NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Home Nieuws Over NOREA Activiteiten

Kennisgroep Betalingsverkeer

How to audit PSD2?

Hans Koster / Frank Waatjes

IIA Nederland

2000-year old roads predict modern-day prosperity

The Romans built roads to all parts of the Roman Empire.

This resulted in larger farms and more trade between agricultural areas and cities.
Roads such as the Via Appia had a major influence on the layout of the landscape around them.

Two-thousand-year-old investments in Roman roads thus determine the current distribution of wealth in Europe.

Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

PSD2 – Why is it relevant?

Article 5

The continued development of an integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.

- Lisbon
- SEPA
- PSD
- PSD2

What developments do you, as an auditor, see regarding payments?

Source: NOREA-webinar 'Developments in payment transactions' (8 October 2020)

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

Payment Services Directive 2 (PSD2)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=NL

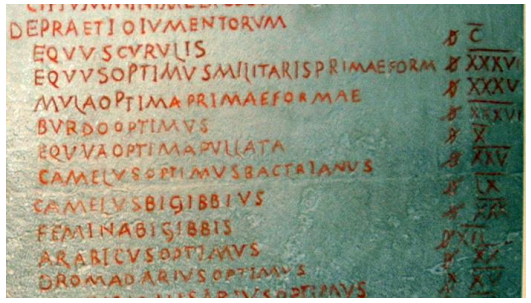
Article 32 Payment initiation services are based on direct or indirect access for the payment initiation service provider to the payer's account. An account servicing payment service provider which provides a mechanism for indirect access should also allow direct access for the payment initiation service providers.

Article 93 The payment initiation service providers and the account information service providers on the one hand and the account servicing payment service provider on the other, should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards.

Article 107 In order to ensure consistent application of this Directive, the Commission should be able to rely on the expertise and support of EBA, which should have the task of elaborating guidelines and preparing draft regulatory technical standards on security aspects of payment services in particular with regard to strong customer authentication.

Article 95 "Management of operational and security risks"

Article 98 "Regulatory technical standards on authentication and communication".



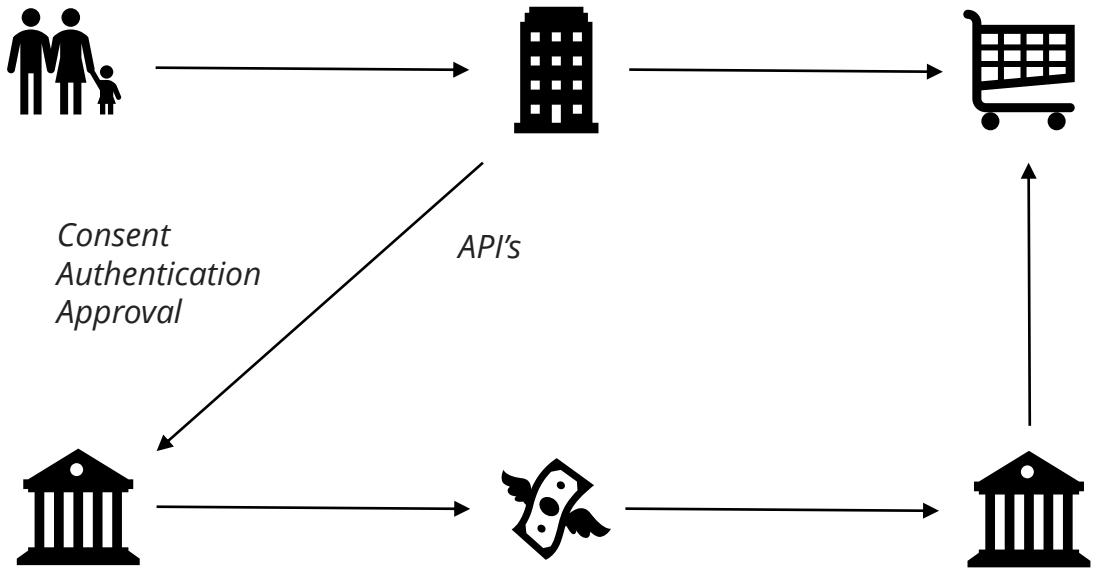
Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

PSD2 Parties

Third Party Payment Initiation Service Providers (PISP's)

Third Party Account Information Service Providers (AISP's)



Account Servicing Payment Services Providers (ASPSP)

Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

Authentication

(4.30) Strong user authentication

two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is)

that are independent, in that the breach of one does not compromise the reliability of the others

(97) 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;

..and..

