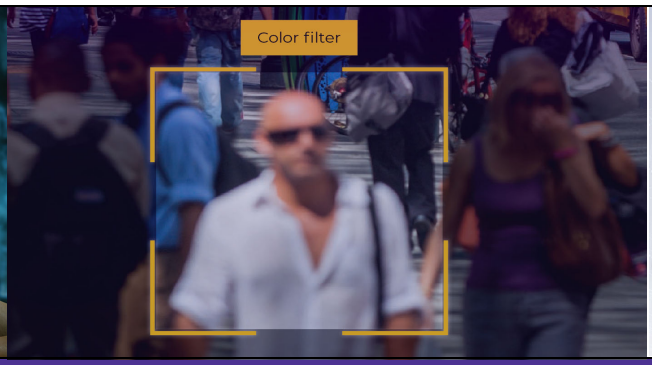
IDEMIA
National Security Solutions

IDEMIA National Security Solutions

An Affiliate of IDEMIA Public Security North America

Corporate Profile

Providing trusted identity and biometric solutions to the defense, justice, and intelligence communities for over 60 years.



www.idemia-nss.com | 703-797-2600 info@idemia-nss.com | 675 N Washington St. Alexandria, VA 22314

IDEMIA National Security Solutions LLC (“IDEMIA NSS” or “Company”), is a Delaware Corporation and United States-based subsidiary of IDEMIA Identity & Security USA LLC (“IDEMIA I&S”) and is mitigated from Foreign Ownership, Control, or Influence (FOCI) via a Special Security Agreement (SSA) approved by the Defense Counterintelligence and Security Agency (DCSA). IDEMIA Identity & Security USA LLC, is wholly owned by Morpho USA Inc. (DE), which is wholly owned by IDEMIA Government USA Corporation, which is wholly owned by IDEMIA Finance SAS (France), which is wholly owned by IDEMIA Group SAS (France), which is 95% owned by three funds managed by Advent International Corporation, a U.S. investment manager headquartered in Boston.

v2.0

Table of Contents

Chapter 1: About Our Company

IDEMIA National Security Solutions (NSS) provides proven identity security and authentication services to the U.S. Federal government. Our biometric technology powers four out of five of the largest government identity databases. NSS delivers critical identity proofing for key biometric programs, including the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) and the Department of State (DOS). NSS multi-modal identity solutions are NIST-rated as top performers for speed, accuracy, and reliability.

NSS serves a plethora of U.S. Federal government customers, delivering products that provide:

- Biometrics and Forensics solutions
- Physical Security infrastructure
- Augmented Vision monitoring and analysis
- Enterprise Identity validation and enrollment services
- Secure Credentialing through digital and physical verification

1.1 About NSS

IDEMIA's National Security Solutions (NSS) is the Foreign Ownership, Control, or Influence (FOCI) mitigated IDEMIA affiliate, supporting the national security interests of the United States of America through cutting-edge identity solutions and services. Our best-in-class identity solutions are top rated by National Institute of Standards and Technology (NIST) for speed, accuracy, and reliability. For over 60 years, our extensive hardware, software, and services portfolio has driven consistent results enabling America's defense, intelligence, and homeland security posture. NSS delivers the most sensitive U.S. Government identity proofing and biometric collection programs, such as the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) program.

All IDEMIA products and solutions are built upon an extensive history of biometric systems and their deployment and operation throughout the industry. IDEMIA systems are integrated with the most critical infrastructures and services across the country at the local, state, regional, and federal levels. This includes thousands of LiveScan and AFIS systems, as well as some of our government's largest and most important criminal and military biometric identification systems. These solutions are driven by our industry-leading algorithms for fingerprint, iris, and facial recognition technologies, which consistently receive top rankings throughout NIST evaluations. We strive to be on the cutting edge of biometric technologies, providing the latest and greatest solutions to our customers around the world. Across IDEMIA and specifically at NSS, it is our mission to make this world a safer place through this pursuit of advancement in the critical field of biometrics.

We provide an Applied Biometrics Center of Excellence for customers to explore our product suite in person.

1.2 Mission, Vision, and Values

Mission	Vision	Values
Our mission is to be a trusted partner, delivering innovative, proven, and scalable identity and biometric solutions that support force protection and the entire identity lifecycle for national security customers.	NSS strives to provide continued leadership in global biometric use for the purpose of protecting our U.S. National security partners from Identity-Related threats.	We are committed to protecting individuals and security interests, dedicated to delivering mission-driven results to our trusted partnerships, and attentive to our customers ensuring we provide cost-effective solutions.

