BANCA D'ITALIA
EUROSISTEMA

Normativa EBA: la Strong Customer Authentication (SCA)

Ravenio Parrini

Servizio Supervisione sui mercati e sul sistema dei pagamenti

Le regole europee in tema di pagamenti e gli effetti sulle imprese

Confindustria, Viale Astronomia 30

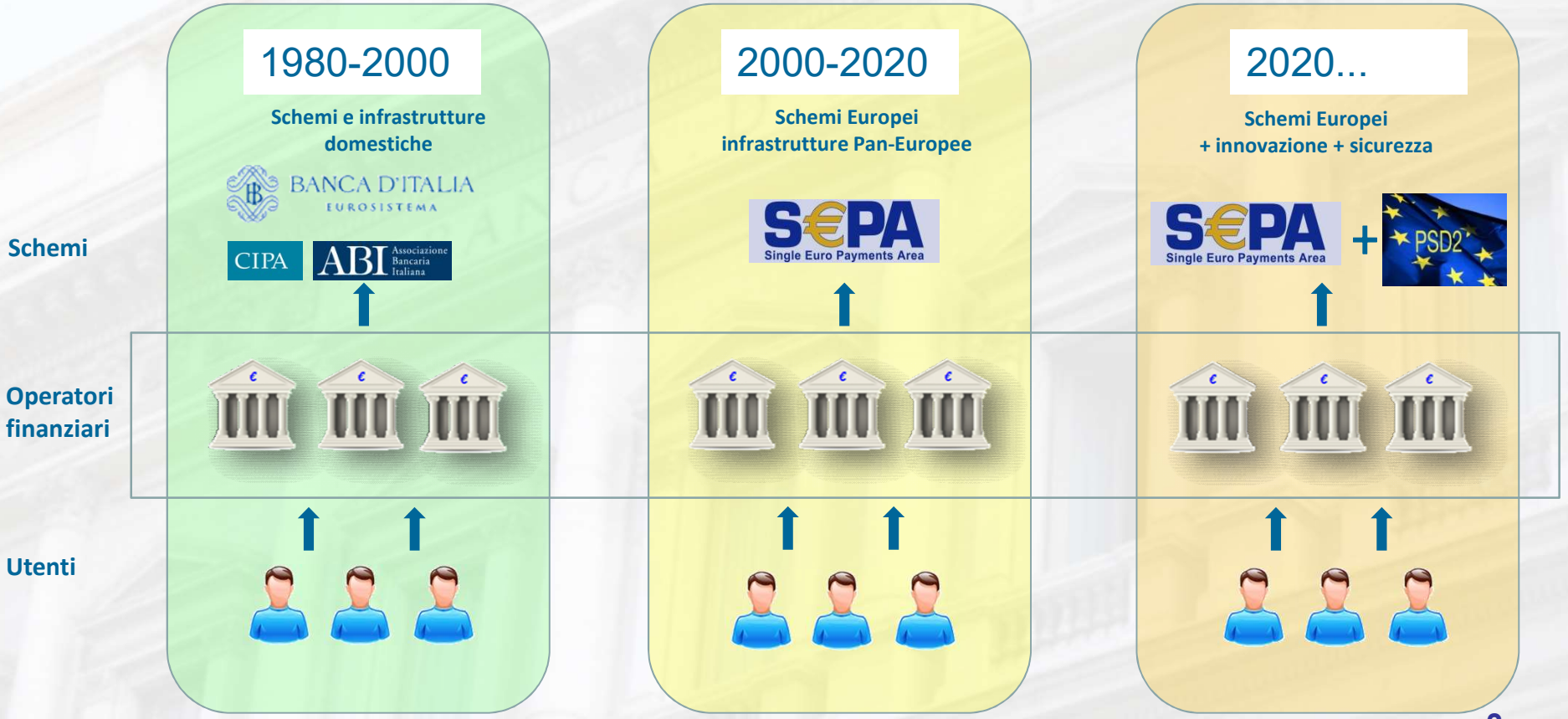
(Roma, 10 luglio 2019)