'also when the information is requested through an account information service provider'

'dynamically link the transaction to a specific amount and a specific payee'

Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

Can you fulfil the required PSD2 audit responsibilities?

- Regulatory technical standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC)
- Final report on EBA Guidelines on the security measures for operational and security risks under PSD2
- Final Guidelines on ICT and security risk management (2020)
- Exemption from the contingency mechanism
- Guidelines on major incidents reporting under PSD2
- EBA guidelines on fraud reporting under PSD2
- Opinion on the use of eIDAS certificates under the Regulatory Technical Standards (RTS) on Strong Customer Authentication and Common and Secure Communication (SCA&CSC).

https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2

And now we that know this… how can we audit PSD2?

Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

NOREA/NVB/Betaalvereniging Consulation paper

- During several meetings in April – June 2019 representatives of NOREA, Betaalvereniging, Nederlandse Vereniging van Banken (NVB) and several Dutch Banks discussed the required audit approach for PSD2.
- In this consultation paper you find our conclusions and recommendations.
- The goal of this consultation paper is to gather feedback which will be used for further improvement of a proposed audit approach for PSD2.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Betaalvereniging Nederland

Nederlandse Vereniging van Banken

IIA Nederland

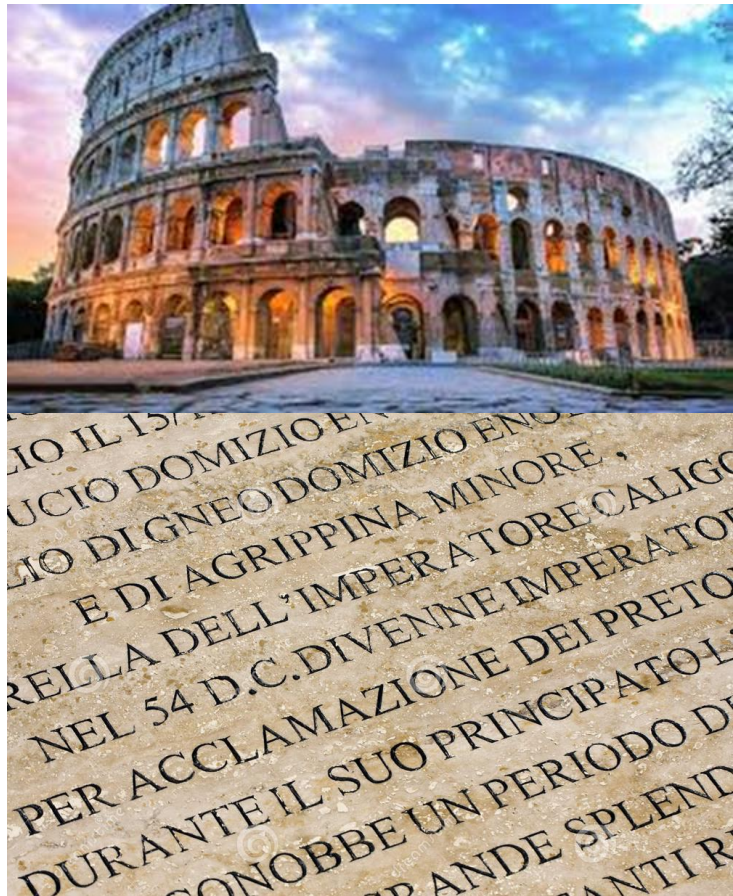
EBA Guidelines on ICT and security risk management

3.3.6. Audit

25. A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

26. A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.

27. A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.



RTS SCA – “Regulatory technical standards for strong customer authentication and common and secure open standards of communication”
Article 3 Review of the security measures

1. The implementation of the security measures shall be documented, periodically tested, evaluated and audited in accordance with the applicable legal framework of the payment service provider by auditors with expertise in IT security and payments and operationally independent within or from the payment service provider.

2. The period between the audits referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider. (note; except article 18 ‘exemption’ is applicable)

3. This audit shall present an evaluation and report on the compliance of the payment service provider's security measures with the requirements set out in this Regulation. The entire report shall be made available to competent authorities upon their request.

Recommendations

- Recommendation 1: The auditor should frequently (at least yearly) make a risk assessment of the PSD2 environment.
- Recommendation 2: The auditor will use the standard control matrix PSD2 (see Annex) for risk assessment and planning purposes. Underlying idea of using the control matrix PSD2 is that the potential large amount of required PSD2 audit activities is executed in the most efficient and effective way.
- Recommendation 3: The auditor yearly will make an overview of the audit activities performed and audit results based on the Control matrix PSD2 structure.
- See separate attachment Control matrix PSD2_meeting 17 June.

