



BANCO DE PORTUGAL
EUROSYSTEM

Security aspects resulting from PSD2

Rui Pimentel • Head of Unit

5 July 2017



Agenda

- Evolution of the regulatory framework – PSD 2
- Overview of EBA mandates
- Article 97 – PSD 2
- Article 98 – PSD 2
- RTS on Strong Customer Authentication and Secure Communication
- Concluding remarks



Evolution of the regulatory framework – PSD 2

Innovation

"We have already used EU competition rules to ensure that new and innovative players can compete for digital payment services alongside banks and other traditional providers"

Commissioner Margrethe Vestager, European Commission – Press Release, 8 October 2015





Evolution of the regulatory framework – PSD 2

Competition

“Aims at providing a legislative framework to facilitate the entry of such new players and ensure they provide secure and efficient payment services”

Commissioner Margrethe Vestager, European Commission – Press Release, 8 October 2015





Evolution of the regulatory framework – PSD 2

Open-Access

"The new Directive will greatly benefit European consumers by making it easier to shop online and enabling new services to enter the market to manage their bank accounts, for example to keep track of their spending on different accounts"

Commissioner Margrethe Vestager, European Commission – Press Release, 8 October 2015





Evolution of the regulatory framework – PSD 2

- Political agreement among the European Commission, Parliament and Council on 5 May 2015
- Publication on 23 December 2015 in the Official Journal of the EU – entered into force on 13 of January 2016
- How will the current landscape evolve? Maximum harmonization but diversity in the transposition process across countries





Evolution of the regulatory framework – PSD 2

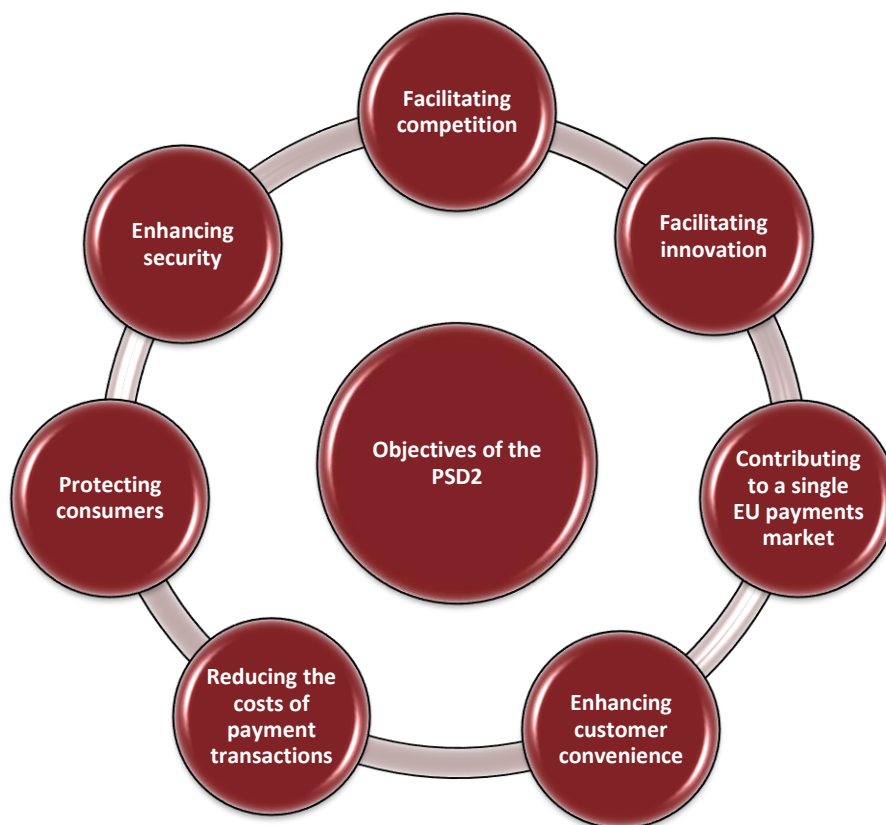
- Facilitate **competition** by **removing barriers** from the payments market
- Contribute to a **single EU payments market**
- Promote **innovative solutions** that are attractive to end-users
- Foster **efficiency** and lower the **costs** of transactions for the society as a whole
- Promote **security** and **robustness** of payment solutions





Evolution of the regulatory framework – PSD 2

In a nutshell...





