Access Control

Special benefits for your customers to boost your bussines.

Introduction

Access Control is an advanced business solution designed to meet the growing needs of modern companies, banks, fintech and financial institutions. This product is specifically addressed Mastercard card users and enables them to access various perks such as entrances to amusement parks, fast lane access, airport lounge privileges, and other valuable extras. Basing on card transactions or product type cardholder can get access to particular benefit. Example:

- All Gold card users can get access to Airport Lounges.
- All business card users that do minimum 1000 USD transaction per month can get access to special loyalty program.
- All cardholders of particular BIN (bank) can get access to concert or event organised for them.

Features:

User-Friendly Admin Panel:

Access Control incorporates a user-friendly admin panel that facilitates easy management of the solution. The admin panel offers several options for convenient control and monitoring of the system.

Rule Management:

The admin panel allows administrators to manage rules effectively. Rules determine the eligibility criteria for accessing different perks and benefits. With this feature, administrators can easily configure and modify rules based on the specific requirements of the company and its customers.

Traffic Monitoring:

Access Control provides a comprehensive traffic monitoring feature through the admin panel. This allows administrators to keep track of user activity across the system. They can monitor number of entrances, guest entrances, time and date, free or paid entries and many more.

Report Exporting:

The admin panel incorporates a reporting function that enables administrators to generate reports for further analysis. These reports contain valuable insights and metrics related to user activity, benefits redeemed, and other relevant data. Administrators can export these reports in various formats for easy sharing and data analysis.

Card Enrollment Verification:

Access Control includes a card enrollment verification feature that ensures the security and validity of Mastercard users. The admin panel enables administrators to verify and manage card enrollments, ensuring that only authorized users can receive the various perks offered by the solution. This feature adds an extra layer of security, preventing fraudulent usage and unauthorized access.

Benefits:

Users can be rewarded with a variety of unique experiences at different service points. Anywhere there is a payment terminal. From airports, amusement parks, sport stadium, museums, travel entertainments to stores.

Enhanced Customer Experience:

By providing Mastercard users with access to a wide range of perks and benefits, Access Control enhances the overall customer experience. Users can enjoy valuable extras such as amusement park entrances, fast lane access, and airport lounge privileges, resulting in increased customer satisfaction and loyalty.

Efficient Administration:

The user-friendly admin panel simplifies the management of Access Control. Administrators can easily configure rules, monitor user activity, export reports, and validate card enrollments. This streamlines administrative tasks and enables efficient control of the system.

Data-Driven Decision Making:

The traffic monitoring and report exporting features enable administrators to gain valuable insights into user behavior and system performance. By analyzing this data, businesses can make data-driven decisions to optimize the Access Control solution and improve customer satisfaction.

Increased Security:

The card enrollment verification feature ensures that only authorized users can access the perks and benefits offered by Access Control. This security measure safeguards against fraudulent usage and unauthorized access, providing businesses and users with peace of mind.

Terms & Definitions:

Term	Definition
MRS	Mastercard Rewards System
ICA	Interbank Card Association - x-digit number assigned by Mastercard to a financial institution, third party processor or other member.
TPP	Third Party Provide
BIN	Bank Identification Number (First 6 card digits.)
PAN	Primary Account number (Full card number.)
GUI	Graphical User Interface
ASI	Account Status Inquiry
Token	Digital card number

Intro slides

Access Control is available to users through a friendly and easy-to-use admin panel accessible through a personalized website.

Panel admina.jpg

Web-based and Customizable Admin Panel:

The system features a web-based administrative panel that allows users to access and manage various aspects of the application through a web browser. Additionally, the admin panel is fully customizable, enabling administrators to tailor it to meet specific organizational needs and preferences.

Compliant with Safety Standards:

This system adheres to industry-specific safety and security standards, ensuring that it meets all necessary regulatory and safety requirements to safeguard users and data.

Implementation Time: 3 Months from Contracting

The system can be fully implemented and operational within a timeframe of three months from the signing of the contract. This includes all necessary development, testing, and deployment phases.

Compatible with Various Entertainment Outlets, Airports, Stadiums, Theaters, Museums, Cinemas, etc.:

The system is designed to seamlessly integrate with a wide range of entertainment and public places, including but not limited to airports, stadiums, theaters, museums, and cinemas. It can be deployed wherever accessible payment terminals are present.

Unique Access Control Engine Fully Prepared by Verestro:

The system offers a proprietary and exclusive access control engine developed and fully prepared by Verestro. This engine is responsible for managing user access permissions and ensuring the security and integrity of the system's functionalities. It is a distinctive feature that sets this system apart from others in the market.

