IL SALONE DEI PAGAMENTI
PAYVOLUTION

CERTFin
CERT Finanziario Italiano

Regole di attuazione della PSD2 con impatti sulla sicurezza: opportunità e criticità per le banche

Milano, 24 novembre 2017

Monica Pellegrino

TLP GREEN

Normative in ambito sicurezza dei pagamenti – Riferimenti alla PSD2

CERTFin
CERT Finanziario Italiano

La **sicurezza dei pagamenti elettronici** rientra tra gli obiettivi della PSD2 → in base al Recital **95** *"è fondamentale per garantire la **protezione degli utenti** e lo sviluppo di un contesto **affidabile** per il commercio elettronico. Tutti i servizi di pagamento offerti elettronicamente dovrebbero essere prestati in maniera **sicura**, adottando **tecnologie in grado di garantire l'autenticazione sicura dell'utente** e di **ridurre al massimo il rischio di frode** (…)*".

Gli articoli principali della PSD2 che hanno ispirato le normative sulla sicurezza dei pagamenti sono il **95**, il **96**, il **97** e il **98:**

- ✓ **Art. 95(1)**:"*(…) i prestatori di servizi di pagamento stabiliscono e gestiscono **procedure efficaci di gestione degli incidenti**, anche per quanto concerne l'individuazione e la classificazione degli incidenti operativi e di sicurezza gravi.*" → **Draft Guidelines on Security Measures for Operational and Security Risks of payment services**
- ✓ **Art. 96(1)**: "*In caso di **grave incidente operativo o relativo alla sicurezza**, i prestatori di servizi di pagamento lo **notificano senza indugio** all'autorità competente dello Stato membro di origine del prestatore di servizi di pagamento.*" → **Guidelines on major incident reporting**
- ✓ **Art. 96(6)**: "*Gli Stati membri provvedono affinché i prestatori di servizi di pagamento forniscano almeno annualmente alle rispettive autorità competenti **dati statistici sulle frodi** connesse ai diversi mezzi di pagamento (…).*" → **Draft Guidelines on fraud reporting requirements**
- ✓ **Art. 97 e 98**: l'EBA emana "*progetti di **norme tecniche di regolamentazione indirizzati** ai prestatori di servizi di pagamento (…)*" → **Draft RTS on SCA and CSC**

Percorso di perfezionamento di guideline e standard tecnici

CERTFin
CERT Finanziario Italiano

	PUBBLICAZIONE DEL CONSULTATION PAPER	PUBBLICAZIONE DEL FINAL REPORT
DRAFT RTS ON SCA AND CSC	12/8/2016	
GUIDELINES ON MAJOR INCIDENT REPORTING	7/12/2016	27/07/2017
DRAFT GUIDELINES ON FRAUD REPORTING REQUIREMENTS	2/8/2017	
DRAFT GUIDELINES ON THE SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS OF PAYMENT SERVICES	5/5/2017	

Draft RTS on SCA and CSC
Percorso di perfezionamento

CERTFin
CERT Finanziario Italiano

I **Regulatory Techical Standards (RTS) sull'autenticazione forte del cliente e sulla comunicazione sicura** sono attualmente in corso di perfezionamento da parte delle Autorità europee. La Commissione Europea dovrebbe pubblicare a breve la **versione definitiva** da comunicare al Parlamento per approvazione finale (senza possibilità di emendamenti).

- **Discussion Paper EBA**: 8 dicembre 2015
- **Consultation Paper EBA**: 12 agosto 2016
- **Final Report EBA (draft)**: 23 febbraio 2017
- **Emendamenti CE**: 24 maggio 2017
- **Opinion EBA**: 29 giugno 2017
- **Versione definitiva CE per approvazione al Parlamento**

Sono **respinte o parzialmente accolte l**e proposte della Commissione (modifiche sostanziali e ulteriori variazioni)

--> **Applicazione da parte dei PSP**: 18 mesi dopo l'entrata in vigore degli RTS

Draft RTS on SCA and CSC
Struttura e punti principali

CERTFin
CERT Finanziario Italiano

Gli RTS sono strutturati in **6 Capitoli**:

1) **Requisiti generali**
2) **Requisiti sull'autenticazione forte del cliente**
3) **Esenzioni dalla applicazione della SCA**
4) **Confidenzialità e integrità delle credenziali di sicurezza dei PSU**
5) **Standard aperti di comunicazione comuni e sicuri**
6) **Disposizioni finali**

