Are banks ready for PSD2?
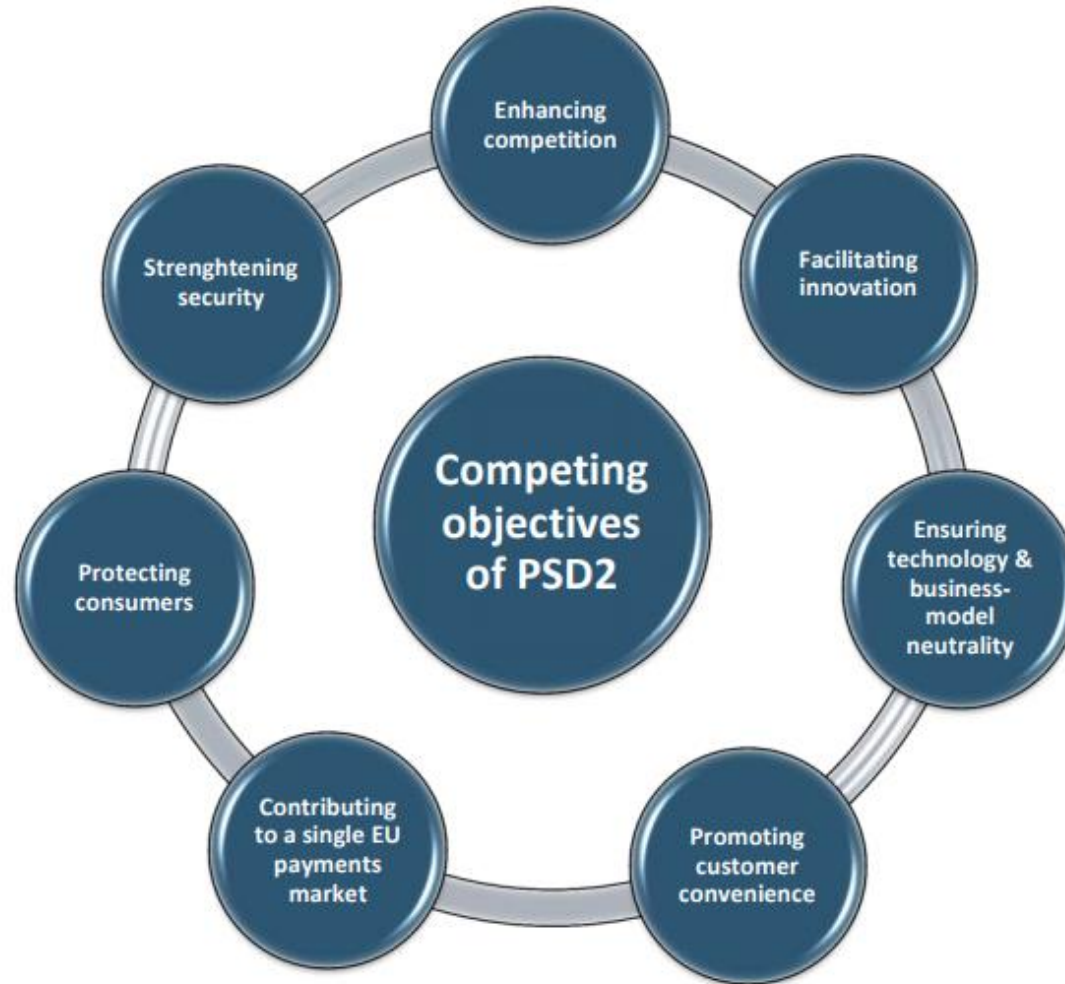
Gijs Boudewijn
Chair Payments Systems
Committee EBF

Croatian Banker's Association,
Zagreb

March 19th, 2018

ERSTE BANK

Brlog Mede Štede

HRVATSKA POŠTANSKA BANKA

NAŠA ZEMLJA
TREBA DJECU
KOJA VJERUJE
U SEBE.
I MEĐU KOJI
VJERUJE
U NJIH.

PRIVREDNA BANKA ZAGREB

splitskabanka

SBERBANK

Zagrebačka banka

banka kovanica

Addiko Bank

Raiffeisen BANK

PODRAVSKA BANKA

KENTBANK

The aims of PSD2

You know the feeling?

PSD2 is a game changer – do not underestimate it!

Four levels of applying PSD2
(focus on XS2A)

DETAIL ↓

Level 1: What? ➜ PSD2-text itself

Should have been implemented before Jan 13th, 2018 in Member States' national law

Level 2: How? ➜ EBA Regulatory Technical Standards on SCA en CSC

Determine how to do "XS2A" safely: Dedicated (API) interface; SCA; fall-back; redirect

Level 3: How? ➜ Multi-stakeholder 'self regulation' on PIS/ AIS-matters

Within ERPB and European API Evaluation Group

Level 4: How? ➜ Market-led API's: UK, Berlin Group, STET, banks..

