PSD2 SCA Migration PMO

Detailed KPI Definitions, Common Root-Causes & Solutions

Version: March 17, 2021

Authentication & Authorization KPIs for *Acquirers, 3DS servers & Merchants* (I/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix

Authentication	1	EMV 3DS Error Rate	Rate of which authentication requests or result responses from the 3DS server are rejected by directory server (Looking at AReq and RRes)	- 3DS server is passing on inaccurate merchant data without checking. In most cases;
				  - Cardholder name includes special characters
				  - Shipping address & billing address has incorrect definition of field presence conditions (the field shouldn't exist or should have 'NULL' value)
				- Error can be solved permanently if 3DS server converts incorrect data to correct data or it will re-appear each time a new merchant enrolls
					3DS server needs to convert the data from merchants
					
					- **Permanent fix:** 3DS server implements a fix to convert all incoming data from merchants – apprx. take a few weeks
					- **Temporary fix:** 3DS server communucates with merchant and merchant corrects the data – a lot of trx are lost in the meantime
						Mid-term (Weeks)

	2	Missing Merchant Registration	Rate of which merchant identification is missing from a transaction	- Authentication request is presented for a merchant ID that has not been registreed - Typically takes long time to fix; and a lot of trx are lost in the meantime - There is a confusion of error ownership between 3 acq. parties and the party who should fix it	- **Ideal fix:** Each time 3DS server adds a new merchant, they request merchant to check whether they are registered or not with their acquirer - Acquirer registers acquirer BIN and merchant ID	Short/Mid-term (Days/weeks)

Authentication & Authorization KPIs for *Acquirers, 3DS servers & Merchants* (II/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authentication	3	Challenge Cancelation 4 Rate *by App*	Rate of challange flow cancellation caused by an error in one of the challenge messages	Challange request/response is being rejected causing a time-out in the whole process due to: - **Technical issues:** There could be an error on app trx flow - **UX issues**: Issuer could be facing a technical problem in user interface or the UX flow may be confusing to the cardholder in the way it's implemented - **Abandonment issues:** Cardholder may be abandoning the process due to lack of education	Process needs to be monitored to identify the exact problem with persistent testing - **Technical solutions:** 3DS Server should check with SDK to understand whether there are any issues on challenge flows - **UX and abandonment solutions:** Easier to address from the issuing side	Mid/long-term **- Technical fix:** Analysis to determine the cause could take long time, fix is quicker **– Another fix:** Takes long time to address
	4	Challenge Cancelation 5 Rate *by App*	Rate of which challenge request is never sent	Merchant abandones the challenge flow due to: - **Technical issues:** There could be an error in CREq which causes ACS to rejects - **SCA strategy of the merchant**	Merchant needs to complete the challenge flow - **Technical solutions:** Merchant should check with ACS to understand if they notice any issues on challenge messages that - **SCA strategy:** Encourage merchant to test at least a portion of their trx so that they are ready when time comes	**- Technical fix**: short-term (days) **- Another fix:** Mid/long-term (weeks, months)

Authentication & Authorization KPIs for *Acquirers, 3DS servers & Merchants* (III/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authentication	5	Challenge Cancelation Rate *by Browser*	Rate of challenge flow cancellation on browser	Challenge flow is being cancelled either by cardholder, by merchant app or by ACS operator *(for more detailed info please refer to KPIs 3&4)*	Process needs to be monitored to identify the exact problem with persistent testing *(for more detailed info please refer to KPIs 3&4)*	Short/long-term (days to months depending on the root-cause)
	6	Merchant Authentication Rate	System Authentication Rate: the merchant receiving either a validation or attempt from DS, over total authentications	Informational only; - Overall indicator of Authentication Performance, driven by all KPIs monitored - There is no single, quick fix - If it is to be improved, the fix mostly lays on the issuer side. Yet, there could be situations where the error is caused by the acquirer side as well i.e., Challenge cancellations		Mid/long-term (weeks/ months)

Authentication & *Authorization* KPIs for *Acquirers, 3DS servers & Merchants* (I/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix

Authorization	15	Incorrect Exemption or Excluded Flagging	Rate of which MIT or recurring exemptions are not flagged correctly in authorization	- Error occurs when merchant sends inaccurate data or hasn't aligned its specifications well with the acquirer
				- **Incorrect authorization specifications:**
				  - Trace ID is missing
				  - The length is incorrect
				  - DE61SE4 has a value of 5 instead of 4 (most common error)
				- **Misalignment on specifications:** Merchant and acquirers haven't covered trx condition well (i.e., the condition doesn't have a definition in the API) in the interface to identify type of trx condition they want to reflect in the transaction
				- **MC specifications are misunderstood or not read**
					- **Trace ID error:** Store trace ID correctly and make sure it is provided when needed
					- **Lenght error:** Make sure to provide the right combination of settlement date and bank net reference no
					- **Misunderstood or misaligned specifications:** Review and correct authorization specifications
						Mid/long-term (weeks/months)

	16	Missing or Wrong DS Transaction ID	Rate of which DS trx ID is missing in authorization messages	DS trx ID field is not carried correctly from authentication to authorization environment by the merchant or the payment gateway. It is either: - **Missing:** Field is not carried from authe to autho environment - **Wrong:** Field value is broken (manipulated) during the flow either by the merchant or payment gateway	- **Missing DS trx ID:** Update the channel between authentication and authorization - **Wrong DS trx ID:** Make sure that when applying conversition, no value is droped or manipulated by the merhcant or payment gateway	Mid/long-term (weeks/months)

Authentication & *Authorization* KPIs for *Acquirers, 3DS servers & Merchants* (II/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	17	OBS AAV 05 invalid	Rate of which On Behalf Service (OBS) 05 service finds that authorization AAV is not valid (3D1 trx are exluded)	- Acquirer includes incorrect AAV - Acquirer damages (manipulates) the AAV value	- Ensure the correct AAV field value from the authentication is inserted into the authorization message - Merchant or the payment gateway is dropping the last bite of the field – ensure complete filed is included	Mid-term (weeks)
	18	OBS AAV 05 result mismatch	Rate of which On Behalf Service (OBS) 05 service finds that trx amount indicated during authorization is mismatching the one indicated during authentication	- Acquirer includes incorrect amount - Acquirer or merchant performs an incorrect value conversion - Merchant authenticates for a higher amount than what is being presented for authorization - Acquirer indicates a different currency than the original trx currency	- Within EEA, merchants and acquirers must ensure that they do not request authorization for an amount that exceeds the authorization amount - Merchants should make sure that acquirer has the correct trx currency info	Mid/long-term (weeks/ months)

Authentication & *Authorization* KPIs for *Acquirers, 3DS servers & Merchants* (III/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	19	Non-compliant transactions	Rate of transactions where acquirers/merchants do not use any exemptions during authorization	The merchant did not go through 3DS (No-3DS with SLI 210 or ID Check Insights with SLI 214) and goes straight to authorization without indicating the reason for not going through SCA in the Low-Risk Merchant Ind. (DE48.22.1) of authorization message	- When authentication does not happen, the merchant/acquirer needs to populate DE48.22.1 in the authorization message - Merchant should ensure to to have the right approach between taking transactions to authentication or straight to authorization	Mid-term (weeks)

Authentication & Authorization KPIs for *Issuers & ACS operators* (I/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authentication	7	EMV 3DS Error Rate	Rate of which authentication response or result requests from the ACS provider are rejected by directory server (Looking at ARes and RReq)	Missing or inaccurate data in key EMV 3DS fields. Examples: - ECI missing/invalid (most common), - Auhtentication value invalid	Review EMV CO & ID Check authentication specifications (may not be implemeted correctly)	Short/mid-term (days/weeks)
	8	ACS EMV 3DS Time-Outs	Rate of which a connection problem between directory server and ACS has occurred (ACS not replying authentication reqest on time - error code 000)	- Connection is not stable & needs to be or insufficient for the volume - ACS provider processing platform doesn not have sufficient capacity for 3ds volume	- Implement monitors to check real-time availability of the connection - Increase resilience of the ACS provider platform (via back-up servers, load balancing, etc.) - Increase the capacity of the connection	Mid/long-term (weeks/months)
	9	ACS Authentication Rate	Rate of successful authentication validations by ACS operator within total authentications sent to ACS	**Low authentication rate:** - Insufficient frictionless authentications - High challenge cancellation rates	- Increase frictionless authentications - Improve challenge success rate - For issuers: Implement 'Smart AuthE Direct'	Long-term (months)