1.3 Identifiers and Codes

The NSS Unique Entity Identifier (UEI), Cage Code, Listed Vehicles, Certifications, and FOCI status are provided in the below table.

UEI	Cage	Vehicles	Certifications	FOCI
KWRSKBHAN4K3	1MJL8	• GS-35F-597GA • DOD CDAO Tradewinds Awardable • FBI ITSSS-2 (Sub) • Authorized FBI Channeler • SeaPort NxG	• CMMI Level 3 • ISO 9001:2015 • ISO 37000-1	Special Security Agreement

1.3.1 NAICS

NSS products are available under the following NAICS codes.

334111	513210	541512	541611	541715
334118	541330	541513	541690	561621
334290	541511	541519	541714	611420

1.4 NIST Multi-modal Biometric Rankings

IDEMIA has actively participated in various NIST evaluations, submitting algorithms across multiple biometric modalities. IDEMIA solutions are driven by our industry-leading algorithms for fingerprint, iris, and facial recognition technologies, which consistently receive top rankings throughout NIST evaluations.

- **Fingerprint Matching**
  Top-ranked in NIST Proprietary Fingerprint Template Benchmark based on 1:1 matching with PFT III for AFIS-class algorithms.
- **mFIT Challenge**
  Top-ranked in NIST Mobile Fingerprinting Innovation Technology (MFIT) Challenge
  - Includes advancements in our contactless fingerprint capture mobile application
  - Earned the First Responser's Choice award for usability
- **ELFT**
  Top-ranked in NIST Evaluation of Latent Fingerprint Technologies (ELFT).
  - Achieved most accurate matching on datasets containing 16M fingerprints and 150K palmprints
  - Received accuracy scores 7% to 60% higher than all other algorithms
- **FVRT**
  Top-ranked algorithm for Facial Recognition Vendor Test (FRVT) 1:1 and 1:N that are valid for U.S. Federal use cases with 99.88% Accuracy in 2023 NIST FRVT evaluations for gallery of 12 Million identities.
  - Highest accuracy rating on large datasets ever achieved in FRVT
  - Most consistent solution among 300+ submissions, among top ranks for all use cases and datasets
  - Far outranks all other submissions for unbiased matching relative to race, gender, and age.
- **Tattoo**
  Top-ranked in Tattoo Recognition technology evaluations including Tatt-E and Tatt-C assessments from NIST for automated image-based tattoo recognition.

1.5 What Sets Us Apart from the Competition?

- Pioneer in Global Biometrics with 60+ years supporting U.S. Federal Government
- AI Identity solutions enabling the future
- Consistent biometrics supplier to FBI NGI, DOD Biometrics Enabling Capability (BEC), DOS Consular Affairs Facial Recognition System, and IC
- Year over year superior NIST ratings
- Superior engineering processes incorporating SAFe principles
- Dedicated Applied Biometric Center of Excellence where clients can explore, test, and engage with our solutions
- Top Secret Facility Clearance
- FOCI mitigated entity with full adherence to National Industrial Security Program Operating Manual (NISPOM) regulations

1.6 Core capabilities

- Full-spectrum biometrics that empower large scale enterprise matching systems, user focused scalable databases, integration with other biometric systems, and customized workflows.
- Physical security access technologies that enable remote and on-premise enrollment for visitors and staff, secure vehicle express lanes for gate entry and exit, passive facility surveillance, and a biometric management control system.
- Multi-modal biometric enrollment that supports mobile, in-person assisted, or self service kiosks, 3rd party enrollment, remote identity verification for civilian and federal government enrollment, and identity proofing.

1.7 Past Performance/Customer Success

- Multi-domain systems fusing biometric, biographic, credential, and digital views of identity
- Multi-modal biometric systems for criminal justice, civil identity, border control, and intelligence community missions
- Unparalleled speed, accuracy, and scalability for fingerprint, face, iris, latent, and Fast-ID searches
- Federal Bureau of Investigation Next Generation Identification – world's largest criminal biometric identification system
- Department of Defense Automated Biometric Identification System – U.S. military authoritative biometrics repository
- Largest government face recognition system supporting visa and passport applicant processing
- Authoritative biometric database for the Intelligence Community

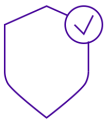
Chapter 2: Our Customers

NSS provides identity solutions to a variety customers throughout the U.S. Federal Government. From law enforcement to critical infrastructure, we provide the solutions you need to protect our country from identity-related threats.