BANCA D'ITALIA
EUROSISTEMA

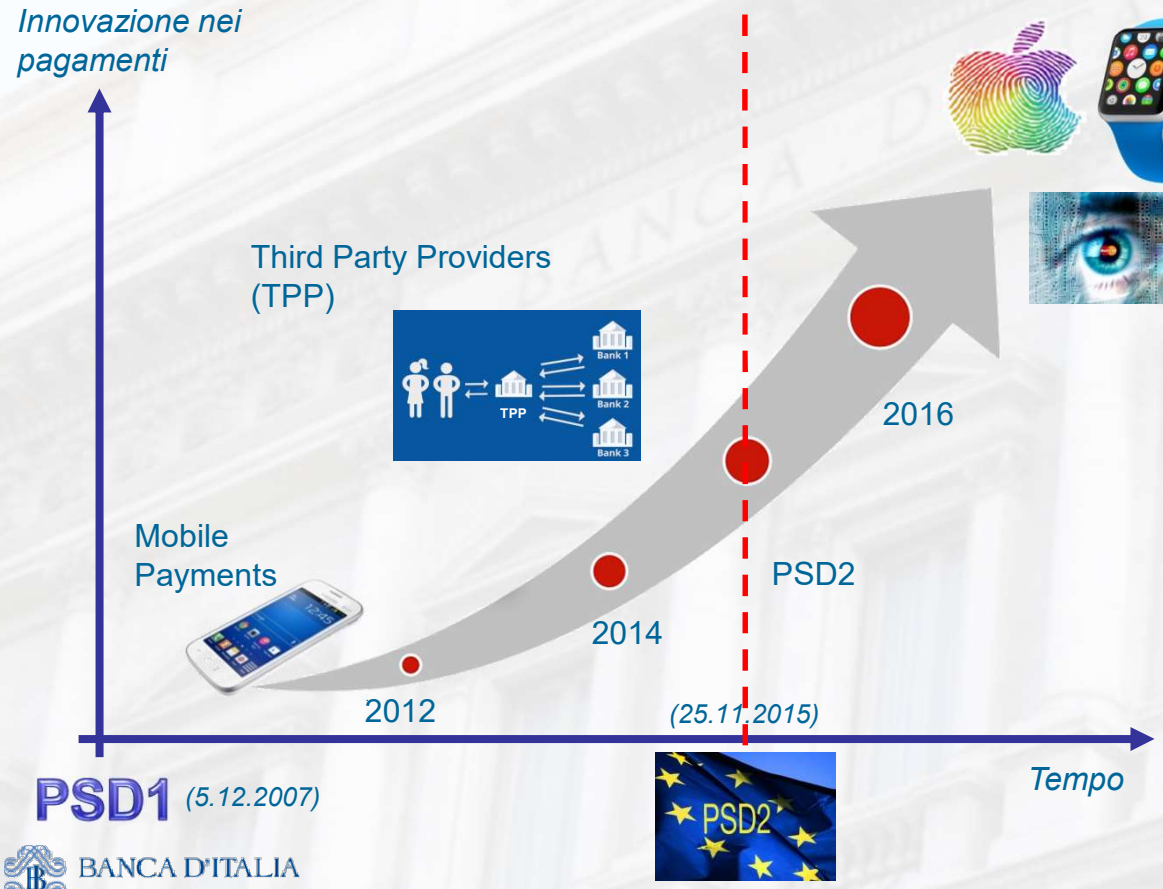
AGENDA

- Profili evolutivi
- Caratteristiche della Autenticazione Forte (SCA)
- Adeguamento degli operatori
- Q&A

Evoluzione ecosistema pagamenti



Il contesto: PSD2 e Innovazione



Instant, Biometria, Werable.

La PSD2 tiene conto della evoluzione tecnologica e dei nuovi intermediari agendo su piani distinti:

1. *regolamenta i nuovi intermediari e i nuovi servizi,*
2. *introduce dei livelli di sicurezza più elevati e armonizzati su tutti i canali (POS/ATM, Web, Mobile APP)*

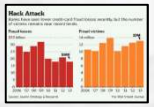
BANCA D'ITALIA
EUROSISTEMA

Normativa secondaria dell'EBA

- La PSD2 fissa dei principi di sicurezza generali, in particolare per contrasto alle frodi (tra gli obiettivi della PSD2);
- L'EBA ha poi codificato tali principi in norme secondarie di maggior dettaglio (in termini di *prevenzione*, *reazione*, *revisione*). In particolare i *Regulatory Technical Standards (RTS)* riguardano la autenticazione forte del cliente (SCA).