Specificy how APIs should be built to be RTS-compliant; must look "good" !

Agreement on all levels to make it work ➜ lots of complexity!

Level 1: The PSD2-text itself

DIRECTIVES

DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 25 November 2015

on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
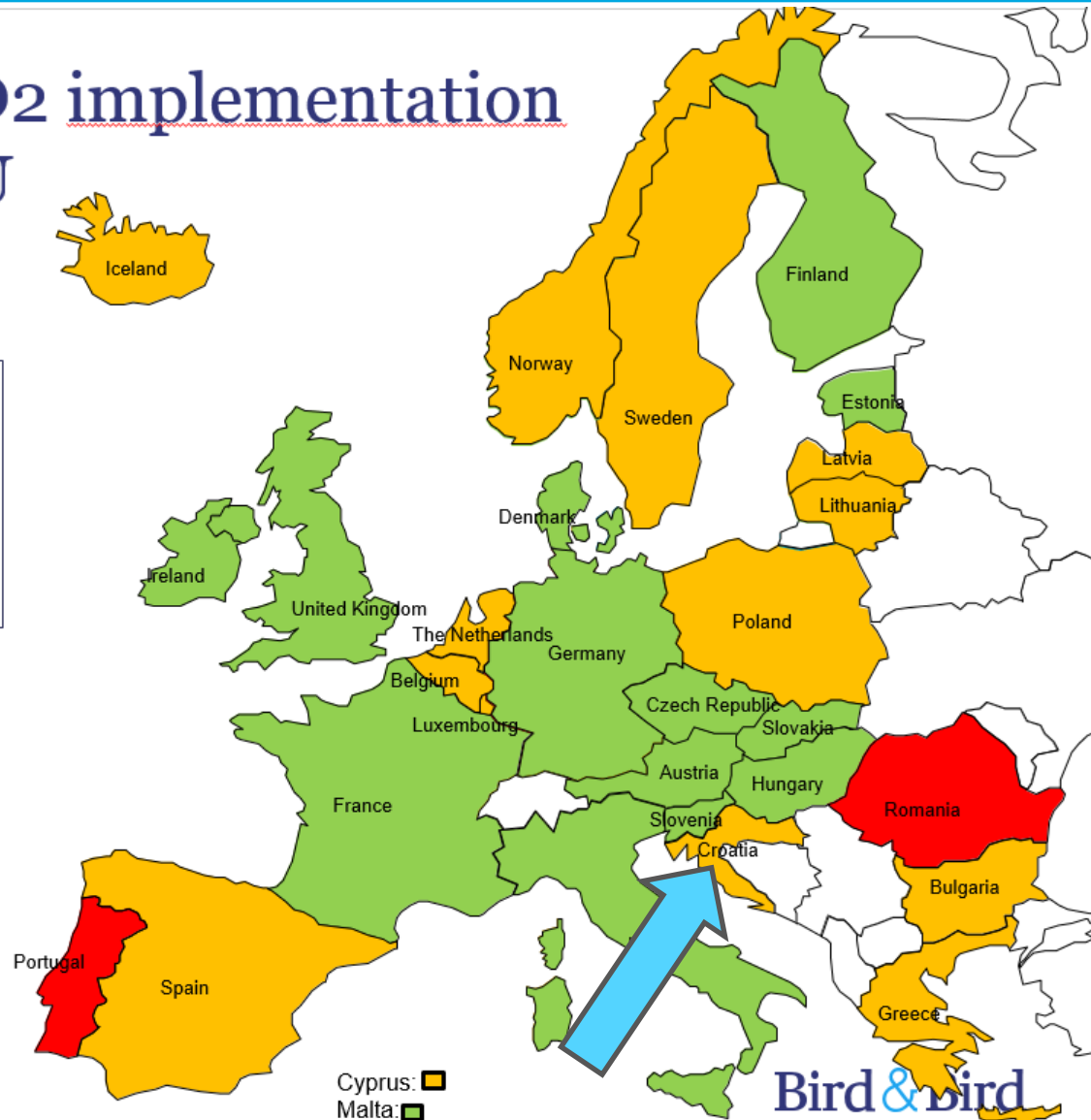
(Text with EEA relevance)

Level 1: PSD-text itself

Many Member States have not made the transposition deadline of Jan 13th, 2018 …

Status of PSD2 implementation across the EU

Legend:
- Implementation process completed (green)
- Draft law officially published (orange)
- No draft law officially published (red)

Iceland

Finland

Norway

Estonia

Sweden

Latvia

Lithuania

Denmark

Ireland

United Kingdom

The Netherlands

Poland

Germany

Belgium

Czech Republic

Luxembourg

Slovakia

Austria

Hungary

France

Slovenia

Croatia

Romania

Bulgaria

Portugal

Spain

Greece

Cyprus: (orange)
Malta: (green)

Bird & Bird

Level 1: Consequences non-compliance in NL
But may also apply for Croatia (?)

