PSD2 is een feit. Hoe werkt die toegang tot de rekening?

Kennisevent – softwarepakketten.nl

Max Geerling
Executive Advisor

Hoevelaken
9 oktober 2019

Historie Currence / Betaalvereniging Nederland

Betalingsverkeer is gebaat bij collectiviteit

Currence – opgericht 1 januari 2005: eigenaar nationale collectieve betaalproducten

PIN	geëindigd 2011
Chipknip	geëindigd eind 2014
Incasso	geëindigd februari 2014
Acceptgiro	--
iDEAL	sinds 2005
Incassomachtigen	sinds 2016
iDIN	sinds 2017

Betaalvereniging – opgericht 2011: faciliteren collectieve aspecten NL betaalinfrastructuur

Rollen en taken

Betaalvereniging Nederland

- Productmanagement
- Kwaliteitsbewaking
- Fraudebestrijding
- Betalingsverkeer expertise
- Verandermanagement
- Voorlichting

SEPA
Single Euro Payments Area

BESCHIKBAARHEID INTERNETBANKIEREN EN MOBIEL BANKIEREN

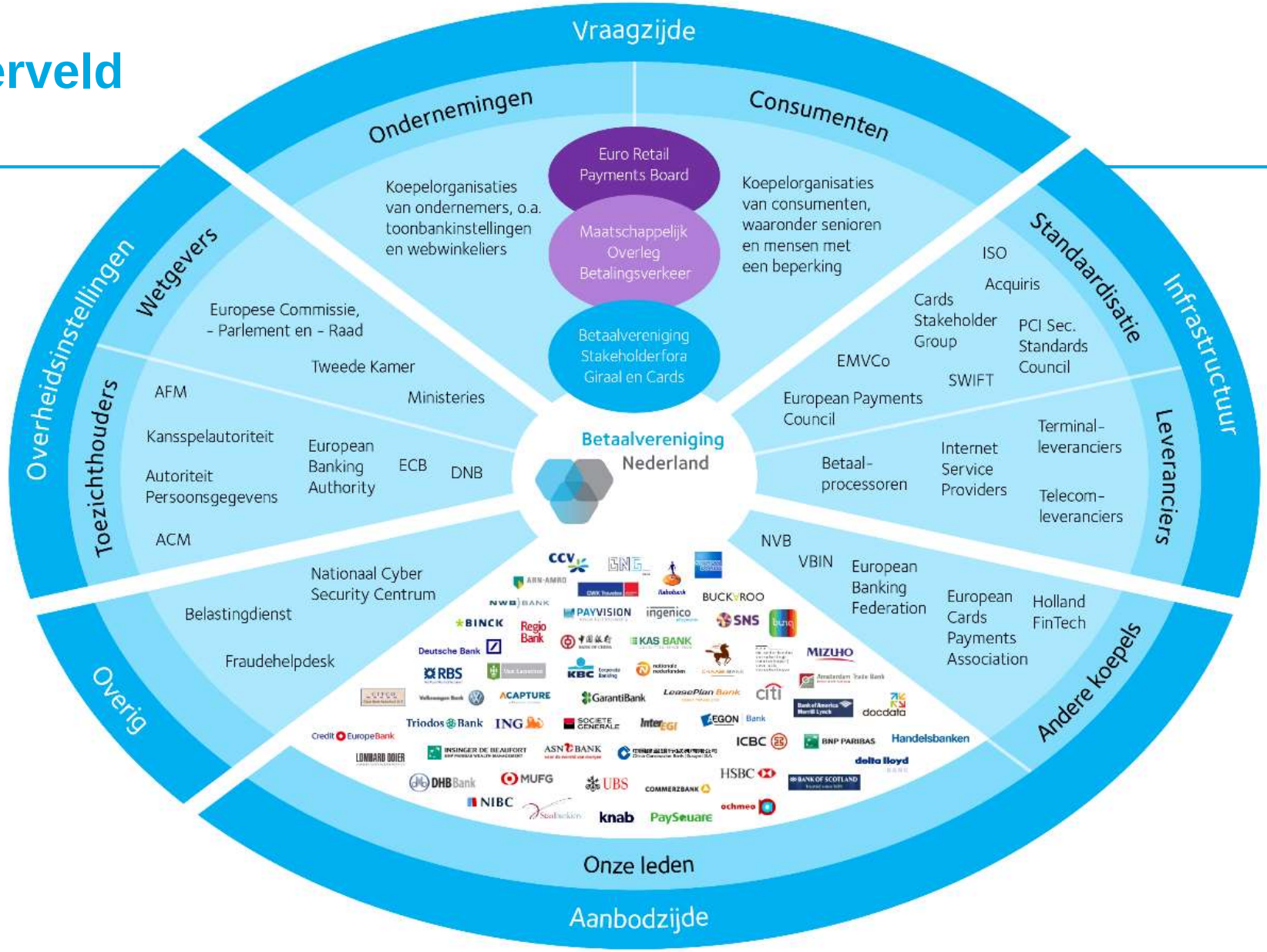
Laatste update: 10-3-2017 11:12

CONSUMENTENBANKEN		
ABN AMRO	✓	✓
ASN Bank	✓	✓
ING	✓	✓
Rabobank	✓	✓
RegioBank	✓	✓
SNS	✓	✓
Triodos Bank	✓	✓

KLEIN BEDRAG? PINNEN MAG!

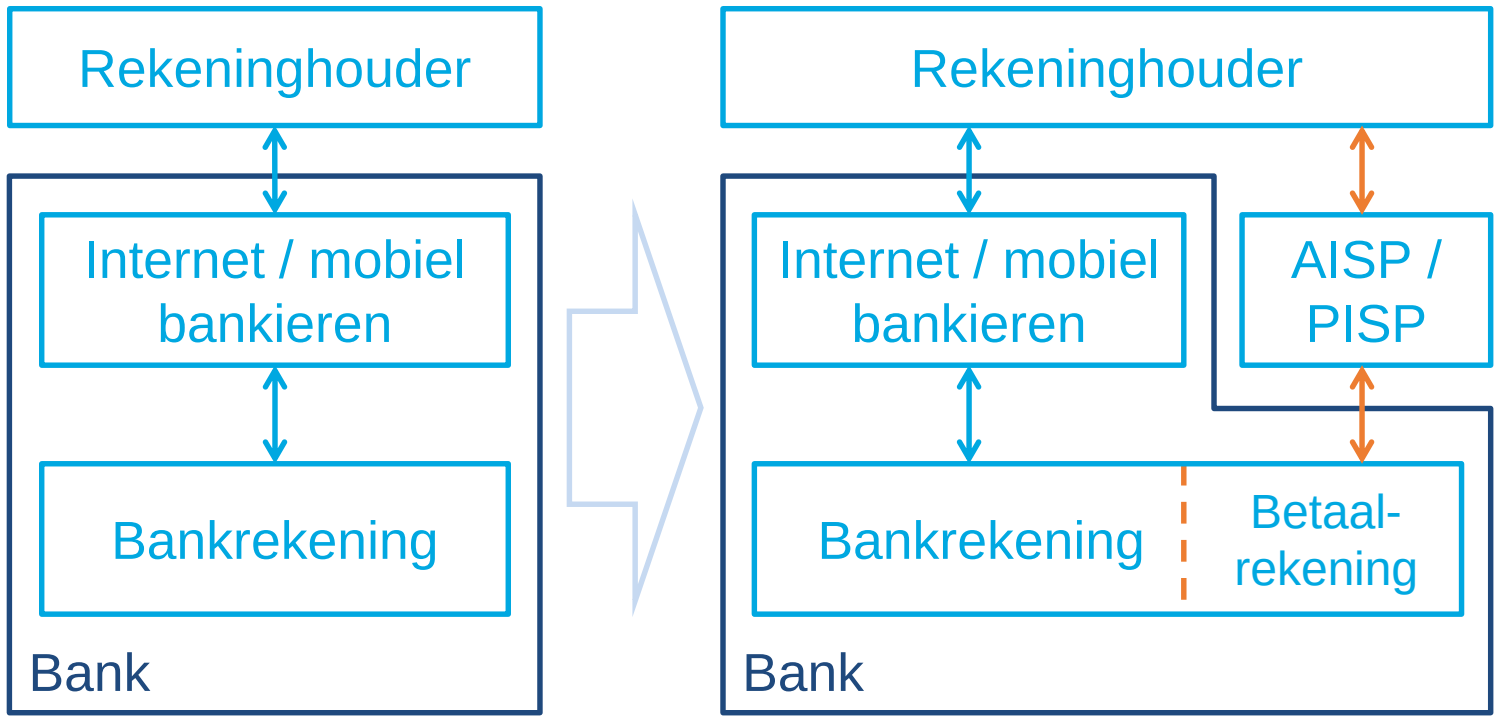
BETAAL HIER OOK

Stakeholderveld



Geharmoniseerde toegang tot de betaalrekening (XS2A)

