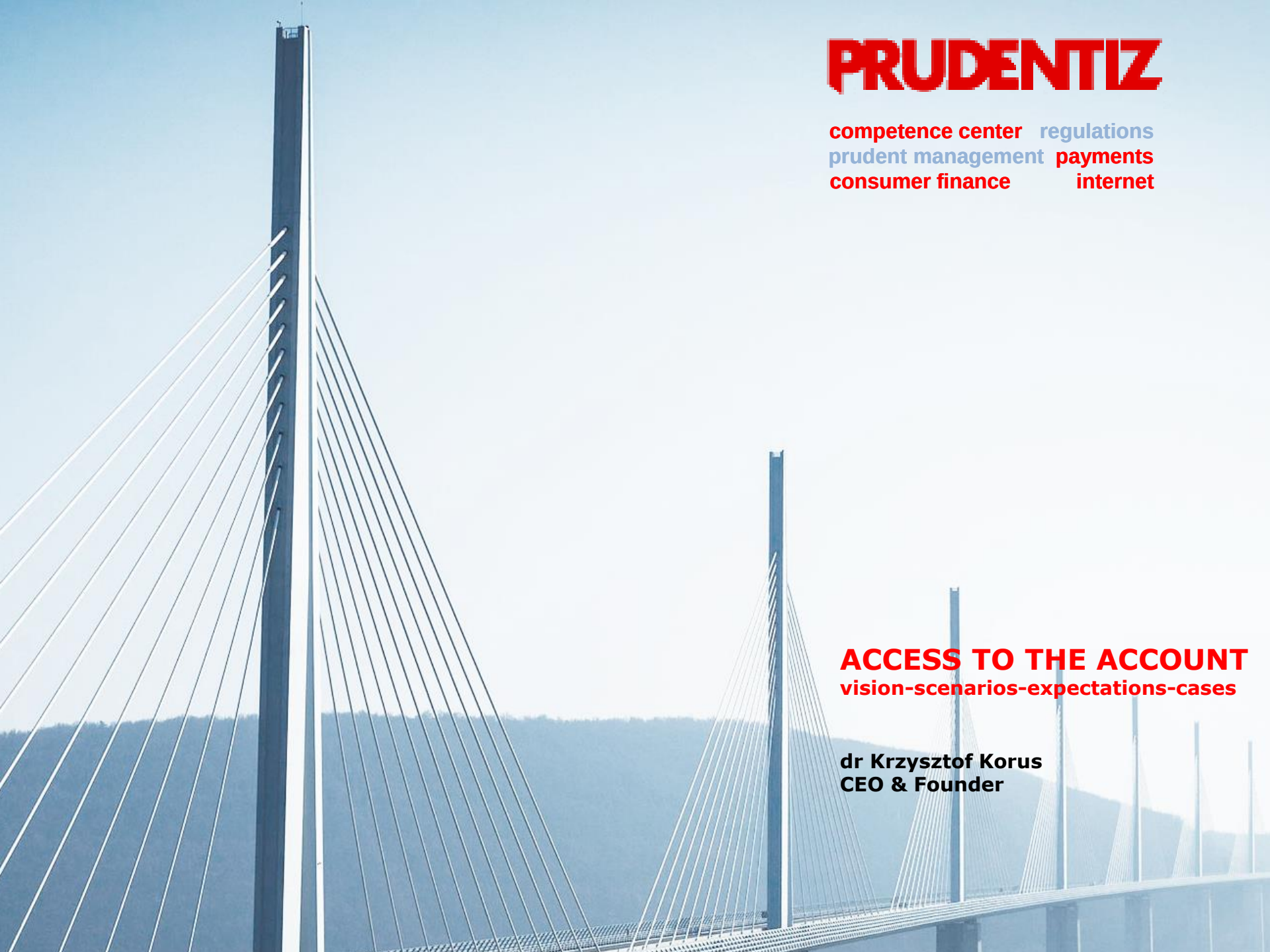

PRUDENTIZ

competence center regulations
prudent management payments
consumer finance internet

ACCESS TO THE ACCOUNT

vision-scenarios-expectations-cases

dr Krzysztof Korus
CEO & Founder

XS2A: current state of play

- CT-OBeP-XS2A
- paradigms-dilemmas-PSD II

OBeP provider approach

PIS approach

outlook 1/3/7 years

PRUDENTIZ

member of epca

agenda

	CT payingpal	OBeP shoppingpal	XS2A xpal?
service	blind CIT	shopping	
underlying trx	no engagement	substantial engagement	
Relation to merchant	MER PSP in the same scheme		
effort re merchant	never contacted merchant before knows merchant if and insofar user tells communication only via ACH	was at merchant's place before customer knows merchant better than customer direct dedicated communication channel to merchant	
merchant readyiness to release merchandise for digits	none	OK	
fees	low, transparent, easy calculable, unitcost prevailing (single CIT fare ~public utility costs)	high, complicated mechanism (efficiency loss), overheads prevailing (subscription)	