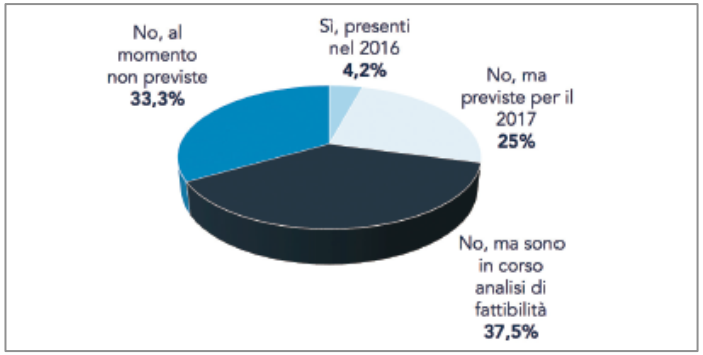
Punti principali

1. **MECCANISMI DI MONITORAGGIO DELLE TRANSAZIONI NELL'APPLICAZIONE DI SCA ED ESENZIONI** → **Capitolo 1**
2. **REGIME DI AUTENTICAZIONE FORTE DEL CLIENTE ED ESENZIONI DALL'APPLICAZIONE DELLA SCA** → **Capitoli 2 e 3**
3. **COMUNICAZIONE TRA ASPSP E PISP, AISP E PIIS** → **Capitolo 5**

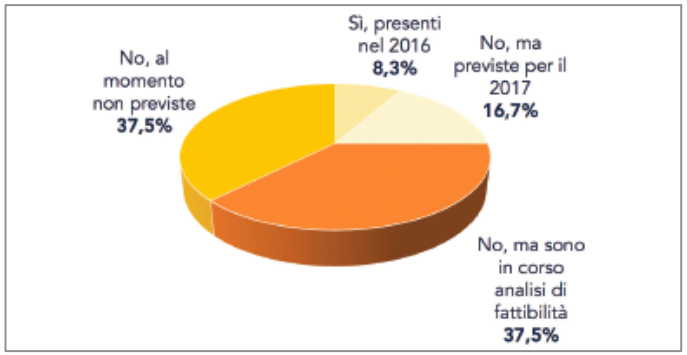
SCA, dynamic linking ed esenzioni: Punti di attenzione e opportunità

- L'evoluzione delle modalità di autenticazione forte come richiesto da EBA spinge a valutare nuove **opportunità** per rafforzare ulteriormente la sicurezza dei pagamenti e, al contempo, garantire **innovazione** e una buona **user experience**. Le banche italiane già si stanno muovendo in questa direzione.

Tecnologie di autenticazione forte con elementi in grado di **collegare dinamicamente** una transazione a uno specifico importo e a uno specifico beneficiario (segmento Retail, 24 rispondenti)



Tecnologie di autenticazione forte con elementi in grado di **collegare dinamicamente** una transazione a uno specifico importo e a uno specifico beneficiario (segmento Corporate, 24 rispondenti)



Fonte: CERTFin, Report Sicurezza, 2017

- Al contempo, rimangono **aperte** alcune **questioni** che richiederanno ulteriori **approfondimenti**, sia a livello interbancario che con l'Autorità, quali ad esempio:
  - ✓ *Dynamic linking e pagamenti massivi*
  - ✓ *SCA/Dyanmic linking e carte di pagamento*
  - ✓ *Modalità di calcolo del tasso di frode*
  - ✓ *Esemplificazione dei dati sensibili di pagamento*
  - ✓ *Gestione del transitorio (dal 13 gennaio 2018 fino all'entrata in vigore degli RTS)*