Oct. 23rd, 2017: Dutch Minister of Finance informed Parliament about consequences of delay:

- As from Jan 13th to June 2018 (when PSD2 is - expected to be - transposed into Dutch law) Dutch ASPSPs are <u>not legally obliged</u> to provide TPPs access to payment accounts

- TPPs with a EU passport from another Member State <u>cannot get access without a contract</u> (even after notification)

- "Unregulated access", i.e. access on a contractual basis, is possible like before

- New TPPs <u>cannot yet</u> apply for a license (PIS) or registration (AIS) in NL

- But Dutch **credit** institutions can get access to payment accounts in Member States that did meet the deadline

Level 1: Consequences non-compliance in NL
But may also apply for Croatia (?)

- Dec 19th, 2017: Publication of European Banking Authority 'Opinion on the transition from PSD1 to PSD2':

  - "*A delayed transposition in a host Member State cannot be used to prevent a legal entity from submitting a* **passporting notification** *in the Member State where that entity is authorised and where PSD2 has been transposed on time, or to prevent an entity from carrying out activities in that host Member State*"

- Dutch Ministry of Finance and Dutch Central Bank seem to indicate that the content of the letter (dated Oct. 23rd, 2017 re. the consequences of the delay) still fully applies

Level 2: EBA PSD2 RTS and Guidelines

Progress update on PSD2 mandates

	Mandates	Milestone 1: EBA has started work	Milestone 2: EBA has published CP with draft GL/TS	Milestone 3: EBA has published Final draft TS or Final GL	Milestone 4: EBA has published GL Compliance table or Commission has published TS in OJ
1	GL on security of internet payments under PSD1	✓	✓	✓	✓
2	RTS on scheme separation under IFR	✓	✓	✓	✓
3	RTS on Passporting Notifications under PSD2	✓	✓	✓	✓
4	GL on Authorisation of payment institutions under PSD2	✓	✓	✓	✓
5	GL on Professional Indemnity Insurance under PSD2	✓	✓	✓	✓
6	GL on Operational & Security Measures under PSD2	✓	✓	✓	✓
7	GL on Complaints Procedures by CAs under PSD2	✓	✓	✓	✓
8	GL on Incident Reporting under PSD2	✓	✓	✓	✓
9	RTS on Strong Authentication & Secure Comms. under PSD2	✓	✓	✓	✓
10	RTS on Central Contact Points under PSD2	✓	✓	✓	
11	RTS & ITS on EBA Register under PSD2	✓	✓	✓	
12	RTS on home-host coordination under PSD2	✓	✓	2018Q2	
13	GL on fraud reporting under PSD2	✓	✓	2018Q2	

Level 2: The EBA RTS on SCA and CSC
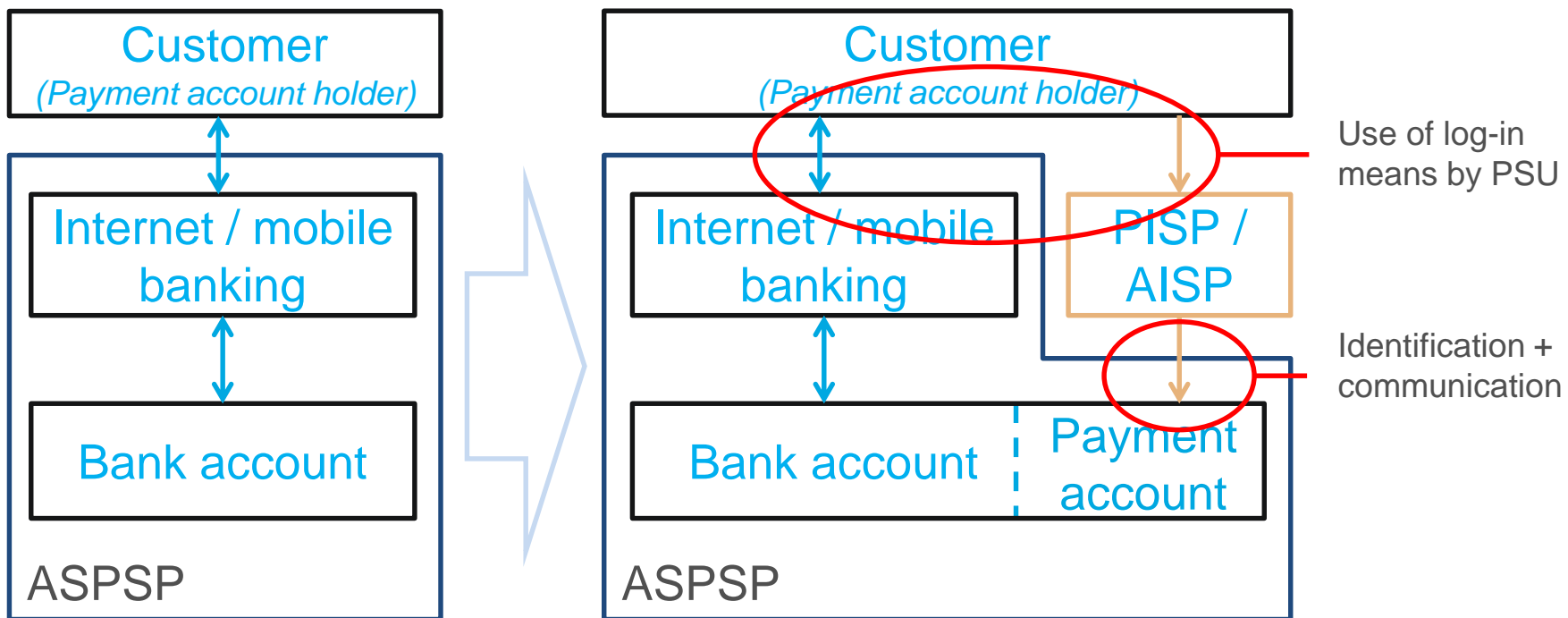
COMMISSION DELEGATED REGULATION (EU) 2018/389