NORMATIVA EBA	LINK sito EBA
EBA RTS on strong customer authentication and secure communication under PSD2	https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2
EBA GL on major incidents reporting under PSD2	https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2
EBA GL on fraud reporting under PSD2	https://eba.europa.eu/-/eba-publishes-final-guidelines-on-fraud-reporting-under-psd2
EBA GL on security measures for operational and security risks under the PSD2	https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2






BANCA D'ITALIA
EUROSISTEMA

AGENDA

- Profili evolutivi
- Caratteristiche della Autenticazione Forte (SCA)
- Adeguamento degli operatori
- Q&A

Autenticazione forte = 2 fattori + codice dinamico

L'identità dell'utente deve essere verificata attraverso l'utilizzo di almeno due tra i seguenti elementi:

- ***CONOSCENZA***: qualcosa che solo l'utente può conoscere (PIN, password, domanda di sicurezza, ecc)
- ***POSSESSO***: qualcosa che l'utente possiede (token bancario, wearable device, telefono, etc).
- ***INERENZA***: qualcosa che l'utente è (identificazione biometrica)

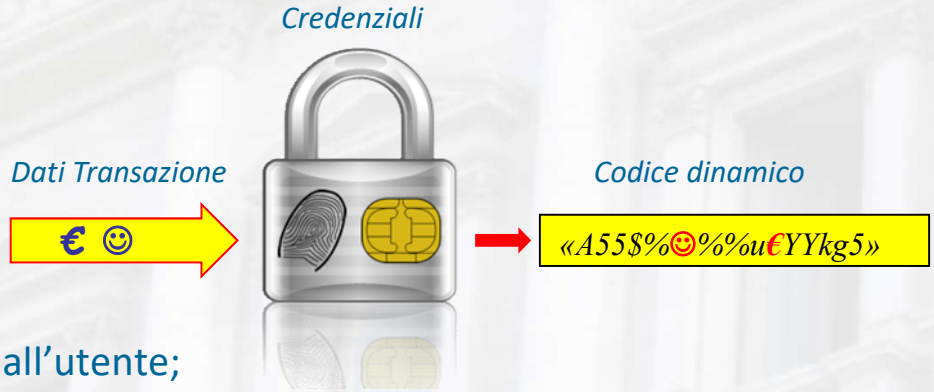
... dall'uso di tali elementi deve essere generato un ***codice dinamico*** *(csd. Authetication Code)* da sottoporre alla verifica della banca emittente.

➔ il ***codice dinamico*** consente la autenticazione a distanza del cliente limitando l'esposizione delle credenziali «personali e segrete» dello stesso.

Pagamenti via Internet: Il *Dynamic Linking*

Per i pagamenti da «remoto» o a distanza, cioè avviati attraverso una rete di comunicazione a distanza, la PSD2 prevede un presidio di sicurezza rafforzato, detto **Dynamic Linking:**

Il *codice di autenticazione dinamico univoco deve essere legato indissolubilmente ai parametri della transazione (ammontare e beneficiario) per tutte le transazioni effettuate su Internet e dal cellulare.*