2.1 Law Enforcement

NSS provides thought leadership and technology innovations that enable U.S. Federal Law Enforcement and Homeland Security missions around the world and at home. Our team of biometric and identity resolution experts support some of the largest information technology, biometrics and identity management, and secure credentialing programs within the Department of Justice (DOJ), Justice Biometric Identity Service (JBIS), and FBI NGI.

2.2 National Defense



NSS has spent decades developing and delivering identity solutions to the Department of Defense - video analytics, contactless biometrics, mobile biometric enrollment, installation security, continuous vetting, and everything in between. Our biometric matching solutions power the DOD Automated Biometric Identification System (ABIS) which enables U.S. military global operations.

2.3 Military Installation Protection

We bridge the gap between high-touch force protection and high-tech threat mitigation capabilities to increase the safety of force protection personnel, improve installation situational awareness, and provide secure and frictionless access to high-priority, mission critical resources.

2.4 Intelligence Community

We support the Intelligence Community (IC) and their missions through the delivery of both enterprise and tactical-level identity solutions. By deploying advanced sensor technology with our proven identity intelligence solutions, we are addressing today's national security threats which often hide in plain sight.

2.5 Critical Infrastructure and Key Resources (CIKR)

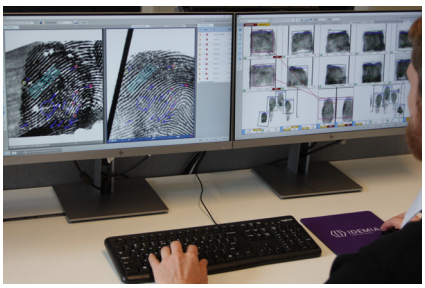
Critical infrastructure includes those assets, systems, networks, and functions—physical or virtual—so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters. NSS utilizes biometric solutions to identify, prioritize, and coordinate the protection of CIKR to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them.

Chapter 3: Biometrics and Forensics

NSS provides a variety of biometric and forensic solutions utilizing IDEMIA's MBIS, with MBSS, STORM ABIS, and LiveScan providing the best biometric and forensic solutions in the market.

NSS has deep penetration in biometrics and forensics with contracts in DOS, DHS, DOD, and DOJ, and specifically within those agencies the Office of Biometric Management (OBIM) and FBI.

3.1 Multi-Biometric Identification System (MBIS)



The Multi-Biometric Identification System (MBIS) Suite is powered by our IDEMIA Multi-Biometric Search Services (MBSS). It is a Commercial Off-the-Shelf (COTS) product forming a system foundation that can seamlessly integrate future modalities and enhancements with minimal effort.

3.1.1 Features and Benefits

- Powerful multi-biometric engine for searching and matching face, finger, palm, iris, and tattoo, designed for speed and accuracy
- Major case prints feature, expanding latent search to entire friction ridge area of hand
- Extended toolset, including minutiae editing tools, image enhancement and filtering tools, latent image sizing controls, and finger selection tools
- Service Oriented Architecture (SOA), built around open system components that easily integrates into your agency's IT architecture and allows internal/external data exchange and manipulation
- Record Archive Service for search and storage of all NIST records, and case documents
- Enhanced criminal case data modeling that supports investigative case management features such as storage of evidence images, case-to-person and case-to-case link information, and the retention of latent print encoding and search history
- Complete digital image repository provided by Oracle or PostgreSQL relational database of all processed records
- Fully modular and highly scalable allowing for upgrades to initial MBIS deployments
- Automated and manual processing capabilities allows for differentiations to be made by expert individuals
- Easily integrated with existing Automated Fingerprint Identification System (AFIS), booking, and collection systems

3.1.2 Use Cases

MBIS is powered by MBSS and supports any MBSS use case as well as use cases of any product with which it is integrated.

3.2 MBSS

MBSS is IDEMIA's core engine for multi-biometric identification designed for both accuracy and speed. It compares biometric data to establish if a person exists in a database. It employs IDEMIA's top performing biometric algorithms for fingerprint and palm print identification, iris recognition, facial recognition, and tattoo recognition. These algorithms consistently perform at the top of NIST rankings. They also drive the world's largest biometric systems in which register more than 1 million records per day and currently exceeds 1.3 billion records.