Evolution of the regulatory framework – PSD 2

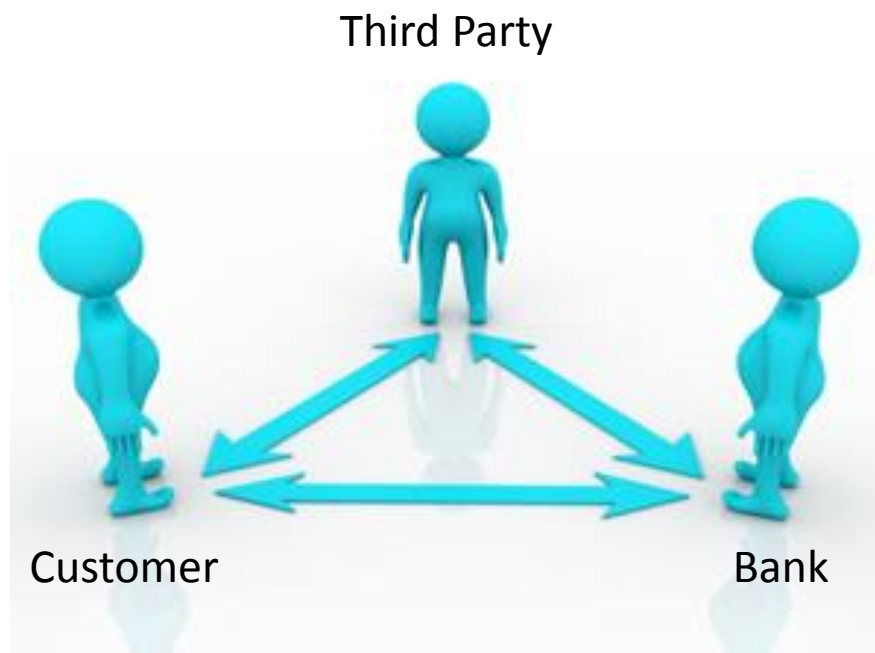
- Introduction of the Third Party Provider (TPP) scope of activities: Payment Initiation (PI) and Account Information (AI) services
- Banks shall offer payment services to Third-Party Providers (TPP) through an application programming interface (API)
- The services provided to third-parties must be responsive, transparent and secure