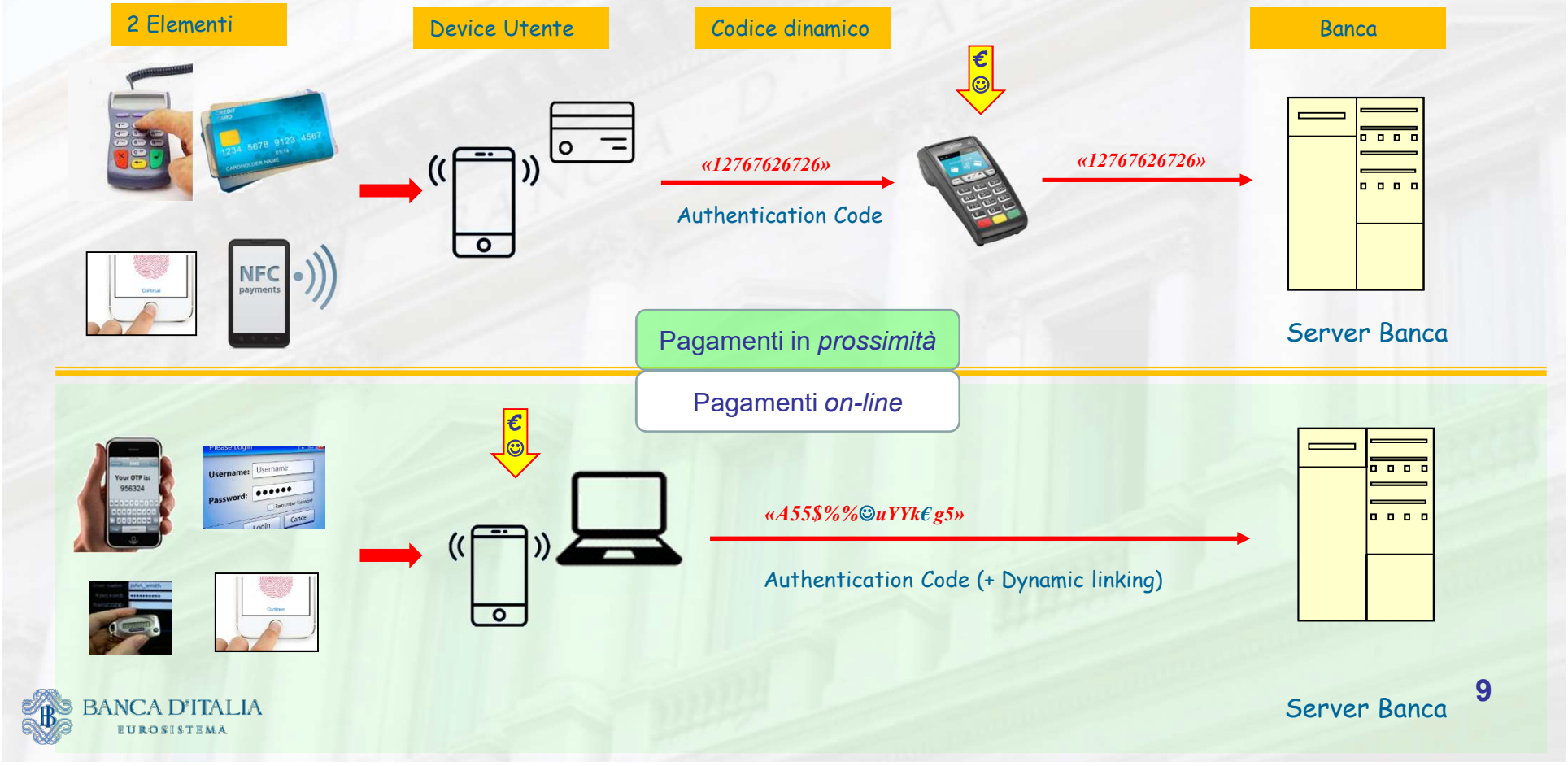


➔ meccanismo invisibile all'utente;

➔ studiato per supportare due obiettivi principali:

1. *migliorare il **contrasto alle frodi** su Internet (WEB, APP);*
2. *consentire la **esposizione delle credenziali** utente alle terze parti (AISP, PISP) senza rischio.*

SCA e Authentication Code

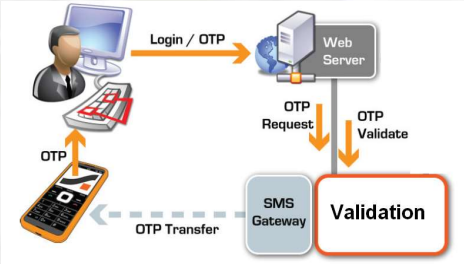


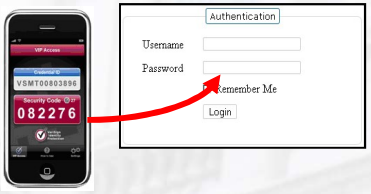
Esempi di soluzioni SCA per Internet

Gli Elementi/Credenziali sono *in genere* oggetti:

- ✓ forniti dal PSP;
- ✓ collegati/collegabili o meno al device di pagamento;
- ✓ associati in maniera biunivoca al cliente;
- ✓ nella piena disponibilità e controllo del cliente.