IDEMIA has a comprehensive range of products powered by MBSS. For example, MBSS powers MBIS and is incorporated into IDEMIA's identity and security products. MBSS is also available to major third-party integrators.

3.2.1 Features and Benefits

- Biometric matching services, including 1:n identification searches, 1:1 authentications, and forensic searches of latent prints
- Image processing services, including feature extraction, template creation, image segmentation and sequence checking
- Database management services including adding, updating, and removing identity records
- Built to manage high throughput and short response times
  - Concurrent 1.3 Billion identity system
  - ~1 Million transactions per hour
  - <3 second response time with ~400 Million identities

3.2.2 Use Cases

Scalable and configurable to meet any biometric use case such as:

- Local services running on Internet of Things (IoT) devices
- Multiple on-premise servers across networks
- High availability through cloud-based deployments
- Any latent search
- Integration into existing or new identity-related systems

3.3 STORM ABIS

IDEMIA STORM is a cloud-native ABIS. It delivers best-in-class fingerprint matching accuracy and the flexibility to scale up or down based on needs, allowing agencies of all sizes to achieve operational efficiencies in their biometric examination operations. It stores, processes, and matches biometric data such as face, fingerprint, palmprints, iris, and scars, marks, and tattoos for the purpose of identification or verification.

Intuitive and streamlined, STORM is designed by examiners for examiners. It is easy to use with only minimal set-up and training needed, and it rapidly provides investigators critical latent print matching information, even right at a crime scene.

3.3.1 Features and Benefits

- Tenprint, palm print, and latent print AFIS support with quality control and comparison
- Enrollment to capture and store biometric data within the system
- Identification (1:n matching) to compare a biometric record against a gallery of biometric records to return possible matches
- Verification (1:1 matching) to compare a captured biometric record against a stored biometric of record. For example, a pic of a face to an image on a driver's license to confirm that person's identity
- De-duplication to resolve identity conflicts by aligning matching biometric records that were not previously associated.
- Person management
- Latent case management, search and comparison, and documentation
- Livescan submissions
- FBI NGI and state-specific via Electronic Biometric Transmission Specification (EBTS) submission interfaces
- Secure connection to cloud deployment through any browser
- Innovative and scalable approach to updates and deployment of new features, keeping customers on the latest technology
- Cost-effective subscription model that operates with minimal setup

3.3.2 Use Cases

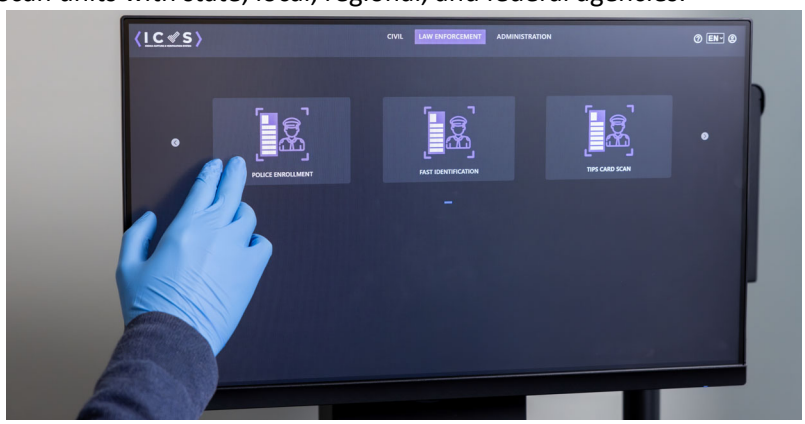
- Law enforcement, criminal investigations
- Border control
- National ID Systems
- Banking and Finance
- Enterprise security and access control

3.4 Livescan

Law enforcement and civil agencies use IDEMIA TouchPrint Enterprise (TPE) LiveScan to speed up the registration and enrollment of biometric data, while maintaining rigorous quality control at each step of the capture process.

TPE LiveScan supports multi-modal biometric data capture and enrollment including fingerprints, palm prints, facial images, DNA, iris, scars, marks and tattoos, and demographics. Registration data is stored and transmitted using industry-standard formats and security protocols.