Evolution of the regulatory framework – PSD 2

Three-way relationship dynamics

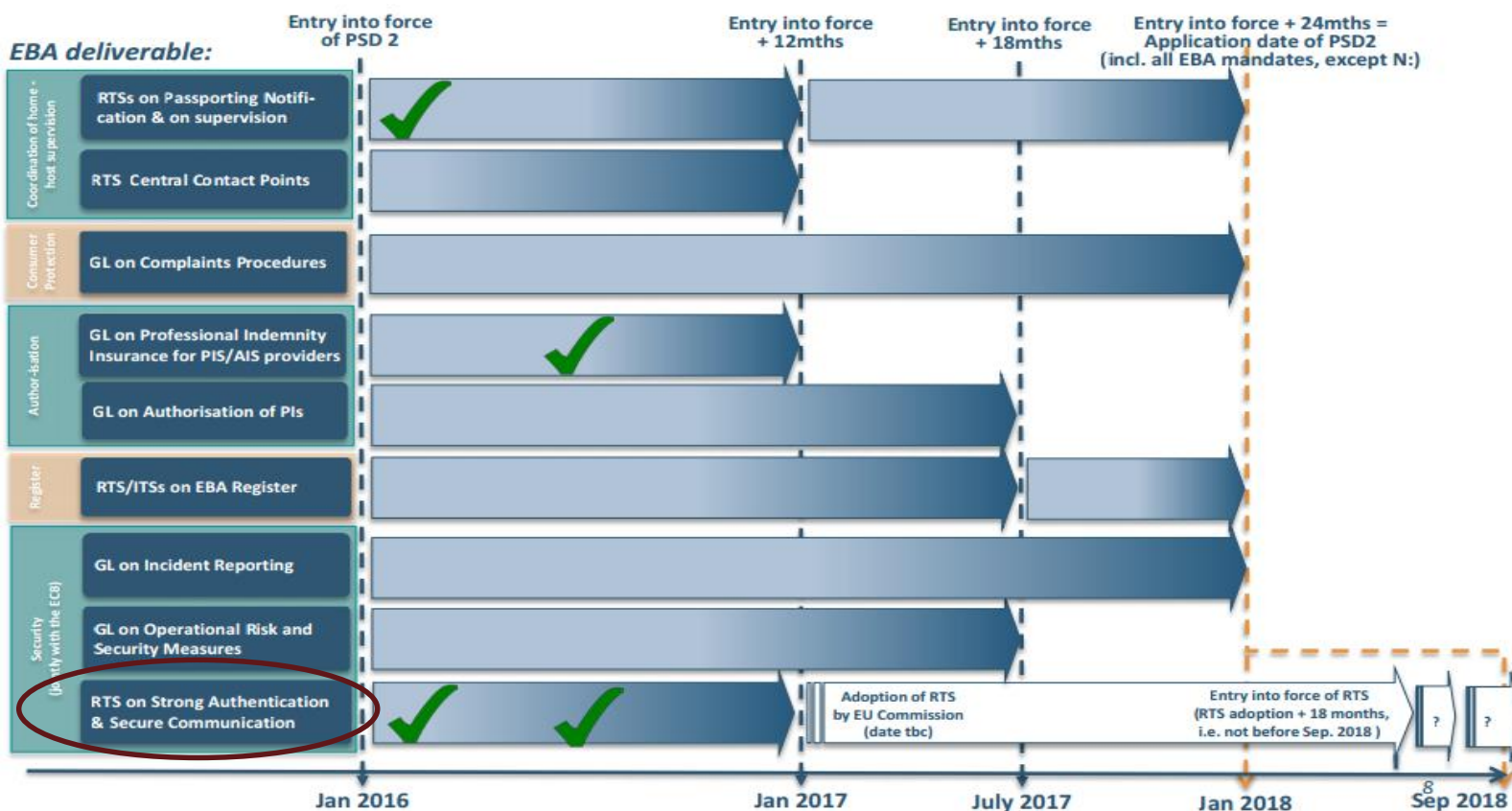




Overview of EBA mandates under PSD2



The PSD 2 has conferred on the EBA the development of 11 mandates.





Overview of EBA mandates

Deliverables	Milestones reached	Milestone 1: EBA has started work	Milestone 2: EBA has published CP	Milestone 3: EBA has published Final Report	Milestone 4: EBA has published GL compl. Table, or Official Journal has published TS
1	RTS on Passporting Notifications under PSD2	✓	✓	✓	
2	RTS on Strong Authentication & Secure Communications under PSD2	✓	✓	✓	
3	GL on Professional Indemnity Insurance under PSD2	✓	✓		
4	GL on Authorisation of payment institutions under PSD2	✓	✓		
5	GL on Incident Reporting under PSD2	✓	✓		
6	GL on Complaints Procedures by CAs under PSD2	✓	✓		
7	GL on Operational & Security Measures under PSD2	✓			
8	RTS on Central Contact Points under PSD2	✓			
9	RTS & ITS on EBA Register under PSD2	✓			
10	RTS on home-host coordination under PSD2	✓			



Extensive information available at
<http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money>



Article 97 of PSD 2

“Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

- (a) **accesses** its payment account online
- (b) **initiates** an electronic payment transaction
- (c) **carries out any action** through a remote channel which **may imply a risk** of payment fraud or other abuses.”





Article 97 of PSD 2

- There should be an **univocal correspondence** between the authentication of the specific transaction and the transaction itself, i.e. for the value and the payee of that transaction
- As a result, the authentication elements should be **dynamic**





Article 97 of PSD 2

Also:

“Member States shall ensure that payment service providers have in place adequate security measures to protect the **confidentiality and integrity of payment service users’ personalised security credentials.**”





Article 97 of PSD 2

Authentication and communication requirements are, in principle, applicable to every payment...



...even those initiated through a Payment Initiation Service provider (PIS).