Implementation Steps

1. Opening project with Verestro.
2. Setup of test environment.
3. Configuration.
4. Customise Admin Panel.
5. POS provider Integration or use existing Ingenico connection.
6. Setting up POS messages.
7. Defining fallback to offline entrances.
8. Integration with MRS (optionally if you need transaction history).
9. Tests on beta environment.
10. Test on production.
11. Friends and family phase.
12. Go live.

Architecture

architecture.jpg

Access Control flow (Example)

Bez nazwy.png

Prototype

https://www.figma.com/proto/zGnlt8oNXsSkXnUIu4F55F/MACS?page-id=180%3A2461&type=design&node-id=1106-15450&viewport=381%2C532%2C0.02&scaling=scale-down&starting-point-node-id=5579%3A125897

Overview

Access Control within the system allows for the allocation of benefits to a specific group of cardholders. This feature empowers administrators to precisely define the criteria and conditions that must be met in specific locations for cardholders to receive these benefits. For instance, administrators can select a particular card type, such as MC Gold, issued by a specific country and bank. Furthermore, the system facilitates the provision of these benefits free of charge, both for the cardholder and their accompanying guests.

In certain scenarios, alongside complimentary access, administrators have the flexibility to establish special pricing structures for benefits upon meeting specific conditions. This means that, in some cases, individuals may qualify for benefits by fulfilling specific criteria while incurring a reduced cost.

The system's additional functionality includes spend-based control, enabling administrators to monitor a program participant's spending behavior. This feature allows for the creation of conditions like spending a minimum of 100 euros within a 30-day period at sports stores to qualify for complimentary stadium entry.

Solution Components:

The Access Control feature is an integral part of the solution, which comprises the following key components:

- Verestro’s Admin Panel: This web-based interface allows administrators to manage and configure the Access Control feature and associated settings. It provides a user-friendly platform for controlling benefit allocation criteria.
- Verestro’s Backend Engine: The core engine of the system, developed by Verestro, powers the Access Control feature. It manages the allocation of benefits, verifies conditions, and ensures the security and integrity of the entire process.
- Integration with POS Providers: To enable the seamless execution of benefit criteria and conditions, the solution integrates with Point-of-Sale (POS) providers. This integration facilitates the real-time verification of spending and other conditions at relevant stores.

Key point to choose Access control:

- Emphasizing the Inclusiveness of a Specific Payment Card: Access Control allows organizations to highlight the inclusiveness of a particular type of payment card, making it an attractive choice for cardholders. This feature enhances the appeal of the card and can drive card usage.

- Activating Users to Utilize the Payment Card in Specific Shopping Categories: Access Control empowers administrators to incentivize cardholders to use their payment card within specific shopping categories. This promotes targeted spending behavior and increases engagement with the card.
- Providing a Premium Experience for Cardholders and Guests: Access Control offers the capability to deliver a premium experience not only to the cardholder but also to their accompanying guests. This enhances customer loyalty and satisfaction.
- User-Friendly Operation with Minimal Additional Steps: The Access Control solution is designed to seamlessly integrate with the user experience at payment terminals. It ensures that users do not encounter additional, complex steps beyond the standard authorization process, simplifying their interactions.
- Compliance with the Latest Security Standards: Access Control is built with a strong focus on security, ensuring compliance with the most up-to-date security standards and protocols.

Terminal User’s Flow

user.jpg

- **Local staff verification of cardholder's identity:**

Prior to granting access or benefits, local staff members are required to confirm the identity of the cardholder. This manual verification step ensures that the correct individual is accessing the designated area or service.

- **Cardholder taps card on POS for authorization:**

The cardholder initiates the process by tapping their payment card on the Point-of-Sale (POS) terminal. This action triggers the authorization process, validating the card's eligibility for access or benefits.

- **POS informs cardholder about the number of available visits:**

The POS terminal communicates the number of available visits or benefits associated with the card to the cardholder. This information helps the cardholder understand their benefits and make decisions.

- **POS Confirms Entrance:**

Once the cardholder's eligibility is established, the POS terminal confirms their entrance, granting access or providing the specified benefits. This step marks the successful completion of the Access Control process.

Access Control Key Components

Component	Description
Admin Panel	Allows to create rules, monitor entrances and download reports.
Access Control Engine	It connects with acquier and the POS provider, counts the carholder's payments, converts the amounts and decides on granting the benefit.
MRS	Mastercard Reward System provides information about the cardholder's spending.
Acquier integration	The acquirer provides an account status inquiry to verify the card.
POS provider integration	Interface for user interaction.

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.