



Identity Management System for Airports

Eliminate the Unauthorized Transfer of Employee ID's

www.idmission.com



IDmission:

IDmission is a solution provider that orchestrates digital transformations for companies relying on identity and ID verifications, by using passive biometrics, AI, and our industry expertise to create an effortless end to end customer experience.

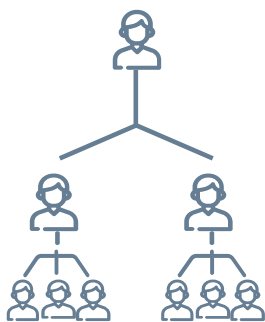
Overview

Airports are large, multi tenant organizations with critical and complex security requirements. Large numbers of employees need to routinely access myriad physical and logical systems. Today this access is accomplished using single factor authentication (login/passwords or key cards). IDmission's IDMS solution enables biometric authentication and offers very strong security, that along with passwords or key cards enables a state-of-the-art two factor authentication system.

Using ubiquitously available smartphones as the conduit for capturing and authenticating selfie biometrics, the system can be implemented with no investment in new hardware at the access points.

The Problem

Airports are multi-tenant organizations with dynamic role relationships.



Onboarding and offboarding processes are manual and cumbersome.



Once onboarded, employees are assigned access to physical and logical systems. Physical systems are typically accessed using security badges. Logical systems are accessed using passwords. In all cases the user access is granted using a single factor of identity and can easily be defrauded.

Solution Overview

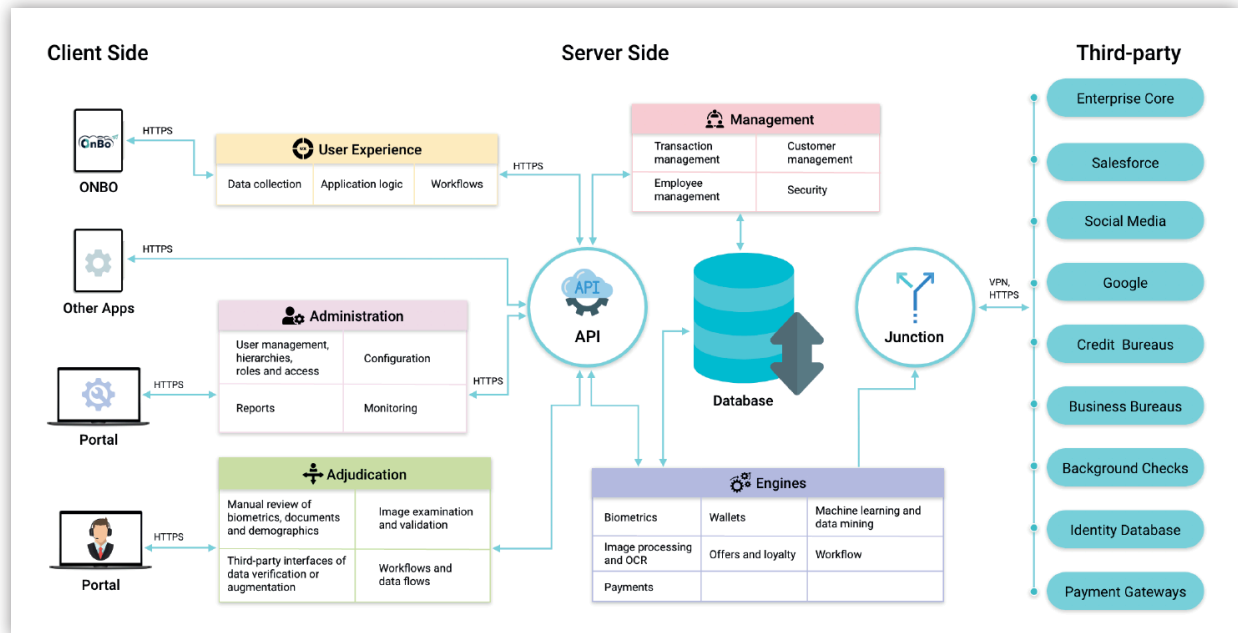


Employee owned smartphones are loaded with a mobile app that conducts the initial enrollment. The app is capable of scanning ID documents, extracting data from them automatically, capturing a selfie while ensuring that the subject is a live person (no printouts, videos, masks etc.). The selfie is matched against the ID photo automatically. The employee record is sent to the signing authority for approval (using a web portal).