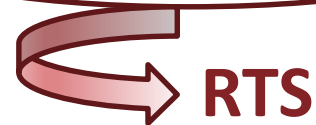


Article 98 of PSD 2

In relation to Article 97

“EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders [...] develop draft **Regulatory Technical Standards**” on:

1. Strong customer authentication
2. Secure open standards of communication



RTS





Article 98 of PSD 2

The RTS should also:

1. Determine the payments **exempted** from the applicability of Strong Customer Authentication methods
2. Require security measures to protect **confidentiality** and **integrity** of payment service users' credentials





Article 98 of PSD 2

Combines several goals...



Safety

Neutrality

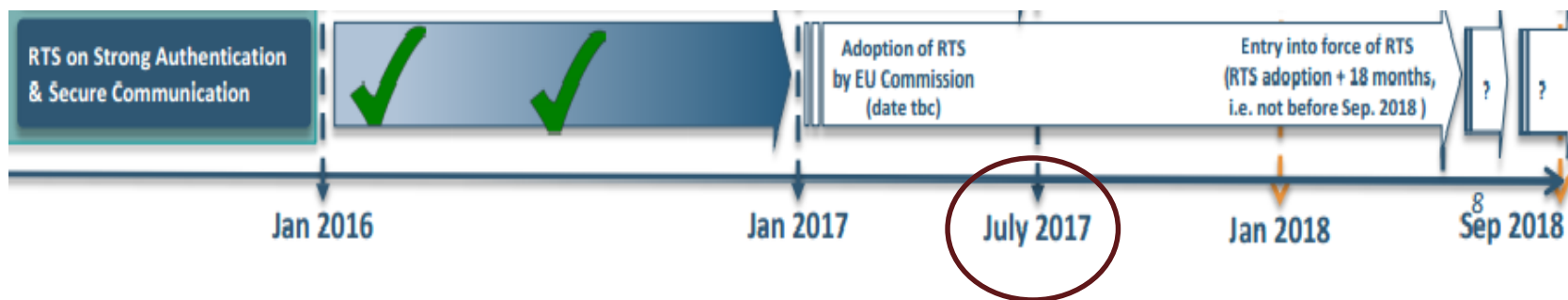
**User-
friendliness**

**Risk-
Based
Analysis**



Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

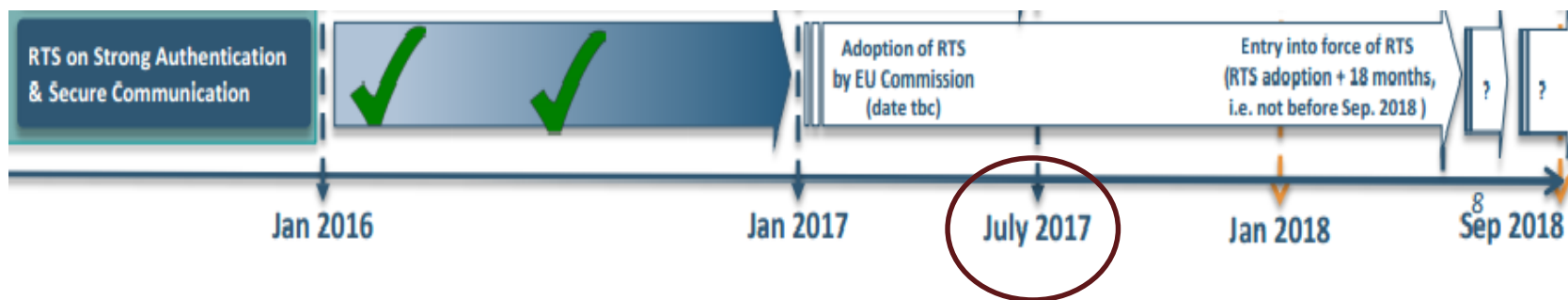
“4. EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission by 13 January 2017. Power is delegated to the Commission to adopt those regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.” (Article 98)





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

“5. In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments.” (Article 98)





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

- General provisions
- Strong Customer Authentication (SCA)
- Exemptions to SCA
- Personalised Security Credentials (PSC)
- Common and Secure Open Standards of Communication

FINAL REPORT ON DRAFT RTS ON SCA AND CSC

EBA/RTS/2017/02

23 February 2017

Final Report

Draft Regulatory Technical Standards

on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

- Date of publication of the final report: 23 February 2017
- The publication is preceded by 18 months of work
- European Commission to approve the final report
- RTS will apply after 18 months after adoption
- **PSD2 and RTS are market-changers**





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

- “In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as **knowledge** (something only the user knows), such as length or complexity”
- “[...]for the the elements categorised as **possession** (something only the user possesses), such as algorithm specifications, key length and information entropy”





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

- “[...] and for the devices and software that read elements categorized as **inherence** (something the user is) such as algorithm specifications, biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties.”
- “It is also necessary to define requirements ensuring that these elements are independent”





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

After a slight delay, this is now underway...