It's comprehensive fingerprinting solution, designed using IDEMIA's extensive experience in supplying and integrating thousands of LiveScan units with state, local, regional, and federal agencies.



3.4.1 Features and Benefits

- Supports multi-modal biometrics, including fingerprint, palm, face, iris, DNA, scars, marks/ tattoos, and demographics
- Available in multiple form factors, including fixed and adjustable height cabinets
- Includes an FBI-certified scanner to capture and deliver unsurpassed image quality
- Provides automated services such as minutiae extraction as well as image quality assurance and measurements
- Moisture Discriminating Optics (MDO) enable better capture of prints including reduced errors from imperfect subjects
- Track submission status throughout all processing stages and receive responses quickly
- Allows for integration with extensive peripheral options, external systems, and other IDEMIA products
- Fully compliant with FBI NGI EBTS and ANSI/NIST standards

- User interface clearly displays roll-to-slap fingerprints and upper and lower palm comparison results, in real-time.
- Easy configuration that can be interfaced or integrated into existing third-party systems such as record management and computerized criminal history systems.
- Supports electronic submissions to AFIS systems as well as card printers

3.4.2 Use Cases

- Offender enrollment at booking: agencies can record both biometric and demographic data and submit these to applicable agencies' databases
- Identity verification: officers can check if a subject has registered previously with a different identity, by comparing scanned biometric data with a database of existing registrations
- Background checks: agencies can compare captured biometric data with other databases, to link a subject to other events.
- Transportable enrollment via workstation with document verification and liveness detection
- EBTS import/export
- Enrollment Synchronization between ID2Access systems

Chapter 4: Physical Security

Protecting your facility from unauthorized access and on-the-go identity verification are of the utmost importance. We provide the systems you need to verify that individuals have vetted access. NSS has proven success providing physical security to DOS, DHS, DOJ, FBI, and DOD.

4.1 ID2Access Solution

The NSS ID2Access™ Solution presents a comprehensive suite of biometrics-based products designed for end-to-end, secure access and monitoring at mission-critical sites and installations. This adaptable solution supports the enrollment, entry, and exit of both visitors and personnel across secure facilities, leveraging IDEMIA's top-rated identity technologies recognized by NIST.

Tailored to specific use cases, the ID2Access Solution can be configured for on-premises, cloud, or hybrid operation. Its modular design facilitates easy deployment, providing a secure system capable of real-time identifications and analytics, customized to meet unique requirements and specifications. The solution streamlines access for residents, employees, contractors, and visitors, ensuring a secure system that appropriately safeguards personnel and assets while allowing flexibility of movement on and off the installation. The ID2Access Solution plays a pivotal role in transitioning from traditional high-touch force protection processes to advanced high-tech biometric capabilities.

Solution Features and Benefits:

- Increased Situational Awareness of personnel and visitors at entry points and throughout the installation using enrolled biometrics and credentials
- Reduced Vehicle Access Point Bottlenecks with contactless express lanes for individuals who have already provided their credentials, biometrics, and biographic information, for enrollment into the system in person or remotely
- Secure Access Control with secure pedestrian and vehicle access points through credential and biometric based authentication. Smart passive surveillance enhances protection in restricted zones
- Convenient Enrollment
- Safe Entry Approval Processes with the ability to integrate with authoritative databases and curated watch lists
- Scalability allowing for seamless adaptation to future endeavors and technological advancements
- Simplified and Contactless Entry
- Reduced physical interaction between guards and passengers
- Integration with existing systems
- Fast, secure entry and monitoring

Physical Security

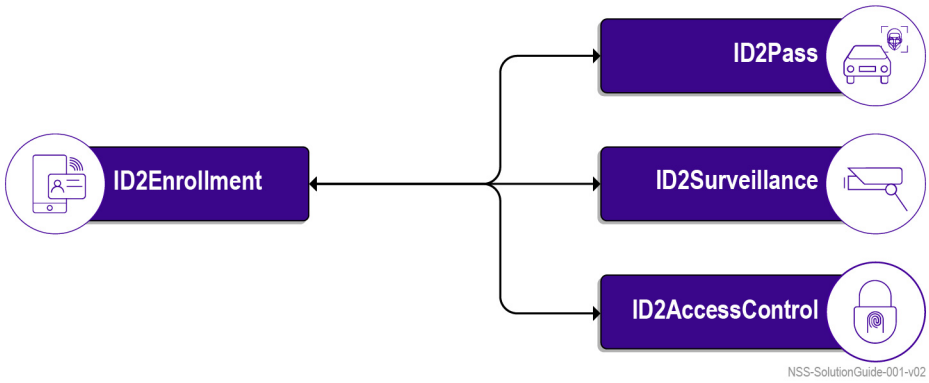
Personnel and visitors enroll effortlessly through ID2Enrollment, either at a designated visitor center or remotely in advance, utilizing a mobile device. Enrolled personnel can then leverage ID2Pass express lanes equipped with biometric sensors, facilitating expedited access. As a vehicle approaches the gate, the sensors perform license plate and/or facial recognition, identifying occupants in real time. The entry process is simplified and contactless.

