MOBEY FORUM
PSD2 RTS – Friend or Foe?
Webinar September 30 2016

MOBEY FORUM PSD2 webinar

- Introduction
- Brief overview of what PSD2 regulates
- Status and timeline
- Regulatory technical standards for strong customer authentication and secure communication – friend or foe?

MOBEY FORUM PSD2 webinar

Todays speaker:

Kasper Sylvest
Head of Financial Market Infrastructures, Danske Bank

Board member of Mobey Forum
Co-chair predictive analytics working group, Mobey Forum
Vice-chair the of Mobile Proxy Forum
Payment Systems Market Expert Group, European Commission
Open Banking Working Group, European Banking Association

From PSD1 to PSD2

The original purpose of the PSD (implementation November 2009)

- To facilitate development of SEPA
- To introduce a new licensing regime to encourage non-banks (payment institutions) to enter the payments market
- To set common standards for terms and conditions and increase transparency
- To establish maximum execution times for payments within EU in EU currencies
- To encourage adoption of more efficient payment types
- To improve consumer protection

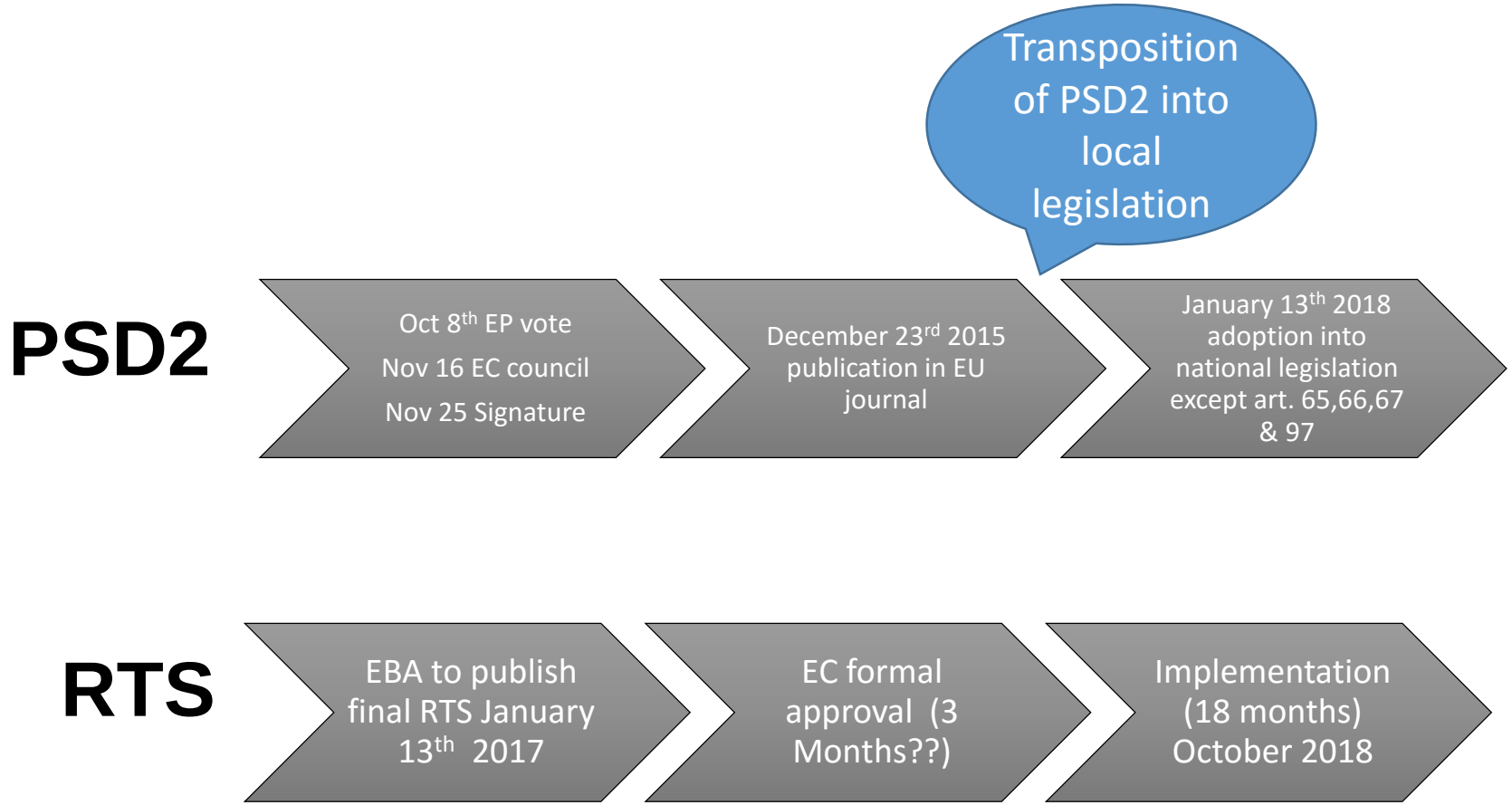
The purpose of PSD2

- To support better integration and a more competitive payment market
- To define conditions of access to the information on the availability of funds for third party providers (TPP), including payment initiation services
- To harmonise the Member States policies on surcharging in line with the regulatory decisions on interchange fees
- To adjust the scope and improve the consistency of the legislative framework

