MACS

Mobile Access Control Services

www.macs.online

mobileid.macs.online / mobileaccess.macs.online

Centralize identity and access management

The MACS access platform is a secure, end-to-end solution designed to enable mobile identification across a wide range of physical resources used in various operational use cases.

It is based on **a highly secure bi-directional token protocol**, allowing operation both in real time and in fully offline mode for autonomous transactions.

MACS enables mobile credentials to be securely shared with any user, allowing access to doors, cabinets, or other protected resources using a mobile phone.

It provides operators with full control over user access rights to designated resources, as well as complete transaction traceability and access history.

The solution is composed of two distinct and combinable services:
MobileID, providing pure mobile identification for multi-application environments across all types of integrated systems.
MobileAccess, an innovative access control solution leveraging the power and connectivity of smartphones to significantly reduce infrastructure requirements and drastically lower deployment and operating costs.

By design, the MACS multifunctional platform delivers a dual-service architecture, making the solution highly scalable and future-proof.

MACS is a solution developed by the SELEPSO Group.

SELEPSO is an expert in electronic security and secure identification.
The Group was formed under the leadership of a French industrial family-owned shareholder, bringing together the expertise of three independent companies: **SCOPUS, ELSYLOG, and SCAP.**

SELEPSO positions itself as a key new player in the protection of assets and people, providing its customers with high-technology solutions certified by ANSSI.

MobileID Service

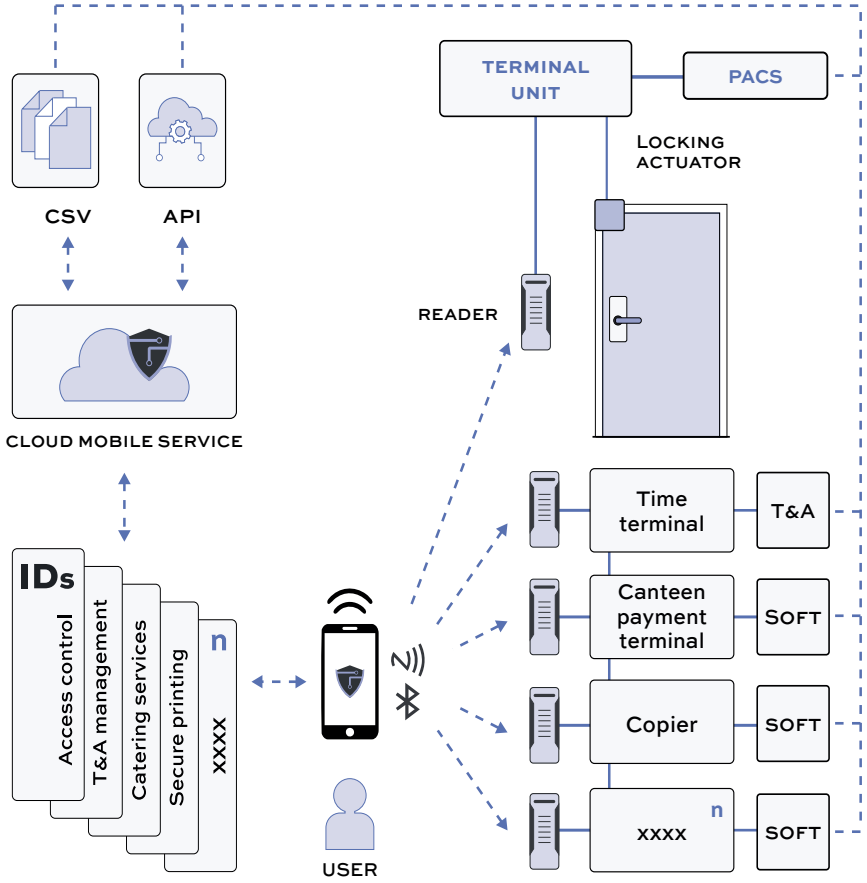
Multiple Digital Identities, Instant and Fully Controlled

MACS MobileID enables simple and automatic mobile identification across multiple solutions and environments.

Multiple digital identities can be assigned to a single user.
Thanks to automatic detection of the intended use by the reader, MACS ensures seamless and efficient multi-application and multi-identity operation.

MobileID is an independent system that operates alongside or as a replacement for RFID badges or other deployed identification technologies.
The service can be easily connected to any existing or new system.

MobileID operates across a wide range of reader-based resources tailored to the intended use, including: access control, time and attendance, catering services, secure printing, EV charging, automated systems, forklifts, dispensing cabinets, and more.



OPERATION

Mobile credentials are used as an alternative to physical badges, particularly for Physical Access Control Systems (PACS), as well as for any other application relying on badge-based identification.

Credentials can be generated directly within the MobileID web platform or delivered via file exchange or dynamic API links.

The cloud service transfers these credentials, encapsulated within a secure token (AES-128 and SHA-1/2), to the user's smartphone(s) (with the option to restrict delivery to a single mobile device) **through a secure channel using public key encryption** (RSA-2048) **and TLS authentication.**

Users authenticate themselves to readers using their smartphone via **NFC and/or Bluetooth communication.**

The correct identifier corresponding to the reader's application is automatically transmitted to the reader.
The identifier is then forwarded by the reader to the management system through its standard communication interface.

The identifier length is fully configurable.

Credential management is dynamic. Credentials can be revoked at any time.

MobileAccess Service

Control Your Access with Your Smartphone

MACS MobileAccess is a comprehensive smartphone-based access control solution.

Hosted in the cloud, it leverages the processing power and connectivity of the smartphone to significantly reduce the complexity and cost of traditional access control infrastructures.