Possono anche essere oggetti del cliente che lo stesso registra presso il PSP per le procedure di autenticazione (es: smartphone, password).





BANCA D'ITALIA
EUROSISTEMA

Esenzioni dalla SCA

Per transazioni a basso rischio, al ricorrere di determinate condizioni:

- accesso solo informativo (per 90gg);
- pagamenti C-less al POS (<50 euro);
- POS trasporti e parcheggi;
- pagamenti ricorrenti/beneficiari noti;
- giroconti;
- pagamenti *corporate;*
- pagamenti *remoti* (<30 euro);
- pagamenti remoti con *analisi rischio (antifrode)* in tempo reale (<500 euro)



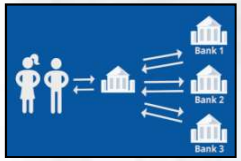


SCA si completa con *Sistemi Antifrode*

Data di implementazione degli EBA RTS

In seguito alle nuove previsioni normative, gli operatori finanziari sono chiamati entro il **14 settembre 2019** a:

- implementare procedure di **autenticazione forte** del cliente con codici dinamici;
- adeguare la **protezione credenziali** del cliente e i dati sensibili ai fini delle frodi;
- implementare **sistemi antifrode** in grado di rilevare transazioni illecite;
- aprire i conti dei clienti alle **Terze Parti Autorizzate** (TPP).



... in aggiunta ai requisiti già pubblicati con specifiche EBA GL:

- ✓ Incident Reporting
- ✓ Fraud Reporting
- ✓ Operational Security

AGENDA

- Profili evolutivi
- Caratteristiche della Autenticazione Forte (SCA)
- Adeguamento degli operatori
- Q&A

Pagamenti con carta per e-commerce

Esempi elementi SCA:

- ***Conoscenza***: Password/PIN, *ma non i dati della carta (PAN, scad, CVV);*
- ***Possesso***: telefono con SMS o APP registrata,...;
- ***Inerenza***: impronta, voce, retina,..

+ Attivazione Dynamic Linking

Esenzioni SCA sotto 30 euro o fino a 500 euro con antifrode in tempo reale

Pagamenti preautorizzati (addebito in carta di utenze o pagamenti rateali) non richiedono la SCA

Adeguamento procedure:

- applicazioni banche;
- credenziali utente (SMS-OTP);
- siti Web di e-commerce;
- Mobile APP.

Recente Opinion dell'EBA: minima flessibilità nell'adeguamento alla SCA sotto il controllo della Autorità Nazionale.

Adeguamento esenzioni:

- Pagamenti «*single-click*».

Pagamenti con Internet/Mobile Banking

Esempi elementi SCA:

- ***Conoscenza***: Password/PIN,...
- ***Possesso***: telefono con SMS o APP registrata, token hardware, ma no matrice di password;
- ***Inerenza***: impronte digitali

+ Attivazione Dynamic Linking

Esenzioni SCA sotto 30 euro o fino a 500 euro con antifrode in tempo reale

Esenzioni particolari (white-list, ricorrenti, giroconti, corporate)

Pagamenti preautorizzati (addebito in conto- SDD) non richiedono la SCA

Adeguamento procedure:

- applicazioni banche;
- credenziali utente (Token);
- credenziali adatte alle Terze parti (PISP/AISP).

Adeguamento esenzioni:

- pagamenti di basso importo;
- procedure pagamenti *corporate* sottoposte ad approvazione autorità competente.

Pagamenti al terminale POS

Esempi elementi SCA:

- ***Conoscenza***: Password/PIN,...
- ***Possesso***: carta a chip, cless, telefono con APP registrata,
- ***Inerenza***: fingerprint sullo smartphone, *firma autografa;*

+ Attivazione codice dinamico

Esenzioni SCA per carte cless sotto a 50 euro (150 cumulati/5 trans.);

Esenzioni carte a chip per parcheggi, trasporti)

Adeguamento procedure:

- EBA sta valutando la adeguatezza della firma autografa;
- eventuali carte statiche;

Adeguamento esenzioni:

- gestione contatori carte cless;
- eventuale aggiornamento dei *Mobile Wallet.*

L’impegno dei vari attori...