Draft RTS on SCA and CSC
Comunicazione con le Terze Parti

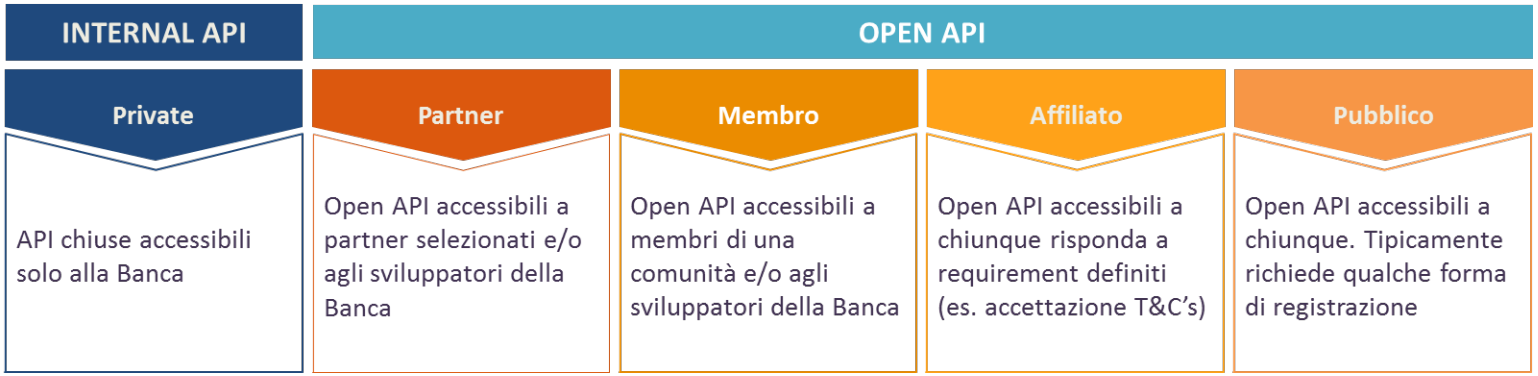
CERTFin
CERT Finanziario Italiano

- Per la **comunicazione con le TPP** (PISP, AISP e PIIS), gli ASPSP devono fornire almeno una **interfaccia** che abbia i seguenti **requisiti:**
  - **AISP**, **PISP** e **PIIS** si **identificano** all'ASPSP;
  - Gli **AISP devono poter richiedere** e ricevere **informazioni** sui **conti** e sulle **transazioni**;
  - I **PISP devono poter disporre ordini di pagamento** e **ricevere informazioni** sulla disposizione e sull'esecuzione del pagamento.
- L'interfaccia può essere "**dedicata**" oppure "**utente modificata**" (interfaccia utilizzata per la autenticazione e la comunicazione con i propri utenti).
- Gli ASPSP sono tenuti a:
  - ✓ definire specifici **indicatori di performance (KPI)**;
  - ✓ consentire agli AISP e ai PISP di «**testare**» le interfacce almeno tre mesi prima dell'applicazione degli RTS;
  - ✓ pubblicare le statistiche su disponibilità e performance dell'interfaccia impiegata.
- L'EBA verifica **l'adeguatezza delle interfacce** messe a disposizione dagli ASPSP nell'ambito della review che dovrebbe essere condotta dopo 18 mesi dall'applicazione degli RTS.
- Nel testo emendato da EBA **non è inclusa la c.d. «fallback solution»** (misure di contingency in caso di indisponibilità o inadeguatezza dell'interfaccia dedicata messa a disposizione dagli ASPSP) → il tema è attualmente in corso di **analisi da parte degli stakeholder di settore.**

Comunicazione ASPSP –TPP: Punti aperti e iniziative in corso (1/2)

CERTFin
CERT Finanziario Italiano

- La **soluzione** tecnico-operativa con cui il mercato si sta orientando per la costruzione delle interfacce di comunicazione tra ASPSP e TPP è rappresentata dalle **API**



- Sul tema delle **interfacce** il **dibattito** è ancora acceso, sia a livello **politico** nel dialogo con la CE, sia sotto il profilo **tecnico-operativo**, tra i diversi player di mercato.

- Sin dalle prime versioni degli RTS, pur non essendo chiari diversi elementi applicativi e interpretativi degli standard tecnici, alcuni Paesi si sono mossi per definire i dettagli funzionali e tecnici di un framework API, da poter applicare a livello nazionale o cross-border. Alcuni esempi:
  - BERLIN GROUP: https://www.berlin-group.org/market-consultations
  - OPEN BANKING UK: https://www.openbanking.org.uk/read-write-apis/
  - STET FR: https://www.stet.eu/en/news/news1/stet-psd2-api-is-now-available.html
  - OPEN API SK: http://docs.sbaonline.apiary.io (draft version)
  - PSD2 Polish API

Comunicazione ASPSP –TPP: Punti aperti e iniziative in corso (2/2)

CERTFin
CERT Finanziario Italiano

- Vi sono diversi **cantieri di lavoro** che sono stati attivati a livello europeo, sotto la guida di **ERPB**, a cui partecipano ASPSP, TPP, associazioni di consumatori, EPC, EBF, EBA, BCE, e che stanno affrontando alcuni **punti chiave** rispetto al tema delle **interfacce**, con l'obiettivo di definire **requisiti comuni** ed evitare la frammentazione delle soluzioni di mercato. In particolare, i temi di discussione più rilevanti, sui cui non sempre si è trovata una convergenza rispetto alle diverse posizioni espresse dagli stakeholder.

  - ***Consenso del PSU*** → a chi (via PISP o no)? In che modalità (anche alla luce del GDPR)?
  - ***Modalità e procedure di SCA*** → browser-based vs embedded vs decoupled? Alcune o tutte?
  - ***Informazioni da fornire alle TPP ("What")*** → pre-payment, account history, PISP vs AISP, etc.
  - ***Metriche e KPI delle API*** → availability, response time, peak, error time, etc.
  - ***Aspetti di sicurezza*** → da definire per mitigare il rischio di frode
  - ***Testing*** → requisiti, check list, KPI, etc.
  - **Certificati** → necessari per identificazione TPP, diverse iniziative in corso anche presso ETSI per la definizione di standard comuni
  - ***Registri*** → necessità di armonizzazione a livello EU e tra NCA (si veda CP dedicato)
  - ***Gestione contenziosi*** → necessità di processi comuni

- L'ERPB pubblicherà un **primo report** entro la **fine di novembre** e proseguirà poi i lavori nei mesi successivi, focalizzandosi soprattutto sugli aspetti tecnici e di testing.