Within the facility, smart passive surveillance is conducted by cameras, while contactless fingerprint, face, and iris scanners secure specific areas, promptly alerting security officers to any unauthorized attempts to access restricted zones. At the end of the day, the exit process is as seamless as the entry.

The ID2Access Solution has the following major components:

- ID2Enrollment – Remote enrollment for visitors and staff as well as on-premises enrollment
- ID2Pass – Vehicle express lanes for gate entry/exit and guard stations
- ID2Surveillance – Facility passive surveillance monitoring for the Security Operations Center (SOC) and local guard stations
- ID2AccessControl – Biometric Management System for pedestrian access control points that can be monitored in the SOC or at the access points

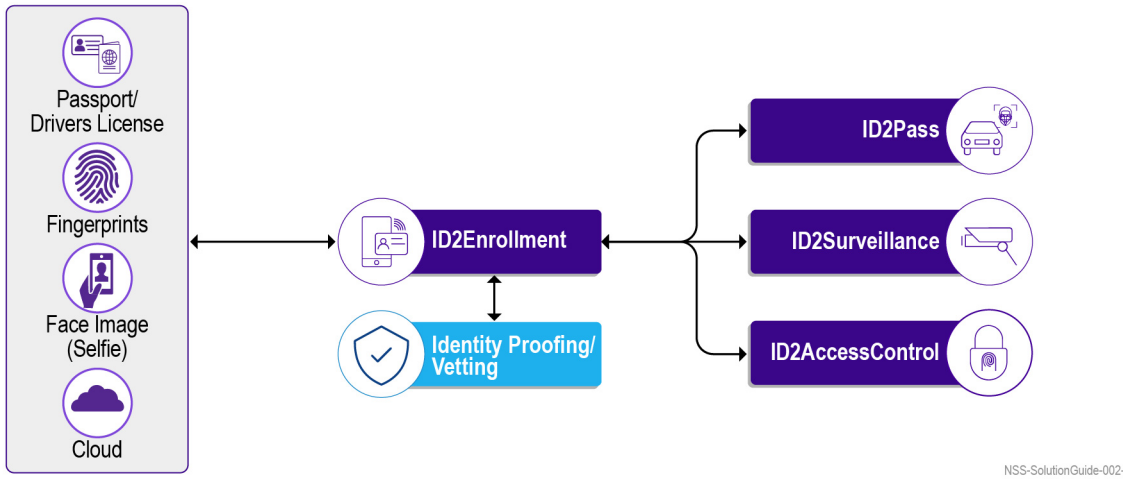
The following diagram illustrates a high-level concept of operation for the ID2Access Solution.



4.1.1 ID2Enrollment – for Visitors and Staff

The ID2Enrollment application empowers employees, contractors, and visitors to verify their identity before reaching the installation express lanes. Installation employees, contractors, and visitors leverage their smartphones to remotely submit credential, biometric, and biographic data, and request vetting for facility access. The application facilitates pre-enrollment for visitors, simplifying the processes of enrollment, check-in, and access. It captures various forms of data, including fingerprints (on-premises), facial images, biographic information, and identification documents such as passports and driver's licenses. This data can be collected through the enrollment web-application on the user's mobile device or in person at a visitor center.

The diagram below provides a high-level concept of operation for the ID2Enrollment component. ID2Enrollment sends enrollment information to the ID2Access server for use in ID2Pass, ID2AccessControl, and ID2Surveillance. Fingerprint capture is available only during on-premises enrollment.