of 27 November 2017

supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

(Text with EEA relevance)

Level 2: RTS on SCA and CSC
*What are they about?*

Level 2: RTS on SCA and CSC
Tough job for EBA…

Strong security standards	vs.	Facilitating future market solutions
Strong security standards	vs.	Stimulating easy user experience
High interoperability between ASPSPs and PISPs/ AISPs	vs.	Providing flexibility for market participants

…means difficult trade-offs

EBA: "*Our goal is to make everybody equally unhappy*"
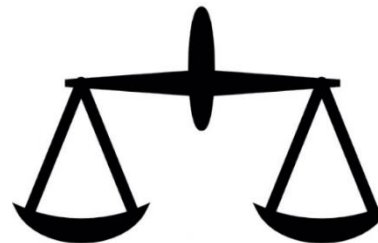
Level 2: RTS on SCA and CSC

- Nov 27th, 2017: RTS published and sent to Parliament and Council.

- So-called scrutiny period ended Feb 27th, 2018. As expected Parliament and Council did not reject the RTS.

- RTS published in OJ of the EU 13 March 2018.

- 13 Sep 2019: RTS apply.

- Interesting exchange of letters (Jan 26th, 2018 and Feb 13th, 2018) between EBA and EC) on the process and substance

- EBA Opinion (Dec 19th, 2017):

  "*The EBA advises CAs to encourage all PSPs to comply with these (the RTS) requirements as soon as possible. For ASPSPs, this means either the early adaptation of the customer interface or the early development of dedicated interfaces.*"

Level 2: RTS on SCA and CSC

- **Dedicated interface and fall-back:** ASPSP should offer TPP access via

  (i) User interface (screenscraping) *with* identification of TPP, or

  (ii) Dedicated interface (API)

- Dedicated interface (API) should offer same availability as compared to user-interface and offer (at least) the same functionalities

- In case of 5 refused API-calls within 30 seconds, TPP may switch to fallback (= screen scraping *with* identification, log sessions and notification to NCA)

- However: NCA can grant exemption to ASPSP of obligation to offer fallback, *provided* that API meets stringent quality and availability requirements, has been extensively tested by and approved by TPPs, etc.

- These requirements are to be drawn up by the *API Evaluation Group* (see also level 3), which was formed on the initiative of the European Commission

The **3** authentication factors:

Strong authentication
=
Combining 2 factors

Something you **HAVE**

Something you **KNOW**

Something you **ARE**

Art 97(1) PSD2 - a PSP applies SCA where the payer:

- Accesses its payment account online

- Initiates an electronic payment transaction
  - Credit transfer? Yes
  - Direct debit? No
  - Cards? Yes – although some card transactions are arguably initiated by the payee?