Riepilogando, PSD2 e normativa EBA in tema di sicurezza, richiedono un impegno a tutti gli attori. In particolare:

- ***Banche e intermediari finanziari***: nuove procedure e applicazioni per la gestione di credenziali e strumenti del cliente (*doppio fattore, Mobile APP, biometria, adeguamento carte..*).
- ***Utenti***: distribuzione delle nuove credenziali a milioni di utenti, installazione APP, informativa, formazione sui nuovi strumenti, nuove abitudini.
- ***Merchant***: revisione delle procedure nella fase di check-out, gestione delle esenzioni.
- ***Autorità di Vigilanza/Sorveglianza***: revisione delle prassi operative, nuovi controlli, nuovi skill, complesso sistema di reporting in tema di frodi/incidenti, gestione esenzioni specifiche.

PSD2 QA: il tool dell'EBA

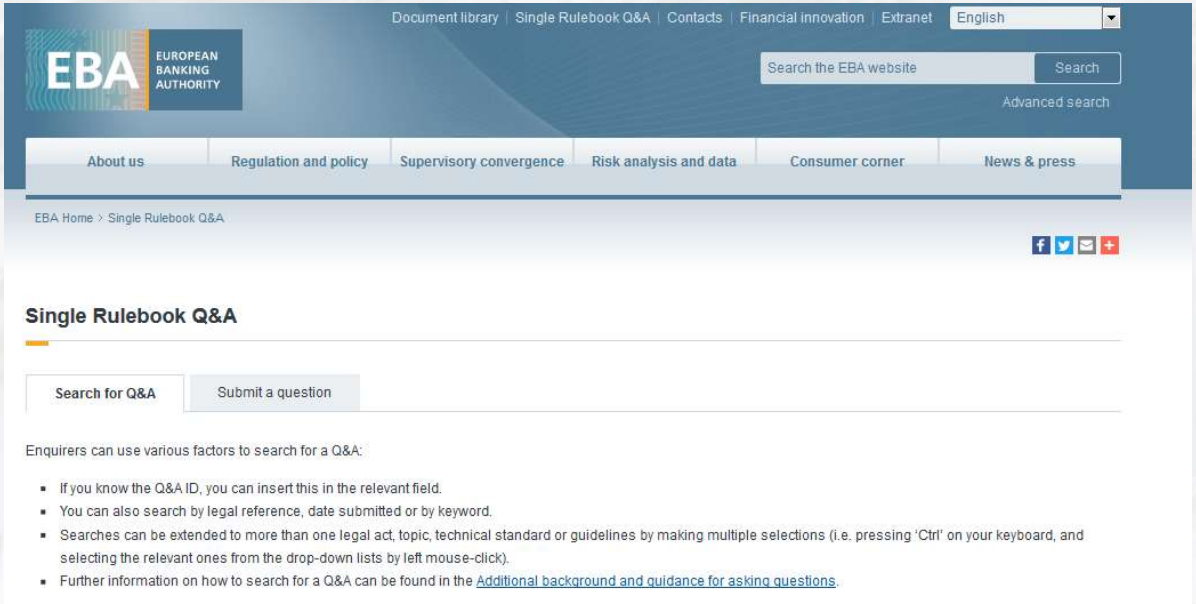
- Una serie di FAQ di tipo giuridico e tecnico sono disponibili sul sito dell'EBA sul tema PSD2, API, SCA, etc...

- Qualsiasi soggetto (banca, impresa, persona fisica,..) può inviare specifiche domande al tool compilando un form (risposta in 2-3 mesi).

- Link:

  https://eba.europa.eu/

  ➔Single Rulebook Q&A ➔ PSD2



Any questions?

Thank you!

Ravenio Parrini

ravenio.parrini@bancaditalia.it

Tel. +39 06 4792 5032

BANCA D'ITALIA
EUROSISTEMA