POS authorization

Technology stack:

- JWT - https://jwt.io
- TLS
- RSA

Actors:

- POS/CMS operator (as Operator) - person who has access to Admin Panel and physical access to POS device.

Objects:

- Admin Panel - as AP - User web interface interface.
- Point of sell device (payment terminal) - as POS - physical payment terminal device.
- Serial Number - as SN - POS unique serial number printed on a device.
- Pairing code - as Pairing Code - temporary code used to pair terminal into MACS. It contains numbers and it length is 8 characters.

All operations are made using SSL/TLS.

It is mandatory on POS to load correct SSL Trusted CA Certificate (MACS SSL) into parameters file of MACS POS application.

Pairing process:

1. Operator adds POS to a location in AP. Operator must read SN from a POS and provide the SN to AP.
2. On list of terminals in AP, Operator select options for previously added POS and select Get Pairing Code option. The code is generated with TTL=2h and displayed to the Operator.

- Pairing code - is connected with SN - only particular POS (SN) can be paired using generated Pairing Code.
- Operator enter the Pairing Code on POS and initiate paring process.
- POS generates RSA key pair - 2048 Length.

POS sends SN, Pairing Code and Public key(base64 encoded) to MACS pairing endpoint "/pos/pair".

3. MACS check if Pairing Code still exists (it's auto removed after TTL ends) and if match to SN. If so, the public key is decoded, checked and saved next to SN in database.
4. MACS changing status of terminal to "paired".

- Pair code cannot be generated for the paired POSes.
- Any other pair request for the particular POS will be declined 6. Success response is returned to POS.

pos.jpg

Operating:

All POS requests must contain authorization header (JWT).

JWT Token must be created according to the RFC 7519 (JWT) - type RS256.

Token in payload should contain fields:

- sub - equal to POS SN,
- iat - issued at date as unix,
- tiemestamp exp - expire date as unix timestamp.

Token must be present for each request - stateless.

1. Each request must be sent with the header "Authorization". The content should contain the JWT token preceded by "Bearer ".
2. MACS will check the sub, iat, exp fields. If any of fields is invalid, access will be forbidden.
3. MACS will search for public key in database for particular POS.

- If public key is found. Macs will verify the JWT token using the POS public key.
- Access will be granted if verification is succeeded.
- If POS SN is not found or signature is invalid for the public key, access will be forbidden.

auth.jpg

POS functionalities

Core functionalities

Functionality	Type	Description	MACS API method
Check possibility to entry	Online	It should send card data in request, in response it receives success or error with code. It should show number selector for guest up to max number of guest received in response.	post/check_entry
Confirm entrance	Online	Should confirm cardholder used a service with selected number of guests along with "accessId".	pos/confirm_entry
Check possibility to entry in offline mode	Offline	It should keep BIN ranges downloaded in some time perion (1 day) or manually from terminal - per each POS. In case a POS has no internet connection at moment cardholder is trying to use it. The POS should check if card is between one of BIN ranges and allow enter in this case.	pos/fallback_bin_ranges
Report offline entrances	Online	Should report all offline entrances made in offline mode.	pos/offline_reports

Allow offline entrances for cardholder from whitelist	Offline	POS should keep hashes of whitelisted PANs downloaded from the AC API in time period (daily) or manually. As cardholder tryin to use it and POS is offline the POS should hash PAN uses HMAC with sha256 algorithm and secret (hardcoded, received from Verestro), then check if hash exists on the list. IF so, POS should accept entry.	pos/whitelisted_pans

Check entry error codes handling

Functionality	Type	Description	MACS
Check possibility to entry	Online	It should send card data in request, in response it receives success or error with code. It should show number selector for guest up to max number of guest received in response.	post/check_entry
Confirm entrance	Online	Should confirm cardholder used a service with selected number of guests along with "accessId".	pos/confirm_entry

Check possibility to entry in offline mode	Offline	It should keep BIN ranges downloaded in some time perion (1 day) or manually from terminal - per each POS. In case a POS has no internet connection at moment cardholder is trying to use it. The POS should check if card is between one of BIN ranges and allow enter in this case.	pos/fallback_bin_ranges
Report offline entrances	Online	Should report all offline entrances made in offline mode.	pos/offline_reports
Allow offline entrances for cardholder from whitelist	Offline	POS should keep hashes of whitelisted PANs downloaded from the AC API in time period (daily) or manually. As cardholder tryin to use it and POS is offline the POS should hash PAN uses HMAC with sha256 algorithm and secret (hardoded, received from Verestro), then check if hash exists on the list. IF so, POS should accept entry.	pos/whitelisted_pans

Check entry error codes handling

CARD_ASI_FAILED	Card status authorization failed. Use the card again to try amount verification.
CARD_AUTH_INSUFFICIENT_FUNDS	Insufficient card funds. Authorization cannot be performed.
CARD_AMOUNT_AUTH_FAILED	Amount verification failed.
LIMIT_EXCEEDED	The usage limit for this card is exceeded.
UNMET_REQUIREMENTS	Requirements to access the service are not fulfiled. Contact your bank for more information.

TEMPORARILT_BLOCKED	The card was recently used and the transaction is not completed. Complete the transaction or wait a while and retry.
MISSING_ACCESS_RULES	Your card is not allowed to be used in this location.

API Error code	On terminal error screen.
UNKNOWN_DEVICE	The device is not assigned to any location.

Revision #8
Created 26 October 2023 07:01:15 by Grzegorz Czajkowski
Updated 22 January 2024 08:20:49 by Jagoda Mazurek