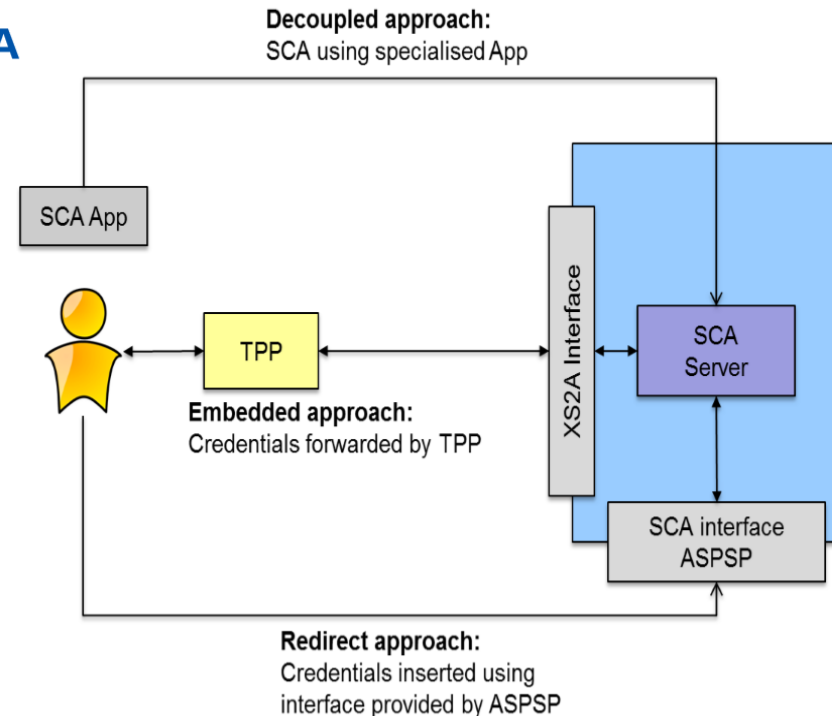- Carries out any action through a remote channel which may imply a risk of payment fraud or other abuses

To redirect or not to redirect, that is the question …

Key concepts: Strong customer authentication (SCA)

Different approaches for implementing SCA

- ■ Redirect approach
  - PSU is redirected to web interface provided by the ASPSP

- ■ Decoupled approach
  - SCA out-of-band using a special APP
  - Same behaviour as for Online Banking

- ■ Embedded approach
  - PSU enters credentials on the interface of the TPP

Decoupled approach:
SCA using specialised App

SCA App

TPP

XS2A Interface

SCA Server

SCA interface ASPSP

Embedded approach:
Credentials forwarded by TPP

Redirect approach:
Credentials inserted using interface provided by ASPSP

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

Copyright Berlin Group

Level 2: RTS on SCA and CSC

To redirect or not to redirect, that is the question …

- **Dedicated interface in combination with a redirect model:**
  Art. 32 (3) of the RTS states:

3. Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.

- Not fully clear what this means in practice: Commission clarified that "redirect" is only an example of a possible obstacle

- The market is in uncertainty …....

Level 2: RTS on SCA and CSC

To redirect or not to redirect, that is the question …

A possible approach…

- Assuming that an API in combination with a redirect model according to art. 32 (3) RTS is not prohibited *per se*, but only when it does form a true obstacle to providing PIS and/or AIS *("let us not make it an ideological discussion")*

  - A poor redirect implementation could be an obstacle, e.g. when it provides for a poor customer journey

- ASPSP offers a well functioning, safe and robust API, which complies with RTS-requirements:

  - ASPSP can request an exemption from NCA to offer fallback;
  - NCA determines whether API complies with RTS (whereby it also checks whether - if the API works via the redirect model - it is not an 'obstacle' within the meaning of art. 32 (3) RTS;
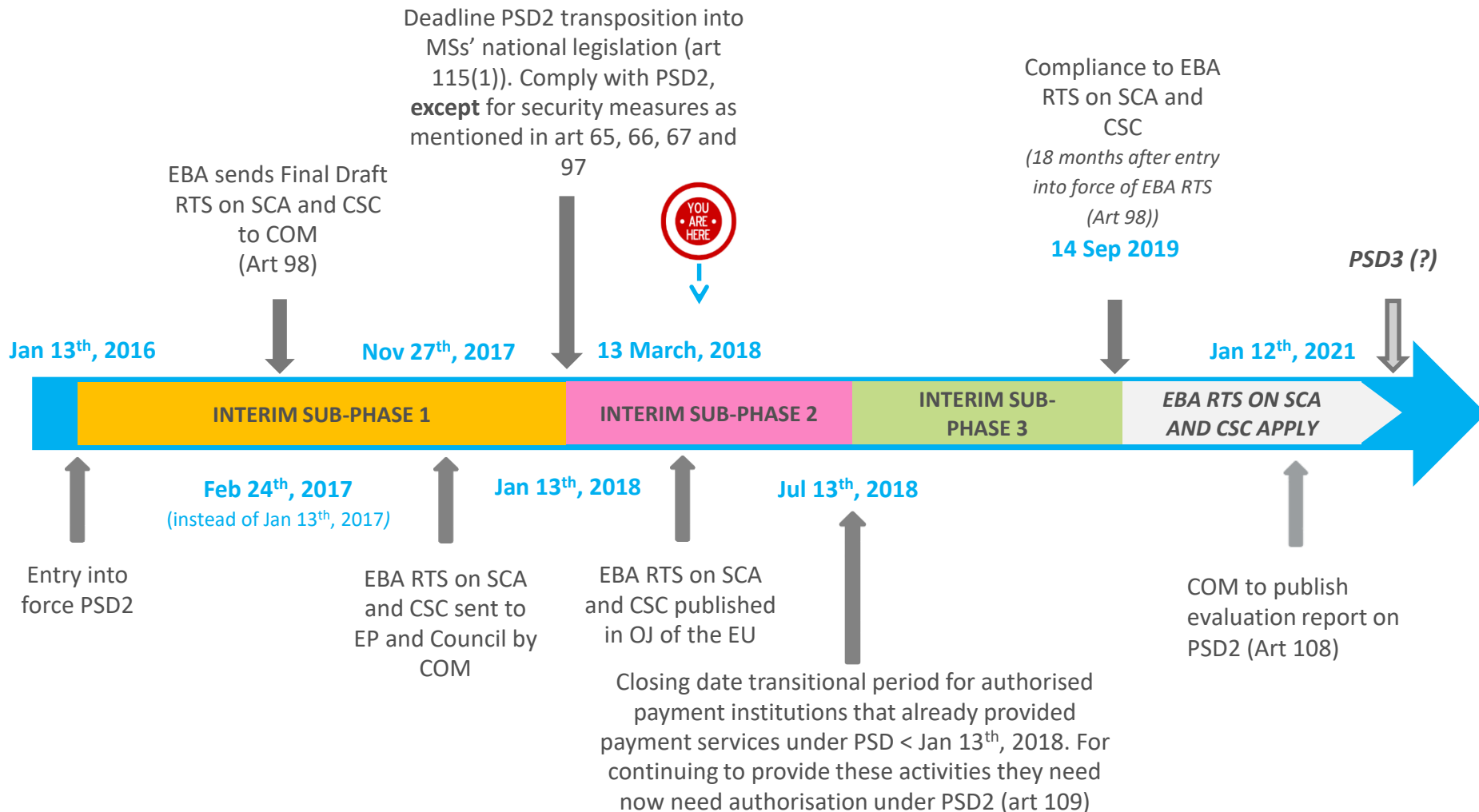 - If yes: Exemption. If not: No exemption