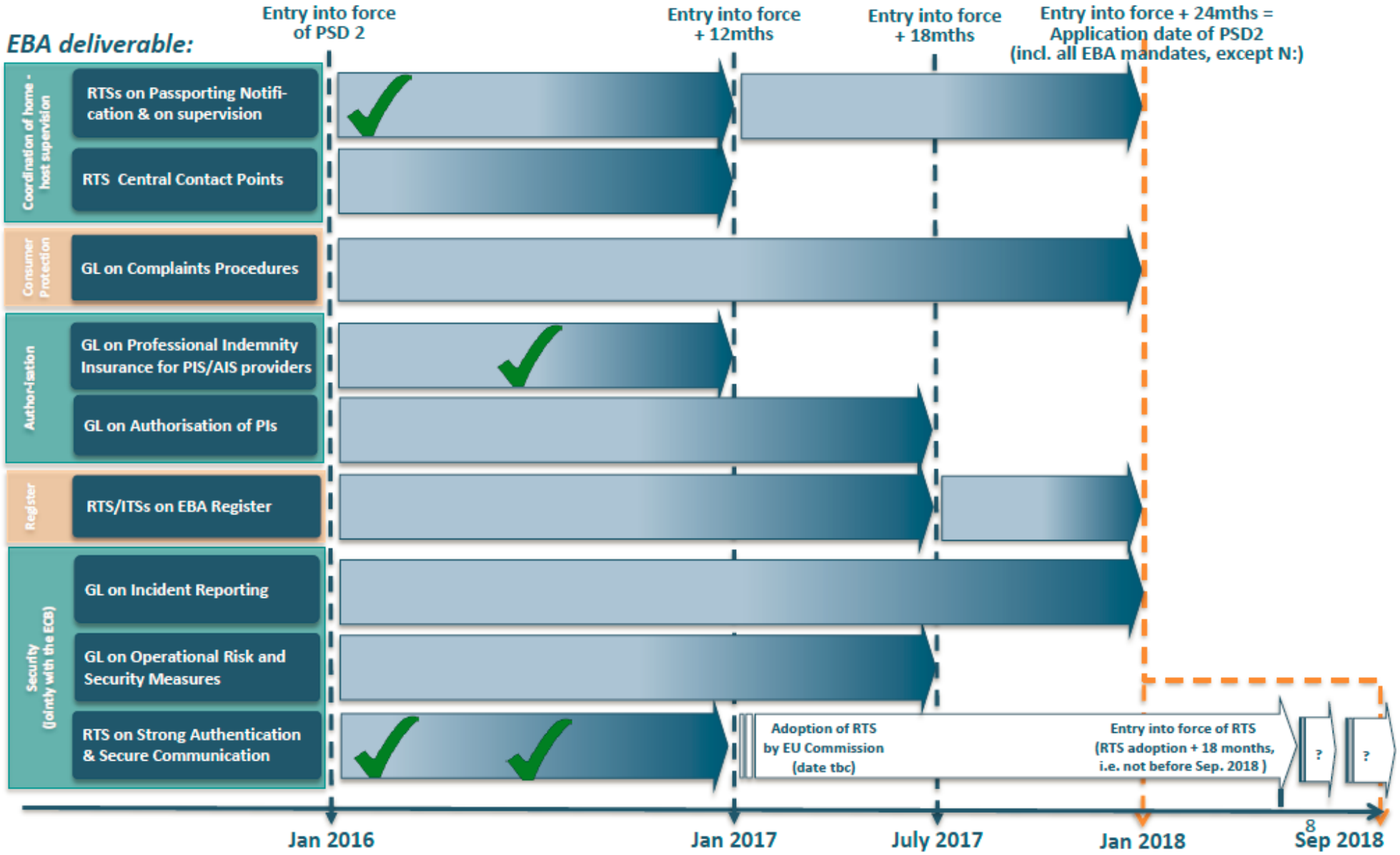
What does PSD2 regulate?

- One-legged transactions (all currencies)
- Unconditionally refund rights — (where goods are not consumed) and consumer do not need to contact merchant.
- Surcharging banned (for cards regulated in IFR and instruments in 260/2012 regulation)
- Payment Service User liability reduced from
  EUR 150 to EUR 50
- Introduction of Third Party Providers (TPPs)
  - TPPs' right to access payment accounts and to initiate payments from Account Servicing PSP (AS PSP)
  - A standard interface between TPPs and AS PSP
- Very specific security requirements

PSD2 follows (at least) two timelines:



EBA have several deliverables for PSD2:

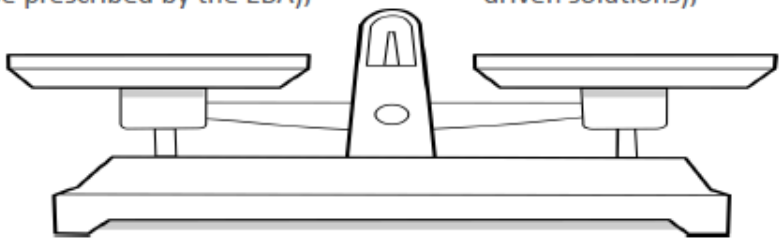


EBAs considerations when preparing the RTS

Strong authentication and secure communication: finding a balance between competing demands

When developing the RTS on strong customer authentication & secure communication, EBA and ECB will have to make difficult trade-offs between competing demands.