Authentication & Authorization KPIs for *Issuers & ACS operators* (II/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authentication	10	Challenge Success Rate *by App*	Success rate of app initiated trx that aren't exempt (challenged) from SCA requirements	**Not succesful:** Challenge cancellation rate is too high (i.e. Not being sent, being cancelled)	• Improve the challenge flow • Educate cardholder	Long-term (months)
	11	Challenge Success Rate *by Browser*	Success rate of browser initiated trx that aren't exempt (challenged) from SCA requirements	**Not succesful:** Challenge cancellation rate is too high (i.e. Not being sent, being cancelled)	• Improve the challenge flow • Educate cardholder	Long-term (months)
	12	Challenge Cancelation 4 Rate *by App*	Rate of challange flow cancellation caused by an error in one of the challenge messages	Challange request/response is being rejected causing a time-out in the whole process due to: - **Technical issues:** There could be an error on app trx flow - **UX issues**: Issuer could be facing a technical problem in user interface or the UX flow may be confusing to the cardholder in the way it's implemented - **Abandonment issues:** Cardholder may be abandoning the process due to lack of education	Process needs to be monitored to identify the exact problem with persistent testing - **Technical solutions:** ACS should check if they notice any issues on challenge messages; could be rejecting - ACS/Issuer to Test with microsoft or google testing platforms - **UX and abandonment solutions:** issuer should check w cardholder to find out what went wrong – can issuer contact cardholder to understand- i.e.survey	Mid/long-term (weeks/months)

Authentication & Authorization KPIs for *Issuers & ACS operators* (III/III)

	#	KPI Name	Definition	Typical root cause	Typical solutions[1]	Timeline for fix
Authentication	13	Challenge Cancelation 5 Rate *by App*	Rate of which challenge request is never sent	More likely a merchant issue Merchant abandones the challenge flow due to: - **Technical issues:** There could be an error in CREq which causes ACS to rejects - **SCA strategy of the merchant**	Merchant needs to complete the challenge flow - **Technical solutions:** ACS should check if they notice any issues on challenge request messages; it could be rejecting - **SCA strategy:** Encourage merchant to test at least a portion of their trx so that they are ready when time comes	**- Technical fix:** Short/mid-term (days/weeks) **- Another fix:** Mid/long-term (weeks/months)
	14	Challenge Cancelation Rate *by Browser*	Rate of challenge flow cancellation on browser	Challange request/response is being rejected causing a time-out in the whole process due to: - **Technical issues:** There could be an error on browser trx flow - **UX issues**: Issuer could be facing a technical problem in user interface or the UX flow may be confusing to the cardholder in the way it's implemented - **Abandonment issues:** Cardholder may be abandoning the process due to lack of education	Process needs to be monitored to identify the exact problem with persistent testing - **Technical solutions:** Issuer should check with ACS provider to understand whether there are any issues on challenge flows - **UX and abandonment solutions:** Survey cardholder on sample trx to understand why challenge process failed; conduct test trx to see if UX flow is working fine; educate consumers	Mid/long-term **- Technical fix:** Analysis to determine the cause could take long time, fix is quicker **– Another fix:** Takes long time to address