Control matrix PSD2 – example of lines

Art. 4 (1) - authentication code	Multi-factor authentication	Authentication is based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.	An exposed element can lead to a higher risk of unauthorized transactions and fraude.
Art. 4 (2) - authentication code	Security measures	Disclosure of the authentication code will not cause any derivation of 1 of the authentication elements (knowledge, possession and inherence).	If elements of strong customer authentication are used by unauthorised parties, there is a risk of decreased or breached security. This can lead to unauthorized payments or fraud.
Art. 4 (2) - authentication code	Security measures	It is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated.	If elements of strong customer authentication are used by unauthorised parties, there is a risk of decreased or breached security. This can lead to unauthorized payments or fraud.
Art. 4 (2) - authentication code	Security measures	The authentication code cannot be forged.	If elements of strong customer authentication are used by unauthorised parties, there is a risk of decreased or breached security. This can lead to unauthorized payments or fraud.

Control matrix PSD2

- Control matrix fields to be filled in by the auditor during the PSD2 audit are:
  - As part of the planning phase:
    - Application landscape
    - Residual risk
    - Coverage Type, 6 defined types: ‘Low risk, no audit’, 2LoD, Continuous Business Monitoring, Re-use of other audit results, Sample based, 3 yearly
  - As part of the audit execution and reporting phase:
    - Comply or Explain
    - Audit activities performed
    - Audit result

PSD2 Landscape

API Gateway

API platform

API security

Consent database

PSD2 shared services

Payment Initiation Services (PIS)

Account Information Services (AIS)

Confirmation Availability of Funds (CAF)

Local Delivery

Back-end systems

Local login

PSD2 services

Which audits in which phase?

- Project Management audit on PSD2 Projects
- Pre- and post implementation audits
- Audits on PSD2 central and local solutions
- Regulatory technical standards for strong customer authentication and common and secure open standards of communication
- Other standards

Future of PSD2?

IIA Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

PSD2 in the media

Date	Topic header
top news	
10 jun 15:02	EBA publishes final revised Guidelines on major incident reporting under PSD2
8 jun 14:00	Excessive Transaction Friction Costing European eCommerce €12 Billion; Riskified Report Identifies
1 jun 12:09	Visa Expands Investment In LoginID — And Authenticated Payments' Future
this quarter	
1 sep 10:54	equensWorldline: agreement with ecolytiq to estimate the sustainability of purchases
26 aug 12:32	The 8 benefits that Big Data brings to financial sector transactions
25 aug 16:30	How banks can help optimize your customer journey
25 aug 14:19	The power of authentication, or how to protect yourself from hackers?
25 aug 10:30	Will open banking be a global success?
25 aug 03:18	Open Banking: The new global standard?
25 aug 02:15	PSD2 – trend break in banking services
25 aug 02:15	Speech Inge van Dijk - "Experiences with PSD2 and open banking: what's next?"
25 aug 02:15	Results of the MOB meeting November 27, 2019
24 aug 15:55	The Limits of SCA and Why Fraud Protection Is More Important Than Ever
24 aug 13:49	Fintech Xelo wants to simplify the payment and authorization scheme. Janusz Diemko announces a revolution - PRNews.pl
23 aug 18:06	Cash Software integrates accounting and banking via PSD2
23 aug 15:13	Analysis: what is #PSD2 and how does it work'
18 aug 10:49	Press release: Jortt introduces new accounting portal

Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

Connecting the dots

Connecting the dots…

New opportunities (or threats?)

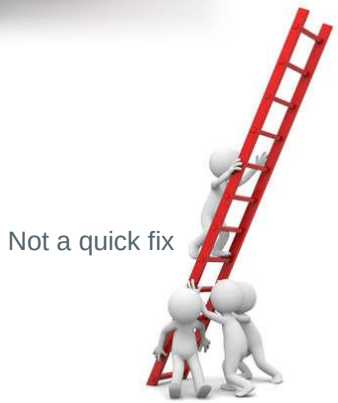
New requirements

Must do

Co-operation business, functions, audit

Sufficient Steering

Better risk monitoring



Not a quick fix

Structured approach

Stay up-to-date

Questions?
Thank you!