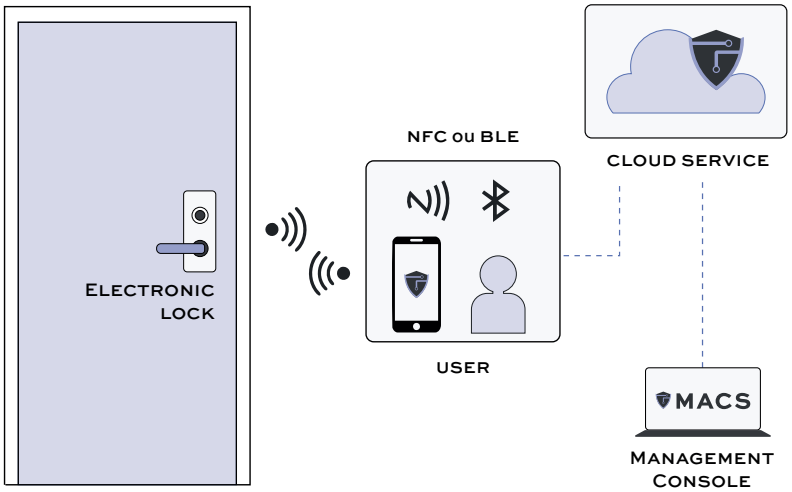
MobileAccess directly supports multi-brand hardware resources such as electronic locks and door controllers.

Operating autonomously, the devices do not require connection to a centralized network or data bus linked to a server and management software.

The cloud service generates secure tokens that are transmitted via the user's smartphone to the physical resources.

These tokens ensure transaction security and enable bi-directional communication, allowing automatic feedback of access logs, technical information (e.g. battery status), blacklists, and more.

- High availability, even for isolated or remote access points
- Low installation and operating costs
- Simplified infrastructure and deployment
- High scalability as requirements evolve
- Compatibility with a wide range of multi-brand products
- Enables access control for all types of doors, lockers, cabinets, racks, and enclosures



OPERATION

Mobile credentials are used as an alternative to physical badges traditionally used in Physical Access Control Systems (PACS).

Credentials can be generated within the MobileAccess web platform or delivered via file exchange or dynamic API links.

The cloud service transfers these credentials, encapsulated in a secure token (AES-128 and SHA-1/2), to the user's smartphone(s) (with the option to restrict usage to a single mobile device) through **a secure channel using public key encryption** (RSA-2048) **and TLS authentication.**

A token is generated for the combination of a user, a smartphone, and a locking resource.

Following an encryption challenge, the token is transmitted to the locking resource via **NFC or Bluetooth**.

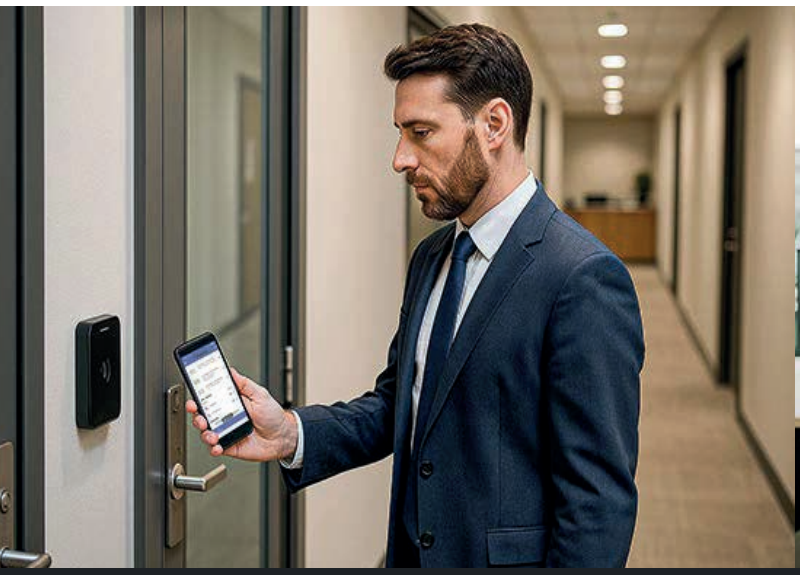
The lock decrypts the data, verifies its validity, and makes the unlock decision based on the received access rights.

The lock records the transaction and returns it within the token, which is then automatically transmitted back to the cloud service for archiving and consultation.

End-to-end security for mobile devices is ensured through a set of proven secure elements, validated and assessed through formal security audits.

MACS

Mobile Access Control Services



Secure Multi-Application Mobile Identification

Move towards greater security, flexibility, and independence.

A single mobile application

One single application

✓

Compatible with iOS and Android, independent of the smartphone hardware environment.

✓

Operates in “Wallet” mode, while remaining independent from proprietary and costly wallet services.

✓

Compatible with NFC and Bluetooth Low Energy (BLE) technologies.

✓

Remote-control mode available.

Open and Integrable System

Multi-tenant, multi-site, multi-application, and multi-identity management.

✓

Automatically detects the reader’s application and transmits the identifier corresponding to the intended use.

✓

Compatible with all types of systems.

✓

Interfaces with any third-party system via APIs or flat file exchange (CSV).

✓

SDK available for integration into an existing mobile application.

End-to-End Security

Encrypted data transmission via a highly secure, patented token.

✓

Operates in remote or isolated areas, even without mobile network or Wi-Fi coverage.

✓

Bi-directional communication enabling the feedback of technical information and full access traceability.

✓

Smartphone biometric unlocking contributes to ensuring strong user identity verification.

SELEPSO

solutions de sûreté et d'identification

www.selepso.com

3/5 place Royale
78100 Saint-Germain-en-Laye - France
pierreyves.dudal@selepso.com