Authentication & *Authorization* KPIs for *Issuers & ACS operators* (I/V)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	20, 22	Issuer exemption decline rate for MIT, RP	Share of issuer exemption decline rates by different transaction types (MIT, RP)	**High decline rate root cause:** 1- Issuer has not implemented acquirer exemption correctly or not supporting it, therefore rejecting 2- Merchant not sending the exemption at a good time, which results in a financial decline	1- Review processes to remove any declines specific to exemptions. Issuers should be supportive of acq exemptions. They should except grandfather trace IDs and should look up original trace IDs to check the initial authentication 2- Merchant needs to review its processes to ensure that at the time of setting up the agreement, the type of product supports the availability of funds; mainly an issue with MIT payments *(merchant side correction)*	Short/ mid-term (days/weeks)
	21, 23	Issuer exemption decline rate for TRA, RP,	Share of issuer exemption decline rates by different transaction types (TRA, LVP)	**High decline rate root cause:** 1- Issuer has not implemented acquirer exemption correctly or not supporting it, therefore rejecting 2- Any reasons for regulation non-compliance must be soft declined	1- Review processes to remove any declines specific to exemptions. Issuers should be supportive of acq exemptions.	Short/ mid-term (days/weeks)

Authentication & *Authorization* KPIs for *Issuers & ACS operators* (II/V)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	24	MIT Financial Decline Δ (fin decline rate: MIT - recurring)	Difference between MIT flagged financial decline rate vs financial decline rate of equivalent recurring payment trx in 2020	1- Average transaction value is higher than before 2- Product is not allowing for sufficient funds	Recommend a product with credit line to cardholder	Long-term (months)
	25	MIT Other Decline Δ (other decline rate: MIT - recurring)	Difference between MIT flagged other decline rate vs other decline rate of equivalent recurring payment trx in 2020	Issuer is less tolerant to transactions with MIT exemption flag; either on purpose or by accident	**1- If by accident:** review the response code provided and course correct **2- If on purpose:** review decisioning policy, presence of flag should not influence the decisioning logic	**By accident:** Short-term (days) **On purpose:** Long-term (months)
	26	RP Financial Decline Δ (fin decline rate: RP - recurring)	Difference between RP flagged financial decline rate vs financial decline rate of equivalent recurring payment trx in 2020	Decisioning logic of issuer changed. It is taking exemption flag into account when deciding to approve or decline	**1- If by accident:** review the response code provided and course correct **2- If on purpose:** review decisioning policy, presence of flag should not influence the decisioning logic	**By accident:** Short-term (days) **On purpose:** Long-term (months)
	27	RP Other Decline Δ (other decline rate: RP - recurring)	Difference between RP flagged other decline rate vs other decline rate of equivalent recurring payment trx in 2020	Issuer is less tolerant to transactions with RP exemption flag; either on purpose or by accident	**1- If by accident:** review the response code provided and course correct **2- If on purpose:** review decisioning policy, presence of flag should not influence the decisioning logic	**By accident:** Short-term (days) **On purpose:** Long-term (months)

Authentication & *Authorization* KPIs for *Issuers & ACS operators* (III/V)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	28	TRA Soft Decline Rate	Rate of soft declines provided on TRA exemptions	**High decline root-cause:** 1- Issuer hasn't implemented regulations for TRA or isn't interpreting the regulation correctly 2- Issuer is using soft declines for reasons other than high risk	Issuer needs to review its decisioning logic: 1- Issuers are allowed to accept acquirer TRA with out applying any issuer TRA 2- Issuer should only apply transaction risk monitoring and only soft decline when risk is preceived high 3- Issuer shouldn't use soft decline if the risk is perceived too high i.e., if the issuer would decline the trx even if it's authenticated	Short/ mid-term (days/weeks)
	29	LVP Soft Decline Rate	Rate of soft declines provided on LVP exemptions	**High decline root-cause:** 1- Issuer is using soft declines for other reasons than the counter (i.e. İnstead of every 6th trx or when total exceeds 100 EUR) *(most common error)* 2- Issuer hasn't implemented regulations for LVP or is not interpreting the regulation correctly 3- Issuer hasn't implemented any counter accumulation yet (no process in place for counting/tracking)	Issuer needs to review its decisioning logic: 1- Issuer should only apply transaction risk monitoring and only soft decline when risk is preceived high 2- Issuer shouldn't use soft decline if the risk is perceived too high i.e., if the issuer would decline the trx even if it's authenticated 3- Issuer could utilize LVP CNP counter program provided by Mastercard	Short/ long-term (days/months) *(MC product shortens resolution process)*