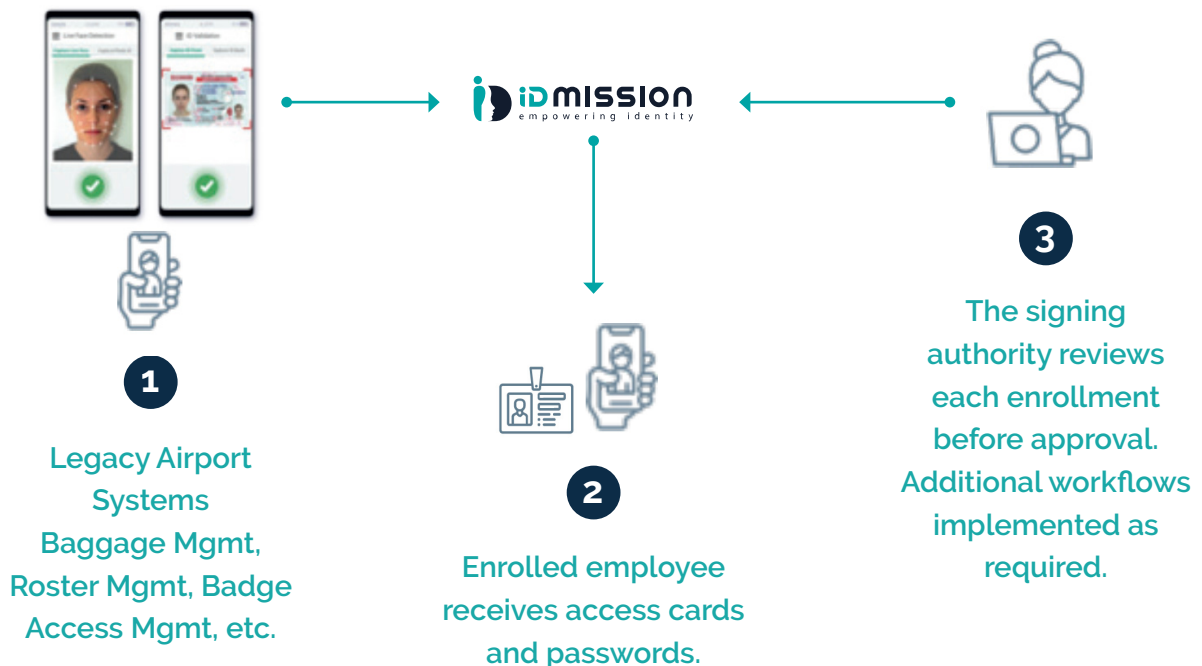
The Identity Management System servers maintain the Identity records, the biometric enrollments and authentications of each employee. Access rights based on employee roles and employee activation/deactivation. Interfaces to legacy systems are maintained here as well. The system comes with a portal for administration, viewing activity and adjudication by signing authorities.

The IDMS offers interfaces that connect to each of the airport's legacy physical access and logical access systems. This enables real time 2-factor authentication with no new hardware required at the point of access. These interfaces also keep the IDMS in synch with the airport systems vis-a-vis the each employees current status and access rights.

Platform Architecture



Digital Onboarding



IDmission Backoffice Review Portal

Face Match	VERIFIED
Name	ENXXXUE CAXXOS LEXN FEXXXDEZ
Address	AV COXXXXRAS 241 CASA 3 COL SAN JEXXXXXO LID- ICE 10200 LA MAXXXENA COXXXXRAS DF
DOB	15/XX/19XX
ID 1	LNFRXXXXXXXXX09H500
ID 2	LNFRXXXXXXXXX09H500
MRZ Valid	YES