Betaalinitiatie en rekeninginformatie



AISP
Account Information Service Provider

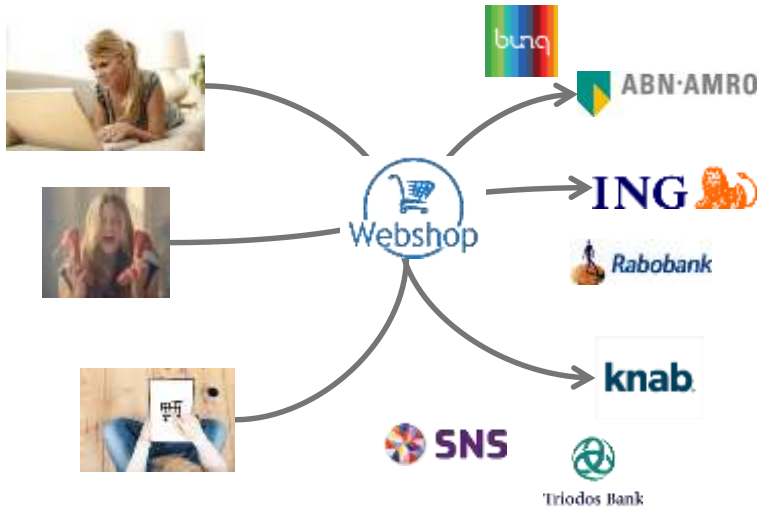
PISP
Payment Initiation Service Provider

Betaalinitiatie- en rekeninginformatiedienstverlening

Waar is het voor bedoeld?

Betaalvereniging Nederland

Payment Initiation Services (PIS)
Betaler initieert via PISP bij zijn bank een betaling (SCT) ten laste van zijn betaalrekening



Voorbeeld: Een webwinkel initieert – met toestemming klant – zelf als PISP een betaling ten laste van de betaalrekening bij de bank van de klant (onder PSD2 vergunning als betaalinstelling nodig)

Account Information Services (AIS)
AISP krijgt toegang tot rekeninginformatie (saldo, bij- en afschrijvingen en omschrijvingen)

Voorbeeld: App van AISP toont geaggregeerde rekeninginformatie van consument die bij meerdere banken betaalrekening aanhoudt. AISP heeft registratie bij nationale toezichthouder

Voorbeelden van AIS
- Financiële planning
- Huishoudboekje
- Kredietbeoordeling
- Schuldhulpverlening
- Prijsvergelijking / overstap

Hoe wordt PSD2 Bankieren mogelijk gemaakt?

Maatregelen voor de bank

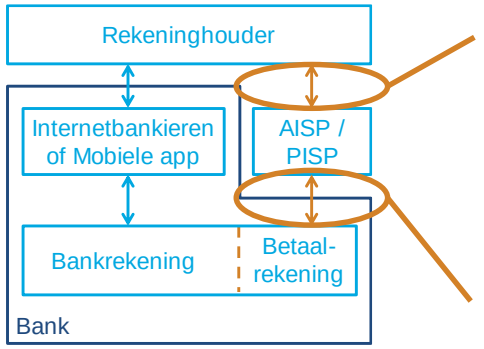
- Strong Customer Authentication (SCA) procedure
  - twee-factor authenticatie
  - koppeling met bedrag + begunstigde (PIS)
- 90 dagen toegang tot rekeninginformatie (AIS)

Toegangsvoorwaarden voor AISP / PISP (TPP)

- Autorisatie door vergunning – eventueel met EU paspoort
- Identificatie met een eIDAS certificaat – geen contract TPP / bank
- Instemming door de rekeninghouder

Rekeninghouder

- Maakt gebruik van de inlogmiddelen zoals verstrekt door de bank – wijze bepaald door de bank