Authentication & *Authorization* KPIs for *Issuers & ACS operators* (IV/V)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	30	Frictionless Soft Decline Rate	Rate of soft declines provided on frictionless authenticated trx	**High decline root-cause:** 1- Issuer is applying authorization risk policy 2- ACS authentication risk policy is not aligned with issuer authorization risk policy 3- Issuer is not capable of detecting frictionless transactions	1- Issuer doesn't need to perform any specific risk monitoring 2- Issuer needs to align its risk policy with ACS 3- Issuer must use the authentication value leading indicator "kA", "kO", and "kR"	Mid/long-term (weeks/months)
	31	Challenged Soft Decline Rate	Rate of soft declines provided on challenged authenticated trx (challenged trx should not be soft declined)	**High decline root-cause:** 1- Issuer is applying authorization risk policy 2- ACS authentication risk policy is not aligned with issuer authorization risk policy 3- Issuer is not capable of detecting challenged transactions	1- Issuer doesn't need to perform any specific risk monitoring 2- Issuer needs to align its risk policy with ACS 3- Issuer must use the authentication value leading indicator "kB" and "kP"	Mid/long-term (weeks/months)
	32	SIRBA Soft Decline Rate	Rate of soft declines provided on SIRBA trx *(trx that are fully authenticated, low risk and below 30 EUR (unless issuer changed the amount))*	**High decline root-cause:** 1- Issuer is not using Mastercard DTI values for risk assesment 2- Issuer is not capable of detecting SIRBA fully authenticated trx 3- Issuer is not taking into account that this is an LVP trx *(unless issuer changed the amount)*	1- Issuers should include DTI score in trx risk monitoring process 2- Issuer must use the authentication value leading indicator "kC" 3- Issuer should apply same decisioning logic as for LVP trx	Mid/long-term (weeks/months)

Authentication & *Authorization* KPIs for *Issuers & ACS operators* (V/V)

	#	KPI Name	Definition	Typical root cause	Typical solutions	Timeline for fix
Authorization	33	Attempt Soft Decline Rate	Rate of soft declines provided on attempt trx *(Trx that are non-low risk or above 30 EUR (unless issuer changed the amount))*	**High decline root-cause:** 1- Issuer is not using Mastercard DTI values for risk assesment 2- Issuer is not capable of detecting attempt trx 3- Issuer is not applying issuer TRA exemption 4- Issuer does not take into account acquirer exemption flags (acquirers can use acquirer exemptions for attempts)	1- Issuer should include DTI score in trx risk monitoring process 2- Issuer must use the authentication value leading indicator "kF" or "kE" 3- Issuer should apply issuer TRA 4- Issuer must take acquirer exemption flags into account	Mid/long-term (weeks/months)
	34	SCA Exemption[1] Soft Decline Rate	Rate of soft declines provided on SCA exempt authenticated trx *(Issuer should also expect an exemption flag in authorization. If acq/ merchant doesn't specify acq exemption in authE, it and needs to repeat in authO)*	**High decline root-cause:** 1- ACS authentication risk policy is not aligned with issuer authorization risk policy 2- Issuer is not capable of detecting exempt transactions 3- Issuer is not capable of dealing with LVP exemptions	1- Issuer needs to align its risk policy with ACS 2- Issuer must use the authentication value leading indicator "kN" 3- Issuer must apply the decisioning logic that corresponds with acq LVP exemption being requested in authorization and **not apply** the decisioning logic with TRA exemption being requested in autho *(If merchant applies LVP exmp, issuer must apply counting as normal LVP. If merchant applies TRA exmp, ACS decision should be taken into account and issuer should accept the trx)*	Mid/long-term (weeks/months)

(1) TRANSACTION WAS NOT AUTHENTICATED EITHER BY ACS OR MASTERCARD AS ACQUIRER SCA EXEMPTION WAS APPLIED
ALL PLAYERS SHOULD REGULARLY CHECK BEST PRACTICES DOCUMENT FOR LATEST UPDATES