PSD2 CHEAT SHEET

callsign

Payer - natural or legal
AISP (Account aggregation)
PISP (Payment initiation)
ASPSP (Bank, Blockchain? etc.)

Authentication Request
- Data access (AISP, IB)
- Create/change SCA
- Individual payment
- Create regular payment
- Batch payment

Excluded from PSD2
Payments as charges to telco bill
Limited network gift or fuel cards
Commercial agents

?

Low risk

Association with User ID, Activation and Renewal of SCA elements performed using SCA

- Secure Execution Environment on multi-purpose device
- Detection and mitigation of device or software alteration
- Ensure confidentiality, authenticity and integrity
- Mitigate risk of disclosure (masking, crypto etc.)
- Mitigate risks of loss, theft, copy prior to credential delivery
- Mitigate misdirection of communication
- Uniquely identified sessions
- Detailed time-synced logging

Strong Customer Authentication

- Must have 2 out of 3 elements:
  - Knowledge (Something you know)
  - Possession (Something you have)
  - Inherence (Something you are)
  - Elements must be independent
- Language specific interface
- For Cards: no SCA elements readable by any staff at any time

Authentication Code and Dynamic Linking

- Payer is aware of payee and amount
- Authentication code specific to payee(s) and total amount
- Authentication code related to consented amount to be blocked on card
- One time authentication code
- Not derivable to/from SCA elements
- Protected against fraudulent code
- Not possible to generate from previous code
- For cards: Authentication codes not readable by any staff at any time

Key Dates:
- **01/18:** PSD2 in force
- **02/18:** Reg Tech Standards (RTS)
- **03/19:** TPP test environments
- **09/19:** SCA in force

- Limit of 5 mins of no activity
- Inform customer if blocked
- Provide method to unblock

Authentication Response

OR

Low Risk Activity

- Access in order to view:
  1. Balance of designated accounts
  2. Payment transactions for last 90 days (but not first time access or if last SCA > 90 days ago)
- Unattended terminals for transport and parking fares
- Anonymous payment instruments

Low risk Payments	Contactless	Electronic Payments
Individual Amount	<= €50	<= €30
Cumulative since SCA	<= €150	<= €100
Consecutive since SCA	<= 5	<= 5

OR

Trusted Beneficiary

Applies to:
- Individual payment
- Create, amend or initiate regular payments of same amount

Previously created/confirmed via ASPSP
CT between same person at same ASPSP

Dedicated Corporate Payments

Corporate transactions via a dedicated SCA equivalent process or protocol

OR

Transaction Risk Analysis (TRA)

- Real-time risk analysis
- Detect unauthorized or fraudulent payment transactions
- Take into account normal use for user in the circumstances
- At a minimum, must take into account:
  - List of compromised/stolen authentication elements
  - Amount of the payment transactions
  - Known fraud scenarios
  - Signs of malware in any sessions of authentication procedure
  - Abnormal device usage
- Plus for SCA exemption:
  - Previous spending patterns for user
  - Payment transaction history of PSP user
  - Location of payer and payee if access to device/software is provided by the PSP
  - Abnormal user behavioral payment patterns versus history
  - Abnormal use of access device or software provided by PSP
  - Proximity of payee to payer (under investigation)
- Amount does not exceed **Exemption Threshold Value (ETV)**

Low risk level Checklist

No abnormal spending or behavioral pattern
No unusual information about the payers device or software
No malware in an session of the authentication procedure
No known fraud scenario identified
Location for payer is normal
Location of payee is not identified as high risk

1st and 3rd Party € Gross Fraud / € all transactions rolling 90 days	Remote Card	Remote Credit Transfer
ETV €500	0.01%	0.005%
ETV €250	0.06%	0.01%
ETV €100	0.13%	0.015%

Reported to National Authorities and European Banking Authority (EBA)

SCA reintroduced if over ETV for 2 consecutive quarters