Level 2: RTS on SCA and CSC
Transition period until Sep 14th, 2019

- As per Jan 13th, 2018 (and in a few Member States some time later): PSD2 applies by transposition into national legislation, ***except*** for the security measures referred to in art. 65, 66, 67 and 97 of PSD2.

  - EBA Opinion (Dec. 19th, 2017): More specifically, it concerns those security measures as described in art. 65(2)(c), 66(3)(d), 66(4)(a), 67(2)(c), 67(3)(a), 97(1) t/m 97(4)) PSD2

- Roughly this means that AISP and PISP do **not** have to **identify** themselves with the ASPSP and do **not** need to **communicate securely** (art. 65, 66, 67)

- Art. 97 PSD2 has already been implemented for the most part into EBA's '*Guidelines on the security on internet payments*' from 2015

  - However, these GLs do not oblige ASPSPs to apply SCA for online access payment account and to use a dynamic code that links amount and beneficiary

  - These EBA GLs remain in force, if they are not in violation of PSD2 (*see EBA Opinion*)

- So SCA was and remains obligatory and "screen scraping" remains permitted for the time being (i.e. until Sep 14th, 2019)

PSD2 & RTS – Transitional period(s)

Deadline PSD2 transposition into MSs' national legislation (art 115(1)). Comply with PSD2, **except** for security measures as mentioned in art 65, 66, 67 and 97

Compliance to EBA RTS on SCA and CSC
(18 months after entry into force of EBA RTS (Art 98))
14 Sep 2019

EBA sends Final Draft RTS on SCA and CSC to COM (Art 98)

PSD3 (?)

YOU ARE HERE

Jan 13th, 2016

Nov 27th, 2017

13 March, 2018

Jan 12th, 2021

INTERIM SUB-PHASE 1	INTERIM SUB-PHASE 2	INTERIM SUB-PHASE 3	*EBA RTS ON SCA AND CSC APPLY*

Feb 24th, 2017
(instead of Jan 13th, 2017)

Jan 13th, 2018

Jul 13th, 2018

Entry into force PSD2

EBA RTS on SCA and CSC sent to EP and Council by COM

EBA RTS on SCA and CSC published in OJ of the EU

Closing date transitional period for authorised payment institutions that already provided payment services under PSD < Jan 13th, 2018. For continuing to provide these activities they need now need authorisation under PSD2 (art 109)

COM to publish evaluation report on PSD2 (Art 108)

Level 3 – Multi-stakeholder 'self regulation'
ERPB PIS Working Group

- Final report of the Euro Retail Payments Board PIS WG was endorsed by ERPB on Nov 29th, 2017

- Since then, WG has made a 'restart' to:

    - Validate its final report against the RTS on SCA and CSC

    - Further work on requirements that require further elaboration, such as standardization of PSD2-certificates under eIDAS (together with ETSI; a telco standards organisation)