3) **Tough security standards** (which may suggest a high degree of prescription in the requirements to avoid circumvention of rules);	vs.	**Facilitation of innovative industry solutions in the future** (which may suggest the opposite, i.e. high level requirements that provide flexibility across firms & time);
2) **Tough security standards** (which may suggest that payment user should be subject to several security and authentication steps);	vs.	**Customer convenience** (which may suggest the opposite, e.g. one-click payments);
1) **High degree of interoperability between all ASPSPs and all PISPs/AISPs** (which may suggest one single standard/ protocol to be prescribed by the EBA);	vs.	**Flexibility for market participants** (which may suggest the opposite, i.e. high level requirements that in turn allow for different market-driven solutions);



mobey forum

@MobeyForum www.mobeyforum.org

The EBA RTS consultation consists of 4 areas:

- Strong Customer Authentication (SCA) procedure
- Exemptions from the application of SCA
- Protection of the confidentiality and the integrity of payment service users' personalized security credentials (not covered in this session).
- Common and secure open standards of communication

Strong customer authentication (SCA) – what is it?

Strong customer authentication (SCA) is 2-factor security (2 of these elements must be used: possession, knowledge and inherence)

FROM EBAs public hearing (sept. 23rd):

- *PSPs must ensure that a valid combination of authentication elements results in the generation of an authentication code that is only accepted once by the PSP for the same PSU.*
- *For electronic remote payments the authentication code must contains elements that dynamically link the amount and payee to the specific transaction.*
- *When SCA procedure relies on a mobile device, the channel, device or mobile application through which the information linking the transaction to a specific amount and a specific payee is displayed shall be independent or segregated from the channel, device or mobile application used for initiating the electronic payment transaction.*

Strong customer authentication – when to apply it?

FROM the EBA public hearing:

- *SCA must be applied when initiating (eletronic) credit transfers, card payments but not for Direct Debits (but must be used when creating the e-mandate).*

- *SCA must be applied when carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses.*

- *The SCA procecure will remain fully in the sphere of comeptence of the Account servicing payment service provider (ASPSP fx a bank). If a Payment initiation service provider wishes to use their own isseud credentials they have to have a contract with ASPSP.*

Strong Cusomter Authentication– when to apply it (2)?

Article 74(2) in PSD2 states that a payee can choose not to require SCA but will get full liability.
Please note that the RTS states that this 'option' is **only possible** in the period from Jan 2018 – to the implementation of the standards.

What if the online merchant is outside of EEA?

- This will be a one-legged transaction and in scope of PSD2 so SCA must be applied.
- At the public hearing the European Commission said that ASPSPs must reject the payment in case the merchant outside of EEA do not apply SCA.

Strong Customer Authentications - Exemptions

It will only be issuers/ASPSPs who can decide on exemptions for SCA (not acquirers or merchants). When exemptions are used the liability will be at the ASPSP.

- Exclusive access to information of payment account online, without disclosure of sensitive payment data (no definition but ECB did provide some thoughts on this in the SecurePay self-assessment document from 2014).
  However SCA is needed first access and every 30 days (at least)
- Contactless electronic payments of maximum 50 EUR and 150 EUR cumulated. This is proximity payments and not limited to card funded transactions.

Strong Customer Authentications – Exemptions (2)

- Credit transfer to a trusted payee (white listed receivers), but SCA first time or when amending the white list (not clear if who has liability and if the liability shift also involves corporates).
- Recurring credit transfers with same amount and same payee, but SCA first time
- Credit transfers to/from yourself and both accounts are held by the same ASPSP
- Credit transfer where the amount do not exceed 10 EUR or 100 EUR cumulated (liability will be with ASPSP).

According to the RTS it will **NOT** be possible to use transactional risk analysis for deciding when to apply SCA.

Common and secure open standards

- Each ASPSP shall offer at least one communication interface between AIS/PIS providers and TPPs. These interfaces must be used by TPPs.
- These must be documented and freely available on ASPSPs website
- The interfaces shall use data elements from ISO20022 where applicable.
- The interfaces must have the same level of functionality and availability (including support) as the online platform made available to the PSU.
- Changes to the interfaces must be announced 3 months before implementation.
- Not clear when ASPSPs must have the interfaces ready!

Common and secure open standards (2)

eIDAS level certificates must be used by PSPs and TPPs for identification purposes.

AIS providers shall request information from payment accounts every time the PSU requests such information and in addition the AIS may fetch information 2 times pr. day when the PSU is not requesting it.

How can we prevent that all AIS providers fetch data at midnight and noon?

MOBEY FORUM PSD2 webinar

THANK YOU for listening ☺

Remember the consultation deadline is October 12th

Let’s talk at MobeyDay in Barcelona next week