Percorso di perfezionamento di guideline e standard tecnici

CERTFin
CERT Finanziario Italiano

	PUBBLICAZIONE DEL CONSULTATION PAPER	PUBBLICAZIONE DEL FINAL REPORT
DRAFT RTS ON SCA AND CSC	12/8/2016	
GUIDELINES ON MAJOR INCIDENT REPORTING	7/12/2016	27/07/2017
DRAFT GUIDELINES ON FRAUD REPORTING REQUIREMENTS	2/8/2017	
DRAFT GUIDELINES ON THE SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS OF PAYMENT SERVICES	5/5/2017	

Guidelines on major incident reporting
Obiettivi e struttura

CERTFin
CERT Finanziario Italiano

Background e obiettivi

Gli Orientamenti, la cui versione definitiva è stata pubblicata da EBA il **27 luglio**, hanno l'obiettivo di specificare:

- I **criteri** per la classificazione dei gravi incidenti operativi e di sicurezza;
- Il **template** che i PSP devono utilizzare per la notifica degli incidenti alle Autorità competenti;
- Gli **indicatori** che le Autorità competenti devono utilizzare nella **valutazione della gravità** degli incidenti e le informazioni minime che devono condividere con le altre Autorità nazionali.

Struttura

I **contenuti** sono distribuiti in quattro capitoli:

- *Capitolo 1* – **Istruzioni per la risposta alla consultazione**;
- *Capitolo 2* – **Executive Summary**;
- *Capitolo 3* – **Guidelines**: Orientamenti rivolti ai PSP per il reporting dei dati selle frodi (con template per la segnalazione) e alle Autorità Competenti (assessment della rilevanza dell'incidente e informazioni da condividere con altre Autorità nazionali);
- *Capitolo 4* – **Accompanying documents** (costi-benefici e feedback ricevuti nel corso della consultazione).

Guidelines on major incident reporting
Dettaglio dei contenuti

CERTFin
CERT Finanziario Italiano

- I **Gravi incidenti di sicurezza e operativi legati ai pagamenti** sono definiti da EBA come eventi, non pianificati dal PSP, che generano **impatti avversi** sulla **integrità**, **disponibilità**, **confidenzialità, autenticità** e/o **continuità** del servizio prestato.
- Un incidente è classificato come **"grave"** se, sulla base della valutazione di **7 criteri** (transazioni coinvolte, PSU coinvolti, inattività del servizio, impatto economico, elevato livello di escalation interna, ulteriori PSP/infrastrutture rilevanti potenzialmente coinvolti, impatto reputazionale), è raggiunta **almeno una** delle soglie di "**Higher Impact**" o **almeno 3** delle soglie di "**Lower Impact**".

CRITERIO	«LOWER IMPACT» LEVEL	«HIGHER IMPACT» LEVEL
Transazioni coinvolte	**Oltre il 10%** del regolare volume di transazioni *e* importo superiore a **100.000 €**.	**Oltre il 25%** del regolare volume di transazioni *o* importo superiore a **5 milioni di €.**
PSU coinvolti	**Oltre 5.000 PSU** *e* **più del 10%** dei PSU del provider.	**Oltre 50.000 PSU** *o* **più del 25%** dei PSU del provider.
Service downtime	Oltre **2 ore**.	Non applicabile.
Impatto economico	Non applicabile.	**Superiore al massimo tra lo 0,1%** del **Common Equity Tier 1** e **200.000 €** *o* **oltre 5 milioni di €**.
Elevata escalation interna	Si	**Si**, con conseguente probabile attivazione dello **stato di crisi**.
Altri PSP/ infrastr. rilevanti potenzialmente coinvolti	Si	Non applicabile.
Impatto reputazionale	Si	Non applicabile.