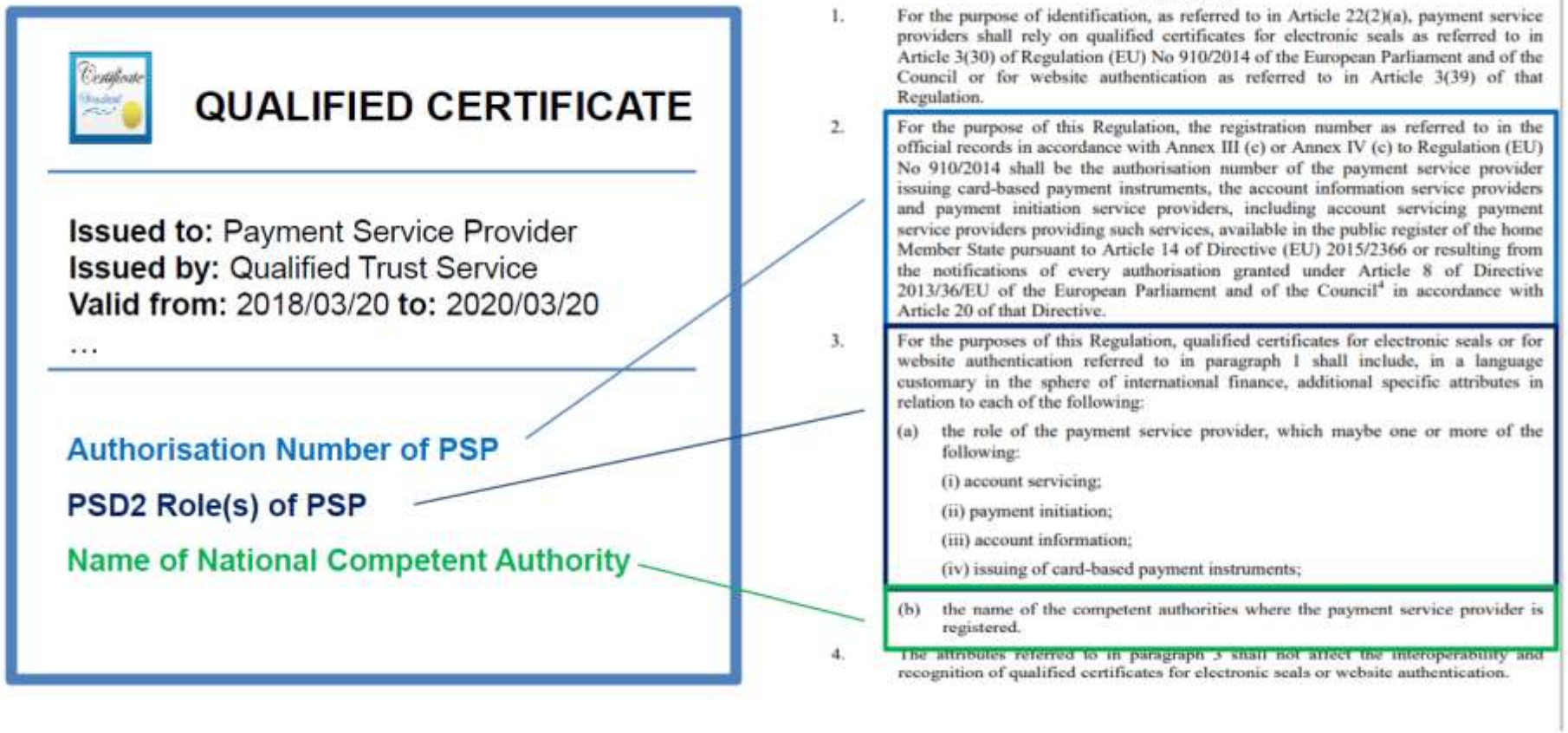


TPP moet kunnen vertrouwen op de ***inlogmiddelen (SCA)*** zoals verstrekt door de ASPSP

Identificatie door de AISP / PISP met een ***qualified*** (eIDAS) ***certificaat***