- EBA published draft RTS in February
- EC reacted by end of May with 4 main comments
- EBA formalised its position with an Opinion by end of June

More info at <http://www.eba.europa.eu/>

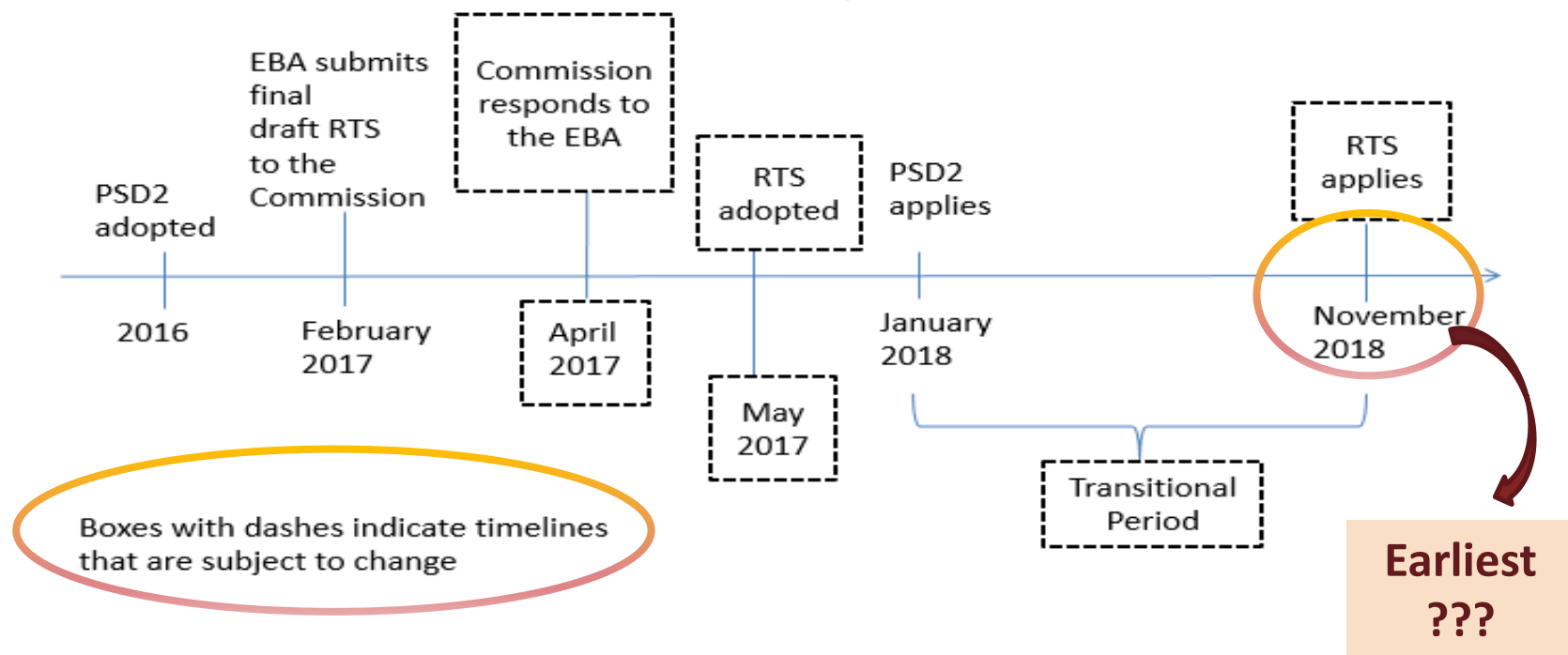


Concerns: i) auditing; ii) corporate payments;
iii) fraud statistics; and iv) fallback solution