Do you want to drive PSD2?

hans.koster@nl.abnamro.com
https://www.norea.nl/handreikingen

IIA Nederland

IIA CONGRES
REINVENT & RECONNECT
16 & 17 SEPTEMBER 2021

Update PSD2 en actuele trends

Ontwikkelingen in het betalingsverkeer

Interessante video:
https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/magazine/4-payment-trends-future

Bron: DNB 2021

Ontwikkelingen in het betalingsverkeer

McKinsey & Company

Global Banking & Securities

Global payments 2021: Transformation amid turbulent undercurrents

The global payments sector is poised for a quick return to healthy growth, but the benefits will not flow evenly to all participants.

https://www.mckinsey.com/industries/financial-services/our-insights/the-2021-mckinsey-global-payments-report?cid=other-eml-dre-mip-mck&hlkid=d83e5072892e4a60b897cd3ef6fa7cb5&hctky=2351249&hdpid=7df07916-33d4-4b0f-971f-6c463715d149

Bron: McKinsey oktober 2021

Ontwikkelingen in het betalingsverkeer

Looking forward, we see a handful of primary drivers influencing the payments revenue trajectory. On the one hand, continued cash displacement and a return to global economic growth will accelerate existing upward trends in the share and number of electronic transactions. On the other, interest margins will likely remain muted. Sustained softness in this key topline contributor will create greater incentive for payments players to pursue new fee-driven revenue sources and to expand beyond their traditional focus to adjacent areas such as commerce facilitation and identity services.

We expect pressure on both fee and processing margins to continue in many regions, while recovery in interest margins is expected to be slow and moderate at best. These combined forces disproportionally affect incumbent players reliant on traditional revenue streams, such as card issuers and banks holding significant commercial and consumer deposit balances, and thus spur a need to rethink payments revenue models and identify alternative paths to value.

The pandemic reinforced major shifts in payments behavior: declining cash usage, migration from in-store to online commerce, adoption of instant payments. These shifts create new opportunities for payments players; however, it is unclear which are

Regulators in countries with dramatic reductions in cash usage are preparing strategies to ensure continued availability of central bank currency and access to resilient and free payments systems for all—including the un- and underbanked. The situation is driving heightened interest in central bank digital currencies (CBDCs), as discussed in

Bron: McKinsey oktober 2021

Ontwikkelingen in het betalingsverkeer

CONTENTS

Ontwikkelingen in het betalingsverkeer

Next-gen payments to drive the growth

After eight years of double-digit growth, global non-cash transactions volume growth decelerated to 7.8% in 2020, reaching 785 billion transactions. We estimate global non-cash transactions growth to rebound to 18.6% CAGR (2020–2025F) and volumes to reach 1.8 trillion by the end of the forecast period. Increasing use of next-gen payment methods – buy now, pay later (BNPL), invisible, biometric, and cryptocurrency – will play a pivotal role in driving the growth.

Payments 4.X is here – buckle up for the new era in payments

The report explores Payments 4.X – an evolutionary, COVID-19-sparked era that's witnessing even more industry consolidation and attracting tech-expert ecosystem players. As part of this phase, expect Payments to become an enabling function that is embedded and sustainable to provide an immersive, seamless, and frictionless customer eXperience. New-age players already exemplify Payments 4.X competencies, while traditional banks seek to maintain positioning by bolstering API maturity, data analytics strength, and processing efficiency.

Regulators support a collaborative ecosystem

In 2020–21, regulators took a balanced approach to key regulatory and industry initiatives (KRIIs) categories – paving the way for a collaborative open finance future. KRII trajectory is drifting towards effectiveness, fostering FIs to collaborate with FinTechs, PayTechs, and peers to share compliance burdens, launch pan-regional initiatives, and to industrialize investments. While it is too soon to count on nascent central bank digital currency (CBDC), it is moving towards reality – urging firms to be ready to act.

https://worldpaymentsreport.com/#

Bron: Capgemini 12 oktober 2021

Ontwikkelingen in betalingsverkeer

- Opkomst van crypto currencies
- Ontwikkeling Central Bank Digital Currencies (CBDC)
- Opkomst bigtechs in betalingsverkeer
- Afnemend gebruik cash geld
- Innovaties in betalen en bankieren
- Betalingsverkeer statistieken in Nederland
- Nieuwe betaalvormen (o.a. iDEAL 2.0, mobile payments en contactloos betalen)

Ontwikkelingen in het betalingsverkeer

Weet u het?