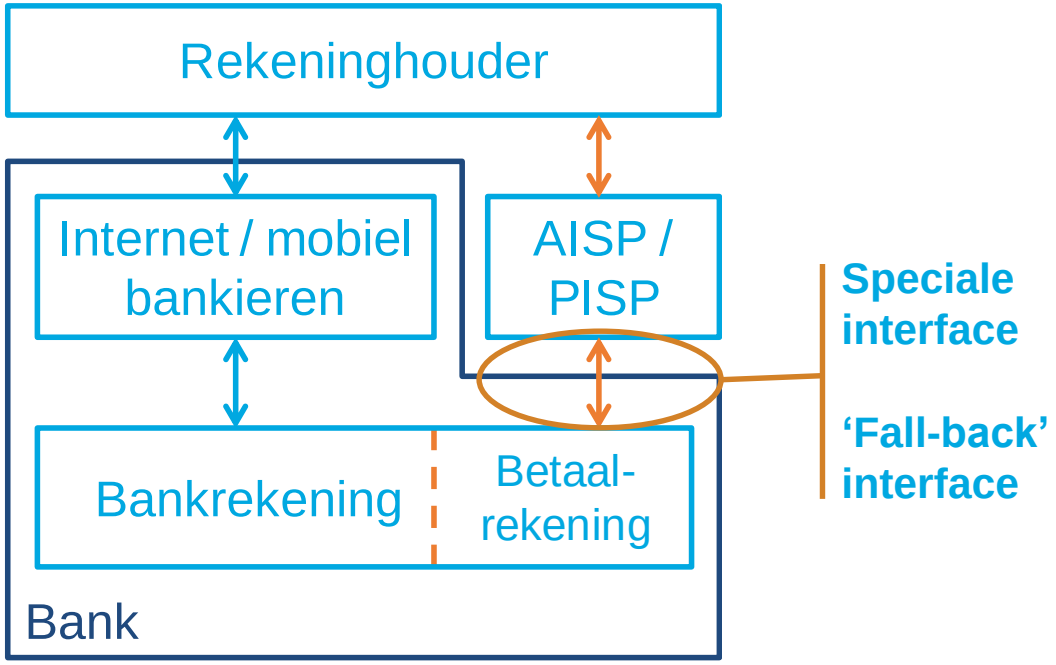
ETSI standard

Data elements in the certificate (RTS Art 34)



AISP / PISP toegang zonder contracten

Uiteindelijk twee compromissen op elkaar gestapeld



Speciale interface (API)

- Oorspronkelijk voorstel EBA
- Voorkeur van meerderheid PSPs

Compromis 1: **'Fall-back' interface**

- "Screen scraping with TPP identification"
- Komt tegemoet aan zorgen van AISP / PISPs
- Voor het geval API niet beschikbaar is

Compromis 2: **Vrijstelling** van 'fall-back' - Art. 33(6)

- Voor banken die goede kwaliteit API aantonen
- Criteria in aparte EBA Exemption Guidelines

Berlin Group / NextGenPSD2 API framework

Participants

60 participants
- Banking associations
- Payments associations
- Banks
- Processors

Dutch Payments Association participates for the benefit of its members.

NextGenPSD2 – API services

Betaalvereniging Nederland

AIS

- Establish account information consent
- Get list of reachable accounts (optional)
- Get account details of the list of accessible accounts
- Get balances for a given account
- Get transaction information for a given account

PIS

- Initiation of a single payment
- Initiation of a future dated single payment (optional)
- Initiation of a multiple / bulk payment (optional)
- Initiation of a recurring payment (optional)
- Cancellation of payments (optional)

PIIS

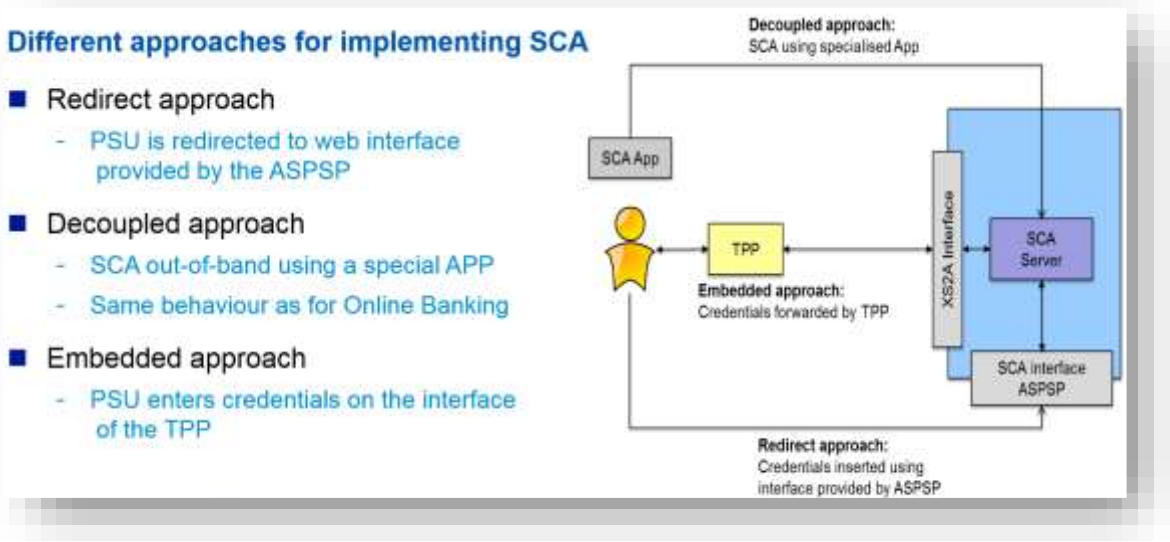
- Get confirmation on the availability of funds