Guidelines on major incident reporting
Template di reporting

CERTFin
CERT Finanziario Italiano

- Per supportare i PSP nel reporting dei major incident, l'EBA ha fornito un **template** strutturato per contenere **3 tipologie di report** incrementali, da inviare durante il ciclo di vita dell'incidente:

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last Intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date: DD/MM/YYYY — Time: HH:MM
Incident identification number, if applicable (for interim and final reports):

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual ☐ Consolidated				
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by [1]		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident		
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM	
Incident status	☐ Diagnostics ☐ Repair	☐ Recovery ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM	

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected ☐ Actual figure ☐ Estimation As a % of regular number of transactions ☐ Actual figure ☐ Estimation Value of transactions affected in EUR ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected ☐ Actual figure ☐ Estimation As a % of total payment service users ☐ Actual figure ☐ Estimation
Service downtime [4]	Total service downtime DD:HH:MM ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR ☐ Actual figure ☐ Estimation Indirect costs in EUR ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack → Type of attack: ☐ Distributed Denial of Service (DDoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other ☐ If Other, specify ☐ Internal attack ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other ☐ If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly — If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building/s affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ E-banking ☐ Telephone banking ☐ Mobile banking ☐ ATMs ☐ Point of sale ☐ Other If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation services ☐ Account information services ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Communication ☐ Clearing ☐ Direct settlement ☐ Indirect settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Database ☐ Hardware ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report

If no Intermediate report has been sent, please also complete section B

C 1 - GENERAL DETAILS

Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root causes analysis - lessons learnt - additional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place? If so, please explain	☐ YES ☐ NO

C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP

What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	

C 3 - ADDITIONAL INFORMATION

Has the incident been shared with other PSPs for information purposes? If so, please provide details	☐ YES ☐ NO
Has any legal action been taken against the PSP? If so, please provide details	☐ YES ☐ NO

Guidelines on major incident reporting
Contenuto e tempistiche di invio del reporting

CERTFin
CERT Finanziario Italiano

A) Report iniziale:

- Contenuto: **informazioni generali** sull'incidente e conseguenze attese
- Tempistiche di invio: entro **4 ore** dalla rilevazione dell'incidente grave

B) Uno o più Report intermedi:

- Contenuto: contengono gli **aggiornamenti** rilevanti sull'incidente
- Tempistiche di invio: entro **3 giorni** lavorativi dal precedente report

- Il primo report intermedio contiene le informazioni di **maggiore dettaglio** sull'incidente
- L'ultimo report intermedio è inviato quando viene ristabilita la **normale operatività**
- Se l'**operatività** è ristabilita entro **4 ore** dalla rilevazione dell'incidente grave, report iniziale e intermedio sono **inviati contestualmente**

C) Report finale:

- Contenuto: inviato al termine dell'**analisi di *root cause*** dell'incidente con i dati effettivi
- Tempistiche di invio: entro **2 settimane** dalla ripresa della normale operatività

L'invio di un report finale è previsto anche in caso di incidente **riclassificato come non grave**

Guidelines on major incident reporting
Opportunità e punti di attenzione

CERTFin
CERT Finanziario Italiano

- Gli **incidenti** potrebbero essere **contrastati più efficacemente se l'informazione di tali eventi** segnalata dal PSP alle Autorità competenti fosse sotto vincolo di confidenzialità, elaborata e anonimizzata (ad esempio attraverso i CERT) per essere **veicolata anche ad altri PSP** per:
  1) approntare difese preventive
  2) circoscrivere gli effetti per gli utenti

Il CERTFin può svolgere un ruolo di supporto attivo nel contesto nazionale.

- È importante **chiarire il quadro legale degli Orientamenti rispetto alla normativa prudenziale in vigore negli Stati membri** in materia di classificazione e segnalazione degli incidenti e sicurezza dei pagamenti via internet

È opportuno che le disposizioni contenute negli Orientamenti siano integrate all'interno del più ampio processo di gestione della sicurezza previsto dalla Regolamentazione.

- La **disomogeneità nelle modalità di trattamento** (report, scadenze e tempistiche differenti) dovuta ai requisiti di norme diverse (PSD2, GDPR, NIS) **comporta duplicazioni** e più **possibilità di confusione ed errori** da parte dei PSP

Una semplificazione delle procedure e delle tempistiche di reporting sarebbe molto apprezzata dal mercato.