    - Harmonisation of license registers and development of directory services

    - Development of other business requirements (such as dispute resolution procedures between TPPs and ASPSPs)

Level 3 – Multi-stakeholder 'self regulation'
API Evaluation Group

- End 2017, COM invited market players to form the API Evaluation Group, which should establish criteria to enable the 'vetting' of standardised API specifications

  - *"The work should support ongoing standard market initiatives and **future decisions by national competent authorities** as to **whether an API meets the requirements for an exemption from the obligation to provide a fall-back mechanism** for the dedicated interface, which would be provided for in the final RTS."*

- It is a "*joint effort by ASPSPs, TPPs and PSUs*", and COM, ECB and EBA join as "*active observers*" who can provide "*guidance*" if needed.

  - Members: EACB, EBF, ESBG, Bankin, Trustly, Klarna, eCommerce Europe, Eurocommerce, BEUC, EMA and EPIF

  - Secretary: EPC, co-chairs New Payment Systems Operator (NPSO) and Trustly

  - COM wants results in Q3 2018, but market parties want results already in Q2, because of back-planning from sept. 2019 (when RTS are expected to apply)

Level 4 – Market-led API's
## *Several standardisation initiatives*

- Berlin Group NextGenPSD2: Version 1.0 of NextGenPSD2 Framework published on Feb 8th, 2018

- Open Banking UK (live)

- PSD2 Polish API (live)

- SBA Open API (draft)

- STET PSD2 API (live)

- API Evaluation Group experts now in the process of applying criteria and evaluating

- Expectations, also of the European Central Bank: more harmonisation is desirable. Possibly only UK Open Banking and Berlin Group as future standards will remain ….

So, where are we?

- **Level 1:** PSD2 transposition into several Member States' national law still underway; some guidance is still required. COM has promised some clarification based on transposition workshops; perhaps Q&A tool by EBA

- **Level 2:** Final RTS on SCA and CSC are published in OJ of the EU on March 13th, 2018

- **Level 3:** ERPB PIS WG continues. API Evaluation Group will 'evaluate' API-standards (*not individual API's!*). What does a good API look like? Horizon June 2018

- **Level 4:** API initiatives to be vetted – will we see more API harmonisation …..?