Various

- Full multicurrency support of accounts
- Support of card transactions accounts
- Dedicated consent API separating consent handling from account access
- Extensible with additional extensions for (non-core PSD2) value-add services

NextGenPSD2 – Authentication, authorisation and consent

- Strong Customer Authentication (SCA) models
  - Redirect
  - Decoupled
  - Embedded
  - OAuth2



- Multilevel SCA approach for corporates, e.g. to support 4-eyes principle

- Signing baskets as signing vehicles for grouped transactions
  (instead of multiple payments functions)

Architecture characteristics

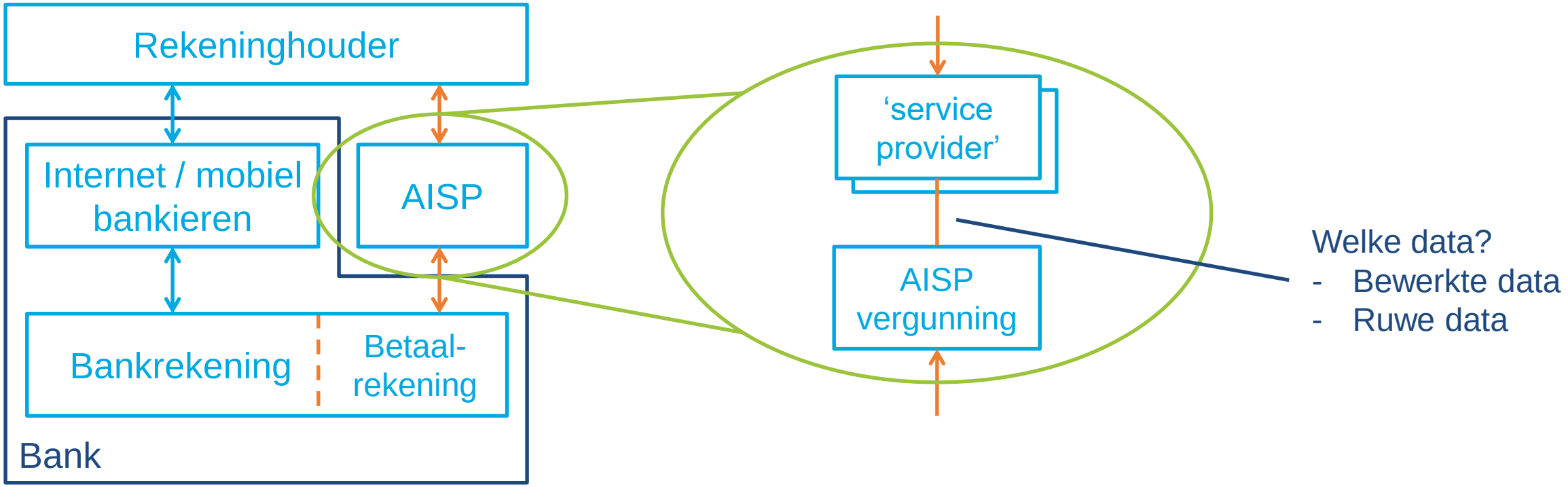
- RESTful API set
- HTTP/1.1 with TLS 1.2 (or higher) as transport protocol

- TPP identification by ETSI-defined eIDAS certificates
  - QWACS mandated (easy measure to protect e.g. against DDOS attacks)
  - QSEALS optional for banks

- Session support (set of consecutively executed transactions), subject to appropriate customer consent

- Data structures either as
  - JSON with data model based on ISO 20022, or
  - XML with pain.001 for PISPs and camt.05x for AISPs

Aggregatie-diensten mogelijk?