	CT payingpal	OBeP Shoppingpal	XS2A xpal?
front	bank	scheme/provider impacted by bank	PIS
backoffice	bank	bank	bank
costs	payer	payee	payer
integration	none (H2M)	bank –OBeP-MER	XS2A – MER
bank >> MER	ACH	OBeP, ACH	ACH
bank feed	user H2M generic access point	M2M payment specific access point	User H2M>>M2M generic >>specific
fee structure	none or H2M	rev share from MER	

XS2A: current state of play

- CT-OBeP-XS2A
- **paradigms**-dilemmas-PSD II

OBeP provider approach

PIS approach

outlook 1/3/7 years

PRUDENTIZ

member of epca

agenda

	paradigm	consequence
HB	• substitute to branch visit with full user verification	• user saves time and costs so unfriendly interface is ok
NonF2F risk	• nobody knows what happenned (except fraudster)	• neither bank nor user can prove the exact failure/fault of the other • ok, then let the bank stand up first (repartition capability); even if authentication all right • but if situation / user not crystal clear (first doubt - correlation) then user stands in regardless causation • **Pay vs compensate** • **Bank chooses the credentials and can refuse if they are absent, but they are never decisive, so they are only 1st level screening (to sort out less smart fraudsters or perhaps event only no to mix orders from 2 different users)**
in lieu	• regular in lieu only if pre-authorized by ASPSP	• utility provider - binding and legal where direct debit • merchant – binding and legal where card • spouse in ATM – binding and illegal if same card • TPP – binding and illegal

	CT	DD	spouse ATM [private in lieu]		TPP [industrial in lieu]	
bank must accept [authorized/confirmed]	+	+	-		-	
user must pay [authorized/confirmed]	+	+	+		+	
bank must provide evidence beyond recording the use of payment instrument	+	+	+	+	+?	+?
user must compensate [user questions 2nd trx]	-	-	fraud	security failure	fraud	security failure
			+	+	+	+

PRUDENTIZ
member of epca

paradigms

	CT	DD	spouse ATM [private in lieu]		TPP [industrial in lieu]	
bank must accept [authorized/confirmed]	+	+	-		-	
user must pay [authorized/confirmed]	+	+	+		+	
bank must provide evidence beyond recording the use of payment instrument	+	+	+ [ale wystarczy że wykaże żonę, czy musi wykazywać co robiła żona?]		+ [ale wystarczy że wykaże TPP, czy musi wykazywać co robił TPP?]	
user must compensate [user questions 2nd trx] Ogólnie: celem jest żeby danie kluczyków do samochodu mającego AC facetowi z myjni nie wygaszało AC gdy on otrze auto albo odjedzie w siną dal] TPP przymusowo insourcerem banku?	-	-	fraud	security failure	fraud	security failure
			+	+ [even if she was more careful than me?]	+	+ [even if she was more careful than me? So even if that was really diligent?

XS2A: current state of play

- CT-OBeP-XS2A
- paradigms-**dilemmas**-PSD II

OBeP provider approach

PIS approach

outlook 1/3/7 years

dilemma	why
in lieu generally allowed?	**You will be able to do not so much as today but do not need to migrate to ideal**
ASPSP needs to be aware who's behind (user or in lieu)?	• **How?** • **What if ASPSP does not respect the method adopted?**
TPP participates in ASPSP costs?	
how to allocate the risk of TPP fraud/failure?	**Who is the primary respondent (and the final one if non liquet)? Needs to provide evidence beyond obtaining payment order from TPP? How? Has no way to do so. Unspoken TPPs duty to provide this evidence, enforceable by the ASPSP against TPP despite contract (ex lege claim)? TPP has to secure this evidence, if not then liable for questionned trx?** **What if TPP used by fraudster and none (ASPSP and TPP) could identify fraud? What if TPP could easier identify irregularity?**
new risks?	• phishing via merchants (more easy – immediately feasible becasue takes longer folks to realize that did not get the merchandise despite payment) / TPP (less possible for immediate use – merchants control flows very strictly and block TPP next after payment due; more prone to long term, ie first payment ok, data store and in few months the real fraud) • limited because of uncertainty (merchants limited drive, customers limited adoption) – folks tend to think too much before using and every effort has discouraging effect; not enough attractive to fraudsters • once acknowledged folks tend to trust generally, especially if merchants