Are *you* ready for PSD2 and beyond?
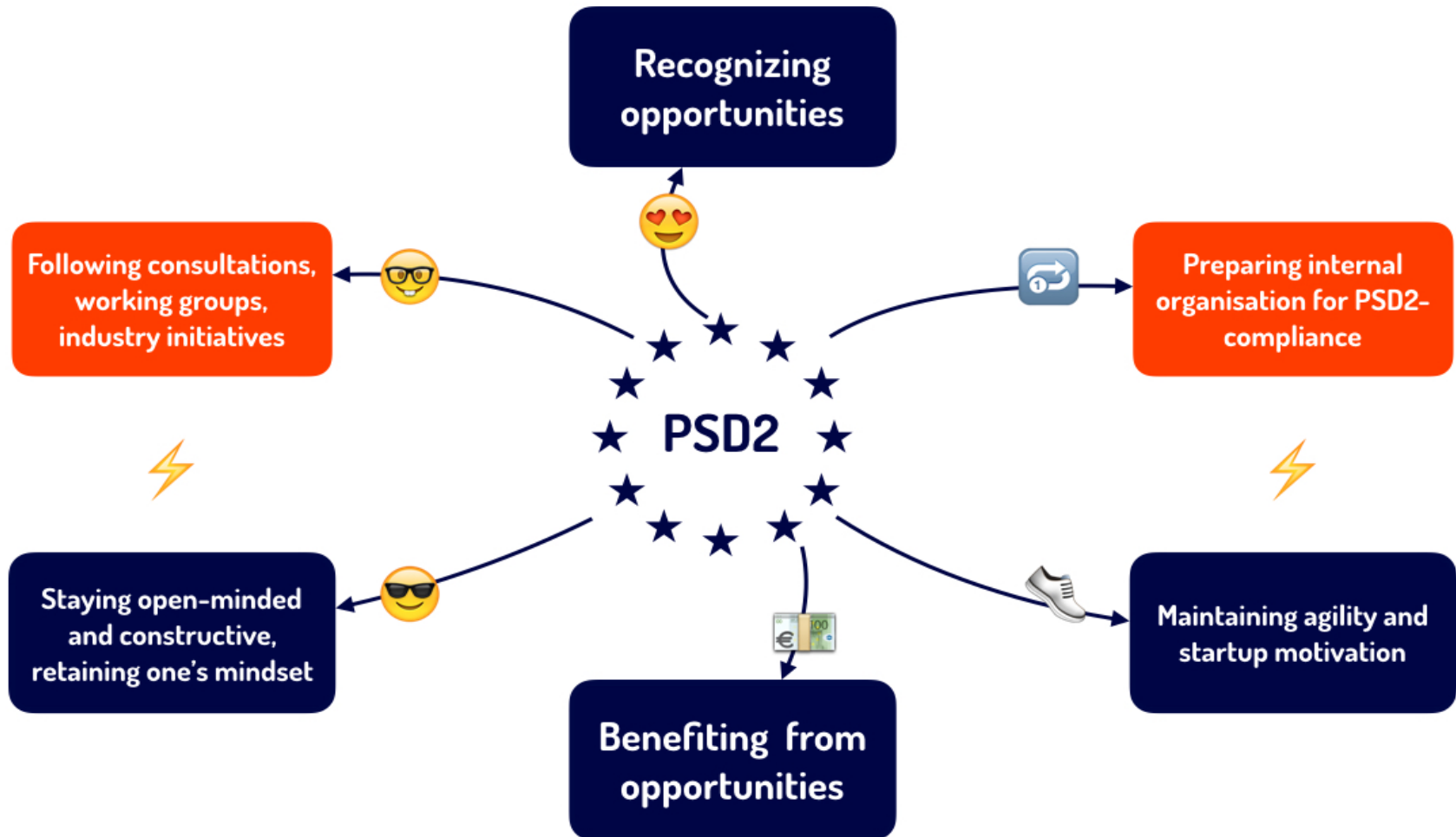
What is *your* strategy?
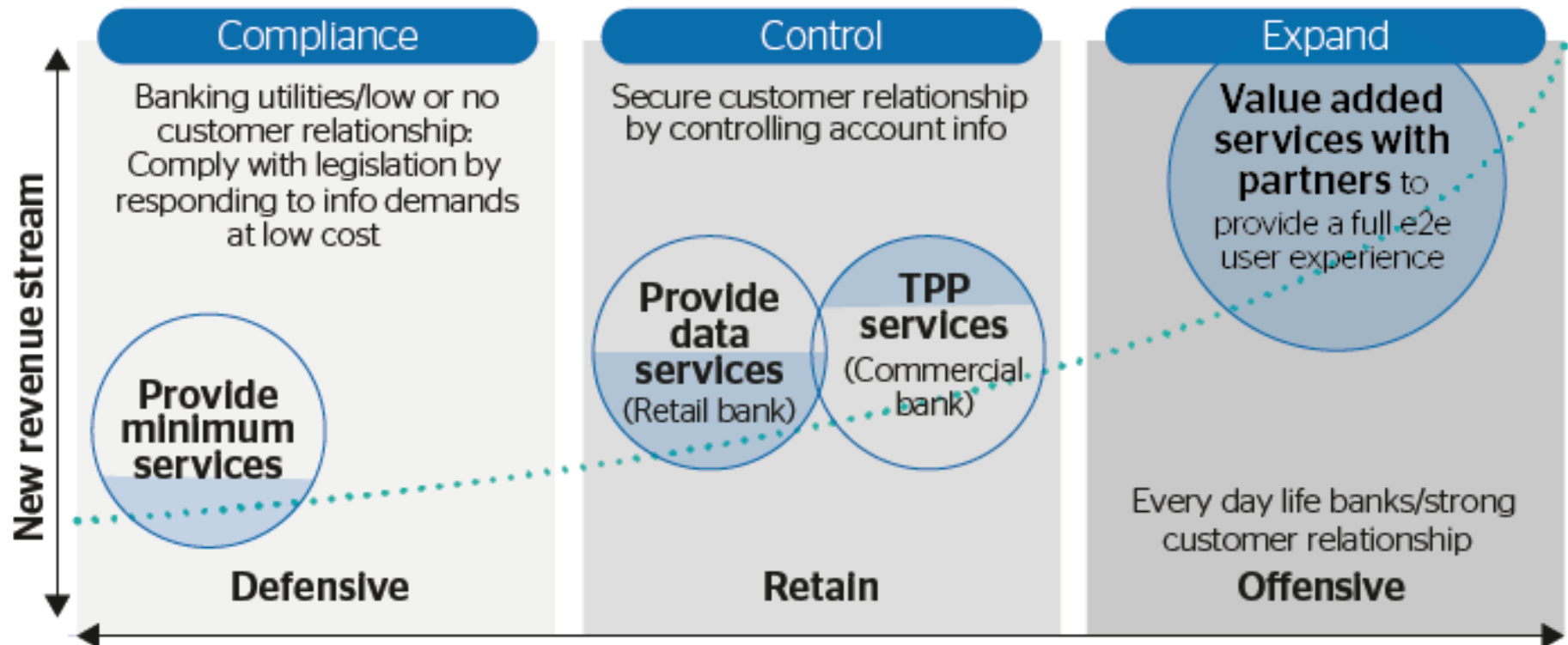
Questions?

g.boudewijn@betaalvereniging.nl