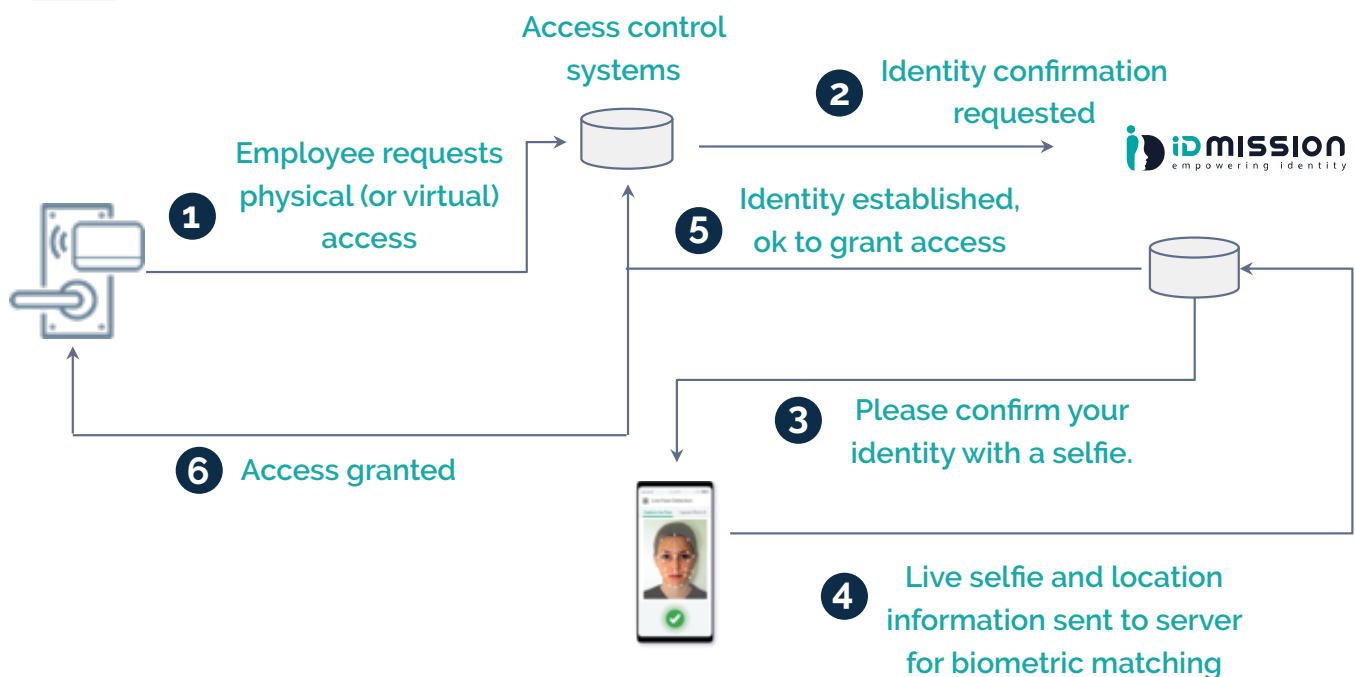
ID Verified	
Background Check	✓
Criminal Check	✓
Credit Check	✓
	✓

Signing Authority Action

Approved	
Return for more information	✓
Additional Review	

Comments:

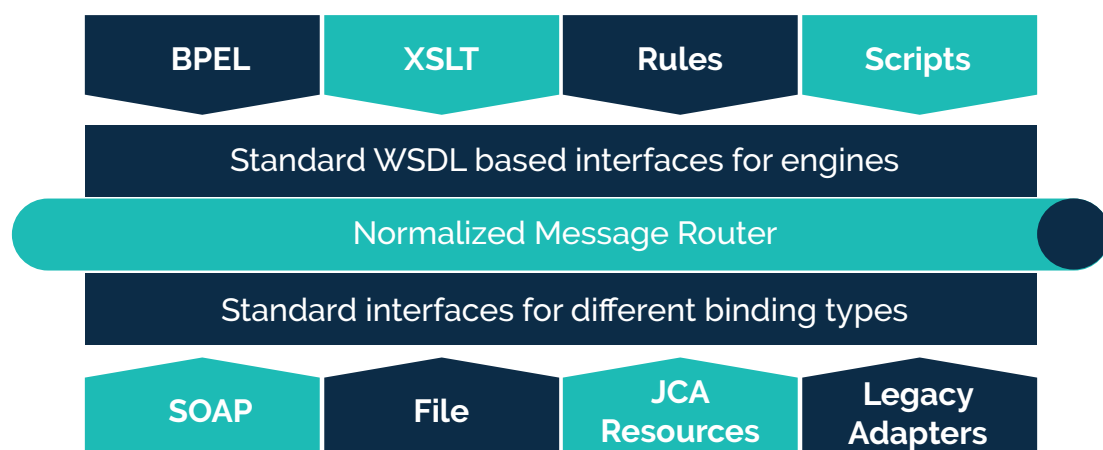
Adding Biometric Identity as a 2nd Factor for Access Control