XS2A: current state of play

- CT-OBeP-XS2A
- paradigms-dilemmas-**PSD II**

OBeP provider approach

PIS approach

outlook 1/3/7 years

issue	approach	
in lieu	only credible	
TPP credibility	authorisation - supervision – indemnity (#trx/#users)- public register	
funds possession	prohibited	ACQ+PIS?
user data	may get user data must not make accessible to 3rd parties (guaranteed by credibility)	
positioning	R18: **comfort** (not service?) to payee A58: payees who offer to payers [] making use of 3rdPPSP [EP] A58: **payer** has the right to make use […] A58: this is „payer's" funds (not „payee's") A39: PIS shall provide or make available to the **payer and the payee** A58: **communicate with ASPSP, the payer and the payee** in a secure way	„on behalf"? „where applicable [to] the payee"
user's right	A58: **payer has the right** to make use […] A61: terms [] use of the payment instrument [] **objective, non-discriminatory** and proportionate A60: deny access [..] for objectively justified [] related to **unauthorised or fraudulent []** A58: treat orders [] **without any discrimination**, [] timing, priority or charges vis-à-vis [] transmitted directly, unless objectively justified	„objective reasons/justification"

PRUDENTIZ

member of epca

PSD II approach – act of faith

issue	approach	
authorisation	A57 Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider.	„shall be considered given" [EP]
credentials	A87 ASPSP **ALLOWS** PISP/AISP to rely on the authentication procedures provided by the ASPSP to PSU. R18 The personalised security credentials used for secure customer authentication either directly by the payment service user **[PIS]** or the payment initiation service provider **[OBEP]** are usually those issued by the account servicing payment service providers.	
introduction	A58 PIS shall [] authenticate itself towards the ASPSP	
communication	A58 PIS [] communicate with the ASPSP, the payer and the payee in a secure way, in accordance with Article 87a.1.d; A58 ASPSP shall [] provide facilities to securely communicate with payment initiation service providers in accordance with Article 87a.1.d; A87a.1.d EBA shall [] develop draft regulatory technical standards addressed to PSP [] common and secure requirements for communication for the purpose of authentication, notification and information between account servicing payment service providers, payment initiation service providers, account information service providers, payers and payees. R51 EBA shall, inter alia, define the features of a standardized protocol or interface [] this standardized protocol or interface should also be used to transmit the authentication codes which demonstrate the consent given by the payer to the PISP/AISP to access the payer's payment account and be properly informed about the extent of this access.	
contract	R18 The payment initiation service providers do not necessarily enter into contractual relation with the account servicing payment service providers.	• EP „no contract required"

issue	approach	
„own system"	A40 Where a payment order is initiated by the third party payment service provider's own system,	[EP]
Initiation	A58 ASPSP [] provide information on the initiation of the payment transaction to the PISP	
SCA	A87 **PSP [ALL!]** apply strong customer authentication [incl. specific security requirements, to protect the confidentiality and the integrity of the payment service users' personalised security credentials; applies also when payments are initiated via PIS] when the payer (a) accesses his payment account on-line; (b) initiates an electronic remote payment transaction (elements dynamically linking the transaction to a specific amount and a specific payee – applies also when payments are initiated via PIS) R51a Encryption systems which may result in authentication codes such as one-time passwords are able to enhance the security of payment transactions; the use of such authentication codes by payment service users shall be considered to be compatible with their obligations in relation to payment instruments and personalized security credentials also when payment initiation service providers or account information service providers are involved.	
Transitory period	R18 . This raises a series of legal issues, such as consumer protection, security and liability as well as **competition** and data protection issues. The new rules should therefore respond to those issues. These rules aim at **guaranteeing continuity** in the market, enabling existing and new service providers to offer their services under a clear and harmonized regulatory framework R18 Pending the application of these rules, without prejudice to the need to ensure the security of payment transactions and customer protection against demonstrable risk of fraud, Member States and the Commission , **should guarantee fair competition** in this market **avoiding unjustifiable discrimination against any existing player** on the market.	

issue	approach	
Liability unauthorized	A65 If the PISP is liable for the unauthorised payment transaction, it shall immediately compensate the ASPSP at its request for any losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction.	Not Securing evidence beyond record = liable? EP: PISP cannot prove that not liable compensate D+1
Liabilit correctness	A80 If the payment initiation service provider is liable for the incorrect execution of the payment transaction, it shall immediately compensate the account servicing payment service provider at its request for any losses incurred or sums paid as a result of the refund to the payer. The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Article 69.	• EP,EC: PISP liable to the payer

XS2A: current state of play

- CT-OBeP-XS2A
- paradigms-challenges-PSD II

OBeP provider approach

PIS approach

outlook 1/3/7 years

k.korus@prudentiz.eu | prudentiz.eu

@dlklegal