ICMS
Credential Management System

Credential management enables governments to issue, reissue, validate, and revoke credentials (paper-based, chip-based, and digital ID credentials). This can be achieved from multiple locations such as city halls, social welfare offices, and other government agencies.ncorrupted.

Streamlined CMS

The Credential Management System (ICMS) is an advanced credential registry enabling government agencies to monitor the lifecycle of credentials for large populations.

Additionally, it offers an application store to manage chip applications for chip-based credentials, to provide access to additional eGovernment services such as healthcare, social security, and driver's license services.

The solution can be easily deployed, interfaces seamlessly with new or existing systems based on OSIA standards, and acts as a central software engine driving all credential-related operations.

ICMS works through the following key steps:

- Receives credential creation requests from an Identity Management System.
- Prepares data (alphanumeric and biometric) and sends production requests to the relevant systems, such as personalization or digital ID systems.
- Tracks and monitors the complete lifecycle of credentials, from creation and issuance to revocation.
- Enables reporting and status modification of a credential (e.g., reporting a credential as lost or stolen and revoking it).
- Stores and manages chip applications.
- Supports post-issuance operations for specific credentials.

Key Benefits

Credential lifecycle management

Issue, renew, replace, suspend, and revoke credentials.

Credential tracking

Track the entire lifecycle of credentials, maintaining a history of changes from request to revocation.

Post-issuance

Compute which operations can be performed on a credential and keep track of all post-issuance operations.

Chip applications

Manage chip applications and synchronize status changes after postissuance operations.



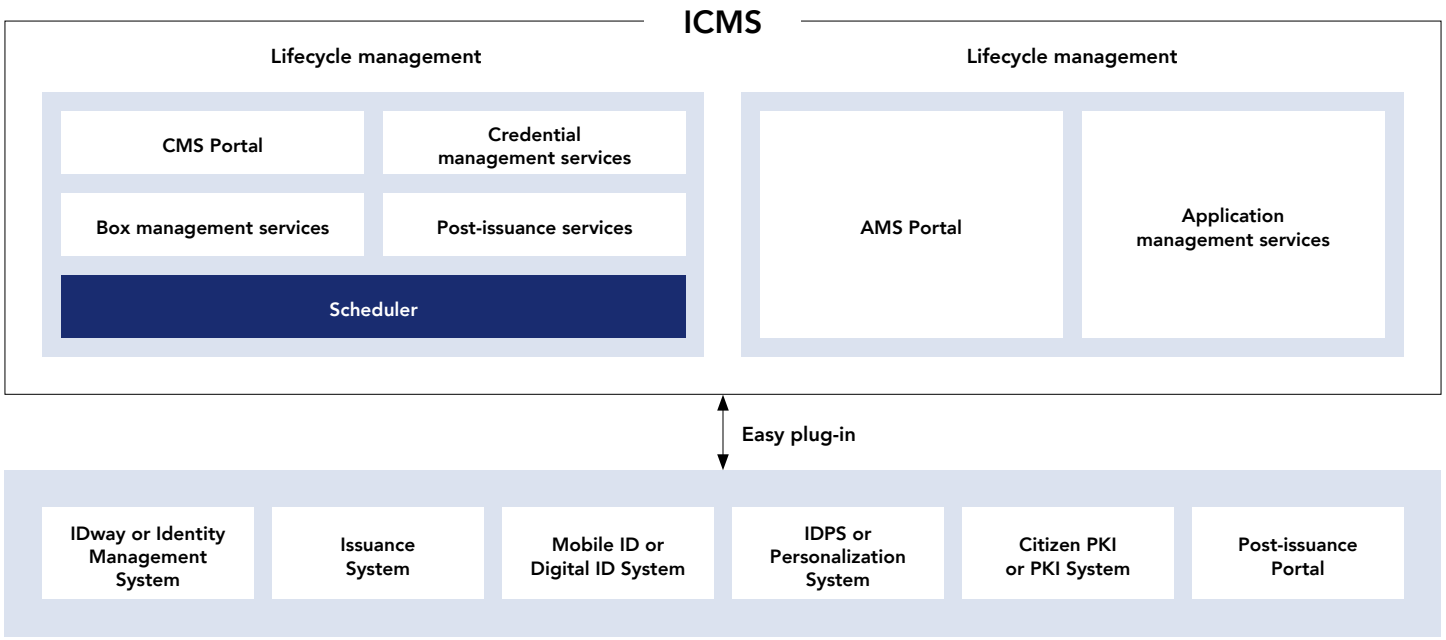
IN GROUPE

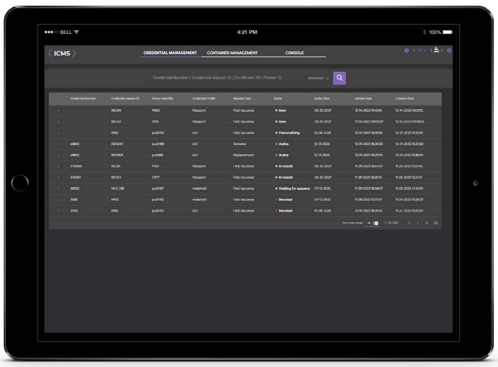
Interaction with external environment

As part of the IDway ecosystem of solutions, ICMS seamlessly interfaces with all other IDway components. In this way, ICMS constitutes one of the components of the IDway ecosystem that governments can use to design systems tailored to their specific needs.

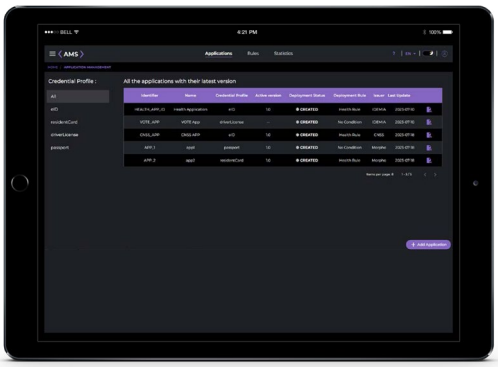
ICMS is also available as a stand-alone component that can easily connect to any external system. Interaction between ICMS and the external environment is done through an easy plug-in based on open standards, ensuring modularity and avoiding vendor lock-in.

ICMS can be directly integrated with the Document Personalization System (IDPS), Mobile ID System, the PKI, and the Data Analytics Portal (IDAP).





Lifecycle management portal



Chip application management portal

Lifecycle and application portals

All portals are web-based applications featuring modern User Experience (UX) to provide access for operating and administrating the ICMS platform.

Cutting-edge technology

Architecture: State-of-the-art architecture based on microservices

Security: Data encryption, TLS-secured connection

Compliance to standards: GDPR, OSIA (Open Standards Identity API)

User interface: State-of-the-art GUI technology based on HTML5 and Angular

User management and access control: Active directory, LDAP, user roles management

Deployment: Deployed with Docker, Kubernetes, and in the cloud

April 2026
Copyright © 2026 IN Groupe. All rights reserved.
www.ingroupe.com