La complessità dei requisiti regolamentari di reporting…non solo PSD2

CERTFin
CERT Finanziario Italiano

	OGGETTO	CONTENUTO	TEMPISTICHE E STRUTTURA
GUIDELINES ON MAJOR INCIDENT REPORTING	**Gravi incidenti di sicurezza** e **operativi** legati ai **pagamenti.**	Template con **3 tipologie di report incrementali** (iniziale, intermedi, finale), con **campi obbligatori**.	**Report iniziale**: entro **4 ore** dalla rilevazione **Uno o più report intermedi**: entro **3 giorni lavorativi** dal precedente **Report finale**: **entro 2 settimane** dalla ripresa della normale operatività.
FRAMEWORK BdI - SSM ISTITUTI SIGNIFICANT	**Gravi incidenti di sicurezza informatica.**	Template con **3 tipologie di report incrementali** (primo report, report ad interim, report finale), con **campi obbligatori**.	**Report iniziale**: entro **2 ore** dal momento in cui l'incidente è stato classificato grave **Report intermedio**: entro **10 giorni lavorativi** dal primo **Report finale**: entro **20 giorni lavorativi** dal report intermedio.
FRAMEWORK BdI ISTITUTI LESS SIGNIFICANT	**Gravi incidenti di sicurezza informatica.**	**Un report** suddiviso in **5 aree tematiche**, con alcuni **campi obbligatori**.	La segnalazione deve avvenire con la **dovuta tempestività** e sulla base del **format** previsto.
GDPR	**Violazioni di dati personali** che comportano un **rischio per i diritti e le libertà delle persone fisiche**.	**Non** è disponibile un **template**. Sono specificate alcune **informazioni minime** per la segnalazione all'Autorità e all'interessato.	L'invio deve avvenire **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore** dal momento in cui il Titolare ne è venuto a conoscenza.
DIRETTIVA NIS	**Incidenti di sicurezza** con **impatto rilevante sulla continuità** dei servizi prestati.	**Non è presente un template**. Sono in corso di formalizzazione **Orientamenti** specifici da parte del Gruppo di Cooperazione.	La segnalazione deve essere inviata **senza ingiustificato ritardo**.

Percorso di perfezionamento di guideline e standard tecnici

CERTFin
CERT Finanziario Italiano

	PUBBLICAZIONE DEL CONSULTATION PAPER	PUBBLICAZIONE DEL FINAL REPORT
DRAFT RTS ON SCA AND CSC	12/8/2016	
GUIDELINES ON MAJOR INCIDENT REPORTING	7/12/2016	27/07/2017
DRAFT GUIDELINES ON FRAUD REPORTING REQUIREMENTS	2/8/2017	
DRAFT GUIDELINES ON THE SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS OF PAYMENT SERVICES	5/5/2017	

Draft guidelines on fraud reporting requirements – Obiettivi e struttura

CERTFin
CERT Finanziario Italiano

- Con l'obiettivo di aumentare la **comparabilità** e l'**affidabilità** dei dati sulle frodi, l'EBA ha formulato il proprio CP in merito agli **Orientamenti** sulla segnalazione delle transazioni fraudolente.

- Il CP è strutturato in **6 capitoli** e contiene **10 Guideline** dirette a:
  - ✓ i **PSP**, per la segnalazione alle Autorità competenti (dalla 1 alla 7);
  - ✓ le **Autorità nazionali**, per l'invio dei dati aggregati all'EBA e all'ECB (dalla 8 alla 10).

GL #	TITOLO
GL 1	General and Fraudulent Payment Transaction
GL 2	General Data Requirements
GL 3	Frequency and reporting timelines
GL 4	Geographical breakdown
GL 5	Reporting to competent authority
GL 6	Recording/Reference dates
GL 7	Data breakdown
GL 8	Fraudolent Payment Transaction
GL 9	Data collection and aggregation
GL 10	Data reporting

Tra gli <u>obiettivi specifici per i PSP</u>, sono inclusi:

- ✓ Confrontare le proprie **capacità di mitigazione** e **prevenzione** delle frodi
- ✓ Includere dati sulle frodi nel processo di **valutazione** e **monitoring** dei rischi
- ✓ Identificare **proattivamente** trend di frodi

- EBA ha formulato nel CP **9 quesiti** per raccogliere il punto di vista dei diversi stakeholder in relazione a specifici punti ritenuti più critici/rilevanti.

Draft guidelines on fraud reporting requirements – Dettaglio sui contenuti (1/2)

- In base al framework EBA – BCE, la segnalazione contiene i dati su:

a) **Transazioni di pagamento fraudolente «gross»**: equivalgono alle transazioni di pagamento fraudolente complessive, a prescindere dal fatto che l'importo sia stato recuperato o meno;

b) **Transazioni di pagamento fraudolente «net»**, corrispondenti alle transazioni «gross» al netto delle perdite che il PSP che genera il report recupera da qualunque soggetto.

«Transazioni di pagamento fraudolente»: sono le operazioni che:

- ✓ non sono **autorizzate** (perdita, furto o appropriazione indebita di dati di pagamento sensibili o strumenti di pagamento);
- ✓ attengono a transazioni eseguite o autorizzate da un **pagatore** che ha agito in modo **disonesto** o **ingannevole**;
- ✓ sono effettuate mediante **manipolazione del pagatore**.