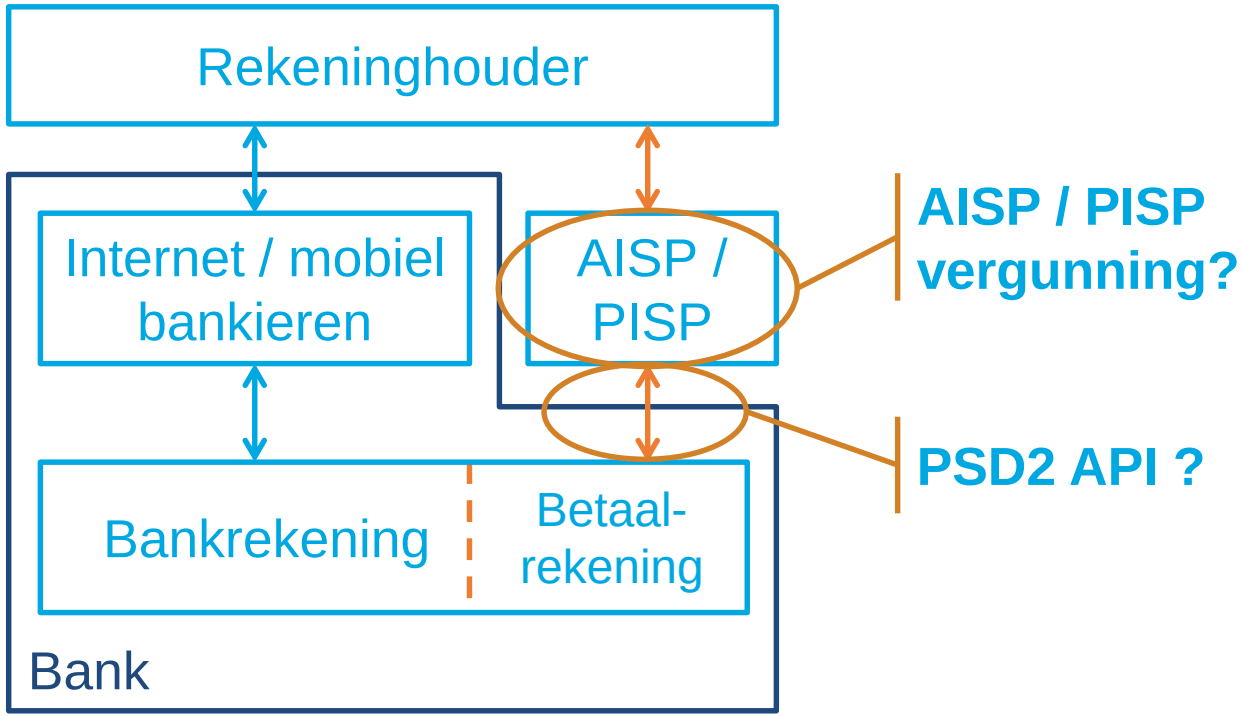
European Banking Authority – Rulebook Q&A

Question ID: 2018_4098

- **Q:** Does a business model where the provider offers a service *sending the account information to third parties* (different from the payment service user) […] constitute the provision of an account information service, *particularly* as it is *not* proposed that the account information obtained will be given *directly to the Payment Service User*?
- **A:** Articles 4(16) and 67(1),(2) PSD2 do not require that the account information service provider (AISP) provides the consolidated information to the payment service user (PSU) in order for the service to constitute an 'account information service' according to PSD2. The *AISP may therefore transmit the consolidated information to a third party with the PSU's explicit agreement.* Regarding the use made by any third party of the consolidated information transmitted, other provisions of EU law may apply, for instance the General Data Protection Regulation (EU) 2016/679 (GDPR).
- **Disclaimer:** […] only the Court of Justice of the European Union can provide definitive interpretations of EU legislation […]

https://eba.europa.eu/single-rule-book-qa

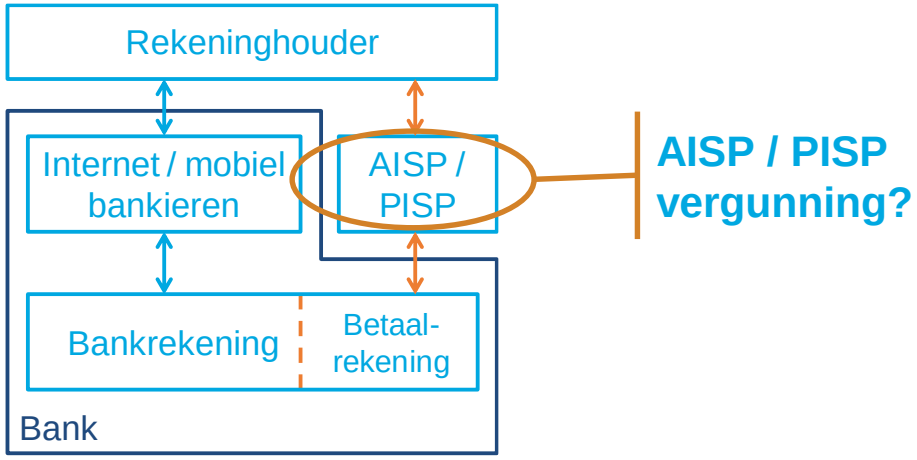
Noodzaak AISP / PISP vergunning en gebruik PSD2 APIs



Wanneer heeft ‘derde partij’ een PSD2 vergunning nodig?