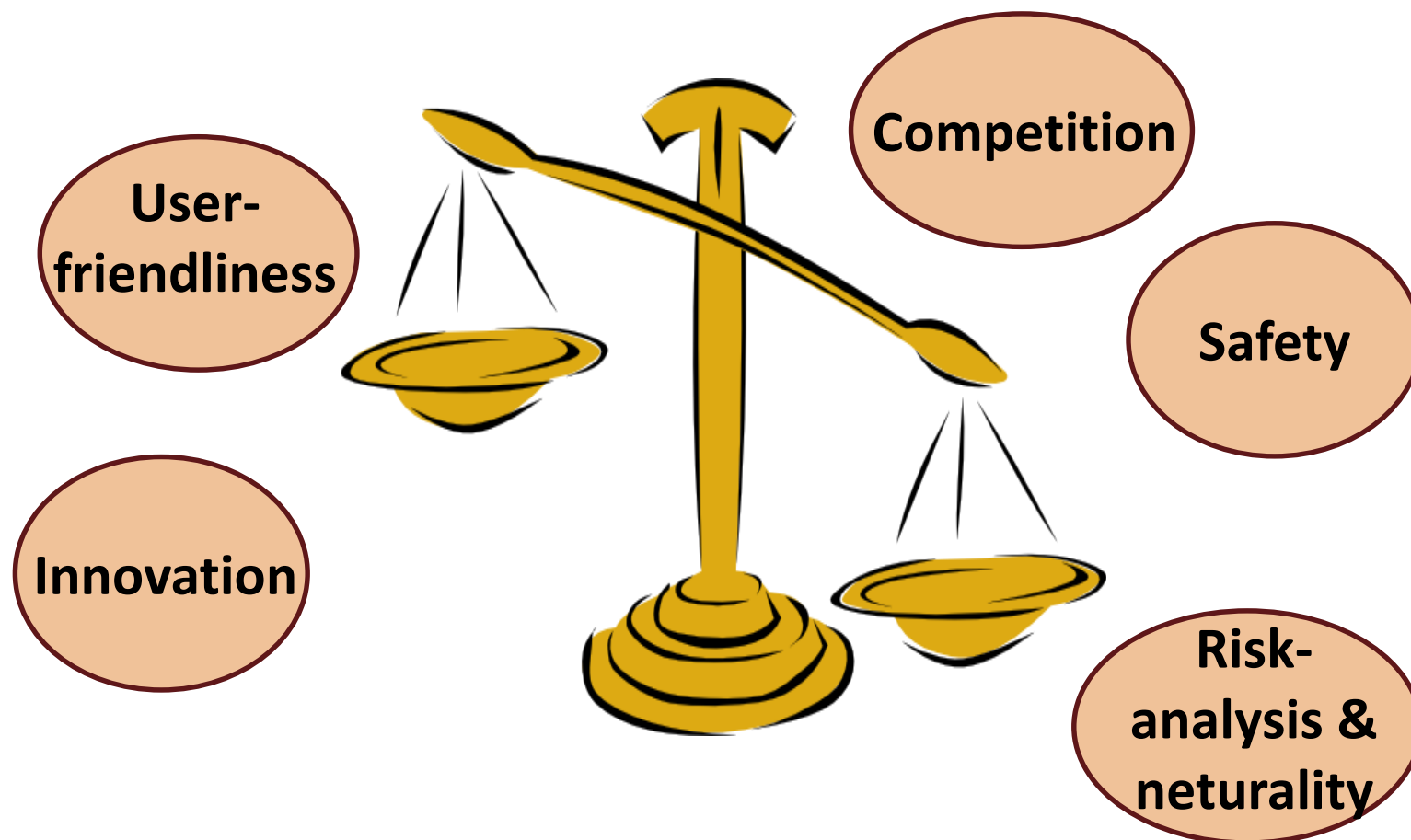
Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

Transposition of PSD2 into national law





Regulatory Technical Standards on strong customer authentication and secure communication under PSD2





One must never forget that security is always a challenge in an interconnected World...





...so the efforts need to be constant, cooperation is key to prevent crime and remain on the safe side!!



Thank you



BANCO DE PORTUGAL
EUROSYSTEM

Security aspects resulting from PSD2

Rui Pimentel • Head of Unit

5 July 2017