Management Portal Summary

Face Match	Reporting	Back Office	Super User
• Create Company & Hierarchies • Create Roles & Access Rights, Languages • Create Users	• Form Summary and details • Customer/Employee Reports • Transaction Reports, Scheduled email reports • Billing reports on per transaction or per user basis	• Workflows • Form Review and editing, Image verification, Resend, Approve, Download, Print.	• Template Creation and Management • Notification template configuration and management • Language setup and management • Logo management • Fee configuration – per transaction or per user

External Interfaces: Enterprise Service Bus



Apache service mix: Built on Apache ActiveMQ, combines Service Oriented Architecture and Event Driven Architecture. Extremely flexible architecture that implements JBI, offers smart routing capabilities and is connectivity centric.

Offboarding



Apache service mix: Built on Apache ActiveMQ, combines Service Oriented Architecture and Event Driven Architecture. Extremely flexible architecture that implements JBI, offers smart routing capabilities and is connectivity centric.

Process Flow Description

1. Employees download the App on their smartphones (Android or iOS).
 - a. ID scan, front and back, selfie capture (with liveness detection), any other data is entered
2. Enrolments are queued in the portal for the corresponding signing authority to approve
3. Optional queue on an external signing authority (government for example)
4. Response from external signing authority. If approved, employee is fully onboarded.
5. Employee requests access to a legacy airport system (password or keycard)
6. Legacy system interfaces with IDMS. Sends IDMS token containing one factor of Identity (login/ password or key card number)
7. IDMS sends employee app a notification requesting biometric verification. App is used to capture location, biometric selfie (with liveness detection).
8. If the employee selfie is matched with the picture on file.
9. IDMS sends the second factor authentication to the legacy system and access is granted.
10. Airport Systems of Record that maintain real time employee status interface with IDMS and update any changes to employee status or access rights in real time. IDMS maintains the status and access rights and authenticates only those employees that have access rights for the service requested.

IDmission IDMS at a glance

Multifactor Identity Management	All 3 factors of identity supported - something you know, something you have, something you are
Biometric Capabilities	Support biometric enrollment, biometric deduplication and biometric authentication. Support multimodal biometrics.
Integration Capabilities	Enterprise service bus (ESB) built into Junctions module. Enables interface integration on demand.
Hierarchy, Role and Access Management	Supports dynamic hierarchy and role creation. Access control managed based on role and hierarchy level.
Password Management	Support biometric passwords, can connect to SSO systems
Service and Support	24x7 support
High Availability	99.99% uptime guarantee
Highly Scalable	Servers are setup behind a load balancer. Scales with load automatically.
	Infrastructure is PCI-DSS certified

IDmission is mentioned by Gartner in the 2019 Market Guide for Identity Proofing and Corroboration and in a Forrester Brief "Emerging Technologies In Financial Services" September 9, 2015. Contact IDmission today to learn more about how we can help you improve airport security.





About Us

IDmission eliminates risk associated with false identities for companies depending on ID verification by using passive biometrics and AI to create an effortless customer experience.

United States

1830 17th St, Suite 100,
Boulder, CO 80302
+1 (800) 925-8041 Ext. 2

sales@idmission.com

United States

7254 East Southern Ave,
Suite 101, Mesa, AZ 85209
+1 (800) 925-8041 Ext. 3

sales@idmission.com

México

Camino a Santa Teresa
187C piso 5,
Col Parque del Pedregal,
Tlalpan CP 14010 CDMX
+52 1 (55) 5528 6490

ventas@idmission.com

India

Icon Tower, 4th floor,
402-403, Main Baner Road,
Baner, Pune 411045
+91 911 225 7300

ventas@idmission.com