Draft guidelines on fraud reporting requirements – Dettaglio sui contenuti (2/2)

CERTFin
CERT Finanziario Italiano

- I dati oggetto di segnalazione sono organizzati in «***data breakdown***», definiti sulla base di **quattro criteri**: 1) il **punto** della catena di pagamento in cui è avvenuta la **frode**; 2) il **metodo di autenticazione**; 3) il **canale di pagamento**; 4) la **modalità** con cui il frodatore è entrato in **possesso** dei dati sensibili di pagamento.
- Per aumentare la completezza e l'esaustività dei dati sulle frodi, sono identificati **sette data breakdown**, distinguendo in base alla tipologia di **servizio** e **strumento** di pagamento:

1. **E-money**
2. **Money remittance**
3. **Payment initiation**
4. **Credit transfer**
5. **Direct debit**
6. **Issuing di carte di pagamento**
7. **Acquiring di carte di pagamento**

- I dati sono riportati:
  - ✓ sia in **volume** che in **importo;**
  - ✓ con riferimento sia alle operazioni di pagamento **complessive** che a quelle **fraudolente**;
- Ciascun PSP potrebbe dover fornire dati relativi a **più di uno strumento** o **servizio** di pagamento.

Frequenza del reporting e tempistiche per l'invio alle Autorità competenti

A. Reporting trimestrale, costituito da dati di più alto livello → da inviare a partire da **H2 2018**, con riferimento al secondo trimestre dell'anno in quanto primo trimestre completo dall'entrata in vigore della PSD2 (13/1/2018)

B. Reporting annuale, contenente i dati di dettaglio → da inviare a partire da **H1 2020**, tenendo conto dell'entrata in vigore degli RTS

Il punto di vista delle banche rispetto ai quesiti proposti

CERTFin
CERT Finanziario Italiano

- A valle del processo di consultazione terminato lo scorso 3 novembre, è stato formulato il paper di risposta di settore evidenziando principali **criticità e punti di attenzione**:

1. I PSP **sono già soggetti** ai requisiti di reporting dei dati sulle frodi verso le Autorità nazionali ed europee → Si ritiene necessario un coordinamento e una maggiore semplificazione;
2. Si ritiene opportuno **ridurre la quantità di informazioni** contenute nel reporting;
3. Per **evitare disomogenietà**, è auspicabile che vengano inserite **timeline e procedure specifiche** per l'invio delle segnalazioni, anche per ridurre il rischio che PSP operanti in più di uno Stato membro debbano implementare diversi framework, con possibili inefficienze;
4. La **frequenza trimestrale** potrebbe essere **eccessivamente gravosa** per gli operatori in termini di risorse e impatto organizzativo;
5. É necessario **allineare** la **terminologia** relativa alle **frodi** e agli **strumenti di pagamento** con la proposta di direttiva del Parlamento Europeo e del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dal contante;
6. Si è **contrari all'esenzione dal reporting trimestrale** prevista per gli istituti di pagamento e di e-money di dimensioni ridotte → i frodatori potrebbero concentrarsi proprio su tali organizzazioni meno impattate;
7. Si ritiene che la timeline implementativa prevista per il 2018 non sia compatibile con la raccolta delle informazioni necessarie per il reporting → si richiede di posticiparne la **data di applicazione**, **collegandola a quella degli RTS su SCA e CSC** (presumibilmente metà 2019).

Fraud reporting…cosa esiste già e quali opportunità

CERTFin
CERT Finanziario Italiano

- Nell'ambito delle attività di ricerca ABI Lab (e più recentemente con il CERTFin) è stata nel corso degli anni consolidata una modalità di raccolta delle **frodi via Internet e Mobile Banking** che ha consentito di **investigare il fenomeno e rappresentare le azioni di contrasto e prevenzione**.
- Alla luce del framework definito da EBA, sono in corso **analisi e approfondimenti** per apportare eventuali modifiche e identificare **possibili evoluzioni** nella struttura del questionario, già nel 2017.

Argomento	Orientamenti EBA	Survey di settore
TIPOLOGIA TRANSAZIONI	**E-money**, **money remittance**, **payment initiation**, **credit transfer**, **direct debit**, **issuing carte di pagamento**, **aquiring carte di pagamento**	**Bonifico Estero** (SEPA e non SEPA), **bonifico Italia stessa banca** (SEPA), **bonifico Italia altra banca** (SEPA), **ricariche telefoniche**, **ricariche carta prepagata**
TENTATIVI DI FRODE	**Non considerati**	**Considerati**
GEO-LOCALIZZAZIONE	**Presente** (dettaglio maggiore)	**Presente** (dettaglio minore)
DISTINZIONE RETAIL E CORPORATE	**Non presente**	**Presente**
DISTINZIONE PER CANALE	**Non presente**	**Presente**
TRANSAZIONI REMOTE E NON REMOTE	**Presente**	**Non presente** (dettaglio solo per pagamenti remoti)
SCA / NON SCA e MOTIVI ALLA BASE DELLE SCELTA	**Presente** (dettaglio maggiore)	**Assente** (dettaglio solo per soluzioni)
MECCANISMI DI ATTACCO	**Non presenti**	**Presenti**
ATTIVITÀ DI CONTRASTO E PREVENZIONE	**Non presenti**	**Presenti**

