   iv) emissione di strumenti di pagamento basati su carta;

b) il nome delle autorità competenti presso le quali il prestatore di servizi di pagamento è registrato.

4. Gli attributi di cui al paragrafo 3 non incidono sull'interoperabilità e sul riconoscimento dei certificati qualificati di sigillo elettronico o di autenticazione di sito web.

([1]) Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

Articolo 35

Sicurezza della sessione di comunicazione

1. I prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, i prestatori di servizi di informazione sui conti e i prestatori di servizi di disposizione di ordine di pagamento provvedono affinché, durante lo scambio di dati via Internet, sia applicata la crittografia sicura tra le parti coinvolte nella comunicazione durante l'intera sessione di comunicazione al fine di preservare la riservatezza e l'integrità dei dati, ricorrendo a tecniche di crittografia avanzate e ampiamente riconosciute.

2. I prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta, i prestatori di servizi di informazione sui conti e i prestatori di servizi di disposizione di ordine di pagamento fanno in modo che la durata delle sessioni di accesso offerte dai prestatori di servizi di pagamento di radicamento del conto sia quanto più breve possibile e terminano deliberatamente ognuna di tali sessioni subito dopo il completamento dell'azione richiesta.

3. Quando mantengono sessioni di rete parallele con il prestatore di servizi di pagamento di radicamento del conto, i prestatori di servizi di informazione sui conti e i prestatori di servizi di disposizione di ordine di pagamento fanno in modo che tali sessioni siano connesse in modo sicuro alle pertinenti sessioni stabilite con l'utente o gli utenti dei servizi di pagamento per prevenire la possibilità che i messaggi o le informazioni che si scambiano possano essere inviati al destinatario sbagliato.

4. I prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta con il prestatore di servizi di pagamento di radicamento del conto forniscono riferimenti espliciti a ognuno dei seguenti elementi:

a) l'utente o gli utenti dei servizi di pagamento e la corrispondente sessione di comunicazione al fine di distinguere le diverse richieste presentate dallo stesso utente o dagli stessi utenti dei servizi di pagamento;

b) per i servizi di disposizione di ordine di pagamento, l'operazione di pagamento disposta identificata in modo univoco;

c) per la conferma sulla disponibilità dei fondi, la richiesta identificata in modo univoco relativa all'importo necessario per l'esecuzione dell'operazione di pagamento basata su carta.

5. I prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di informazione sui conti, i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento che emettono strumenti di pagamento basati su carta provvedono affinché, quando comunicano credenziali di sicurezza personalizzate e codici di autenticazione, questi non siano in alcun momento leggibili, direttamente o indirettamente, da nessun membro del personale.

Nel caso in cui venga compromessa la riservatezza delle credenziali di sicurezza personalizzate di loro competenza, detti prestatori informano senza indebiti ritardi l'utente dei servizi di pagamento cui sono associate e l'emittente di dette credenziali.

Articolo 36

Scambi di dati

1. I prestatori di servizi di pagamento di radicamento del conto rispettano tutti gli obblighi riportati di seguito:

a) forniscono ai prestatori di servizi di informazione sui conti le stesse informazioni relative ai conti di pagamento designati e alle operazioni di pagamento associate rese disponibili all'utente dei servizi di pagamento in caso di richiesta diretta di accesso alle informazioni sui conti, purché tali informazioni non comprendano dati sensibili relativi ai pagamenti;

b) subito dopo aver ricevuto l'ordine di pagamento, forniscono ai prestatori di servizi di disposizione di ordine di pagamento le stesse informazioni in merito all'avvio e all'esecuzione dell'operazione di pagamento fornite o rese disponibili all'utente dei servizi di pagamento quando l'operazione è disposta direttamente da quest'ultimo;

c) su richiesta, trasmettono immediatamente ai prestatori di servizi di pagamento la conferma, sotto forma di un semplice «sì» o «no», relativa alla disponibilità sul conto di pagamento del pagatore dell'importo necessario per l'esecuzione dell'operazione di pagamento.

2. In caso di evento imprevisto o errore durante il processo di identificazione, autenticazione o durante lo scambio di dati, il prestatore di servizi di pagamento di radicamento del conto invia un messaggio di notifica, in cui spiega la causa dell'evento imprevisto o dell'errore, al prestatore di servizi di disposizione di ordine di pagamento o al prestatore di servizi di informazione sui conti e al prestatore di servizi di pagamento che emette strumenti di pagamento basati su carta.

Se il prestatore di servizi di pagamento di radicamento del conto offre un'interfaccia dedicata a norma dell'articolo 32, l'interfaccia prevede messaggi di notifica sugli eventi imprevisti o sugli errori che sono trasmessi dal prestatore di servizi di pagamento che rileva l'evento o l'errore agli altri prestatori di servizi di pagamento che partecipano alla sessione di comunicazione.

3. I prestatori di servizi di informazione sui conti dispongono di meccanismi idonei ed efficaci che impediscono l'accesso a informazioni diverse da quelle relative ai conti di pagamento designati e alle operazioni di pagamento associate, in base al consenso esplicito espresso dall'utente.

4. I prestatori di servizi di disposizione di ordine di pagamento forniscono ai prestatori di servizi di pagamento di radicamento del conto le stesse informazioni richieste all'utente dei servizi di pagamento al momento della disposizione diretta dell'operazione di pagamento.

5. I prestatori di servizi di informazione sui conti possono accedere alle informazioni relative ai conti di pagamento designati e alle operazioni di pagamento associate di cui dispongono i prestatori di servizi di pagamento di radicamento del conto ai fini della prestazione del servizio di informazione in uno dei seguenti casi:

a) ogni volta in cui l'utente dei servizi di pagamento richiede esplicitamente tali informazioni;

b) se l'utente dei servizi di pagamento non richiede esplicitamente tali informazioni, al massimo quattro volte nell'arco di 24 ore, a meno che non sia concordata una frequenza più elevata tra il prestatore di servizi di informazione sui conti e il prestatore di servizi di pagamento di radicamento del conto, con il consenso dell'utente dei servizi di pagamento.

CAPO VI

DISPOSIZIONI FINALI

Articolo 37

Riesame

Fatto salvo l'articolo 98, paragrafo 5, della direttiva (UE) 2015/2366, entro il 14 marzo 2021, l'ABE riesamina i tassi di frode di cui all'allegato del presente regolamento, come pure le esenzioni concesse a norma dell'articolo 33, paragrafo 6, in relazione alle interfacce dedicate e, se del caso, presenta un progetto di aggiornamenti alla Commissione, conformemente all'articolo 10 del regolamento (UE) n. 1093/2010.

Articolo 38

Entrata in vigore

1. Il presente regolamento entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Il presente regolamento si applica a decorrere dal 14 settembre 2019.

3. Tuttavia, i paragrafi 3 e 5 dell'articolo 30 si applicano a decorrere dal 14 marzo 2019.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 27 novembre 2017

Per la Commissione

Il presidente

Jean-Claude JUNCKER

ALLEGATO

	Tasso di frode di riferimento (%):	
Valore della soglia di esenzione	Pagamenti elettronici a distanza basati su carta	Bonifici elettronici a distanza
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015