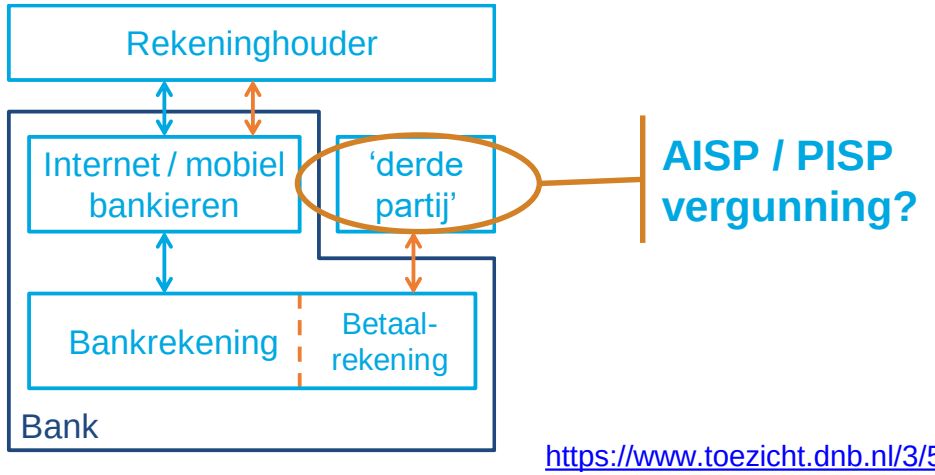
WEL

Rekeninghouder vraagt ‘derde partij’ om namens hem gegevens bij zijn bank op te halen en te bewerken of een betaling te initiëren zonder dat de rekeninghouder zijn bank daarover informeert en/of daartoe opdracht of toestemming geeft.



NIET

Rekeninghouder verzoekt zijn bank aan een derde partij betaalgegevens te verstrekken of deze te mandateren betalingen te verrichten?
De bank bepaalt zelf of zij deze dienstverlening aan niet-vergunningplichtige derde partijen wil verrichten.



https://www.toezicht.dnb.nl/3/50-237764.jsp

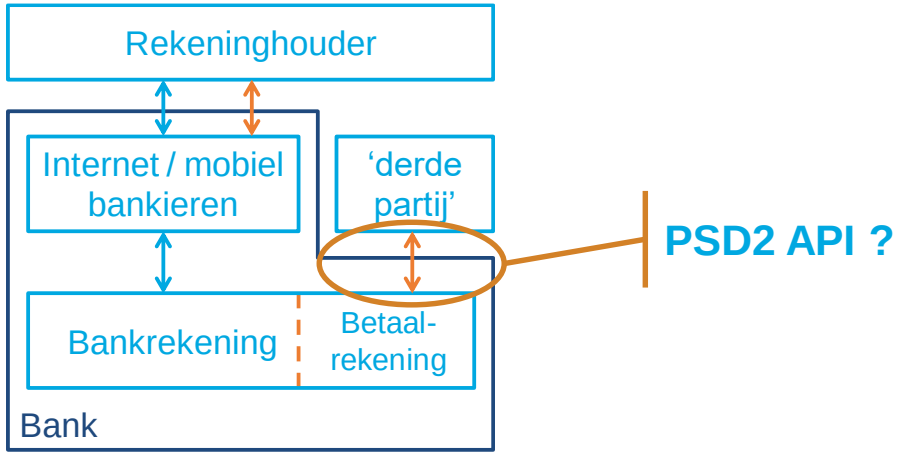
Mag de bank gebruik maken van de PSD2 API?

Betaalvereniging Nederland

JA

Het staat de bank vrij om de wijze van communiceren te kiezen met de derde partij waar de bank op verzoek van de klant mee koppelt.

De bank kan daarbij onder haar eigen verantwoordelijkheid een speciale (technische) koppeling gebruiken. Daarbij mag gebruik gemaakt worden van de in het kader van PSD2 ontwikkelde API (technische koppeling).



https://www.toezicht.dnb.nl/3/50-237764.jsp