Percorso di perfezionamento di guideline e standard tecnici

CERTFin
CERT Finanziario Italiano

	PUBBLICAZIONE DEL CONSULTATION PAPER	PUBBLICAZIONE DEL FINAL REPORT
DRAFT RTS ON SCA AND CSC	12/8/2016	
GUIDELINES ON MAJOR INCIDENT REPORTING	7/12/2016	27/07/2017
DRAFT GUIDELINES ON FRAUD REPORTING REQUIREMENTS	2/8/2017	
DRAFT GUIDELINES ON THE SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS OF PAYMENT SERVICES	5/5/2017	

Draft guidelines on the security measures for operational and security risks of payment services – Obiettivi e contenuti

CERTFin
CERT Finanziario Italiano

Il CP EBA definisce la bozza di Guideline relative al «**quadro di misure di mitigazione e meccanismi di controllo per gestire i rischi operativi e di sicurezza**» che i prestatori di servizi di pagamento (PSP) sono tenuti ad adottare.

Governance	Definizione di un **framework di governo dei rischi operativi e di sicurezza** integrato nel complessivo processo di risk management.
Valutazione dei rischi	Identificazione di **funzioni di business e asset informativi critici** da proteggere contro i rischi operativi e di sicurezza, secondo una logica di **prioritizzazione.**
Protezione	Adozione di **controlli di sicurezza efficaci** a tutela della **confidenzialità**, **integrità** e **disponibilità** degli asset.
Detection	Dotazione di **misure e processi per il monitoraggio di minacce e incidenti** e definizione di **procedure di reporting.**
Continuità operativa	Dotazione di **capabilities e misure** in grado di far fronte a un ampio range di scenari di rischio.
Testing delle misure di sicurezza	Definizione delle **aree** che dovrebbero essere incluse nel **framework di testing**, i cui risultati dovrebbero servire per **migliorare** il framework generale di gestione dei rischi.
Situational awareness e formazione continua	Accrescimento della situational awareness e della capacità di monitorare i trend delle minacce in modo da identificare e reagire al meglio a scenari di rischio non preventivati.
Gestione dei rapporti con i PSU	Adozione di misure volte ad aumentare la **consapevolezza dei PSU** sui rischi di sicurezza sui pagamenti e a definire i canali di comunicazione più adeguati.

Il punto di vista delle banche rispetto ai quesiti proposti

CERTFin
CERT Finanziario Italiano

- Il position paper elaborato a livello di settore ha messo in evidenza principalmente i seguenti aspetti:

1. **Rischio di sovrapposizione** tra normative focalizzate su aspetti differenti della prestazione dei servizi di pagamento, con possibili incoerenze nel quadro regolamentare;
2. Si ritiene che gli Orientamenti debbano essere in linea con i più accreditati **standard internazionali sulla continuità operativa** (p.e. ISO-22301, ISO-22313, ISO-22317);
3. Si concorda con EBA sulla necessità di **aumentare la consapevolezza da parte del cliente delle minacce e delle vulnerabilità**, che autonomamente può individuare e limitare rischi nella fruizione dei servizi di pagamento;
4. Si ritiene che l'**attivazione di un servizio di alerting** nel continuo possa essere **eccessiva** nei confronti del cliente stesso → si potrebbe ottenere l'effetto contrario della informazione continua, generando confusione nel PSU;
5. La **notifica delle minacce potenziali di sicurezza**, come richiesto dal regolatore, si ritiene **poco adatta** perché potrebbe ingenerare reazioni sproporzionate nella clientela, sfiducia nei sistemi di pagamento online e provocare un danno reputazionale ed economico al PSP.

Timeline implementativa delle regole di attuazione della PSD2 con impatti sulla sicurezza

CERTFin
CERT Finanziario Italiano

2016 2017 Today 2018 2019 2020

⚠ Gli ASPSP devono rendere disponibili le interfacce per i test **almeno 3 mesi prima** rispetto all'applicazione degli RTS

RTS ON SCA AND CSC

Pubblicazione versione intermedia

12/8/2016 23/2/2017 TBD TBD TBD TBD

Gli RTS saranno applicati **18 mesi dopo l'entrata in vigore**

GUIDELINES ON MAJOR INCIDENT REPORTING

7/12/2016 27/7/2017 13/1/2018 TBD

GUIDELINES ON FRAUD REPORTING REQUIREMENTS

2/8/2017 TBD 13/1/2018 TBD

GUIDELINES ON THE SECURITY MEASURES FOR OPERATIONAL AND SECURITY RISKS OF PAYMENT SERVICES

5/5/2017 TBD 13/1/2018 TBD

Pubblicazione CP · Pubblicazione Final Report · Entrata in vigore · Applicazione