4.1.1.1 Features and Benefits

- Capture Diverse Data: Capture any combination of fingerprints (taken on-premises), facial images, biographic information, and identification documents
- Real-time Verification: Verify documents and conduct liveness detection in real-time.
- Seamless Integration: Integrate seamlessly with external systems through EBTS file generation
- License Plate Recognition: Optionally, vehicle data can be added to the enrollment for use in ID2Pass for license plate recognition
- Flexible Field Addition: Add subsequent fields for collection to include in the enrollment package, ensuring flexibility in adapting to evolving requirements
- Contactless Fingerprints on Premises: The capability to capture contactless fingerprints, enhancing the system's features as technology evolves
- Functions on iOS or Android device
- Integration of existing enrollment workflows and devices
- Collection workflow supports the capture of driver's license, passport, biometrics (face and fingerprints) all in one place

4.1.1.2 Use Cases

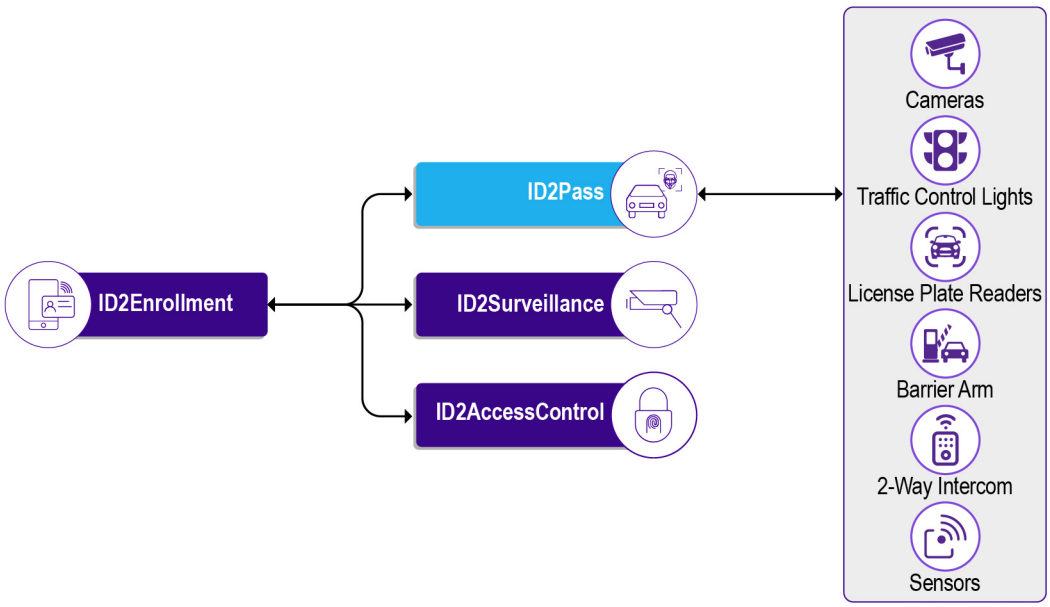
- On-premises enrollment via workstation
- Remote enrollment via smartphone web browser including document verification (remote enrollment) and liveness detection (remote enrollment)
- EBTS import/export
- Enrollment synchronization between ID2Access systems

4.1.2 ID2Pass – for Personnel Entry (Visitors and Staff) and Gate Station Guards

The implementation of ID2Access express lanes is designed to offer a streamlined entry experience for all enrolled individuals, including Common Access Card (CAC)/Personal Identity Verification (PIV) holders, contractors, and visitors. Enrolled individuals can swiftly navigate through the entry gate lane with minimal guard intervention, contributing to a more efficient and expedited entry process. The express lanes utilize facial recognition and license plate detection to perform biometric authentication. Individuals need to be pre-enrolled through the ID2Enrollment system, ensuring that their biometrics and other relevant data are securely captured and stored beforehand. The ID2Pass system employs facial recognition technology to rapidly capture and match facial features and license plate detection technology to identify vehicles, allowing for a comprehensive and multi-modal approach to authentication.

ID2Pass workflows are designed to support the capture and identification of occupants, including occupants wearing sunglasses, face masks, or occlusions that might hinder the full capture of the face. This enhances the system's adaptability to real-world scenarios where individuals may have partial facial coverings.

The diagram below illustrates the high-level concept of operation for ID2Pass. ID2Pass receives enrollments (or enrollment information) from ID2Enrollment and leverages ID2Surveillance for watchlist management, face detection, and face identification. ID2Pass is installed in conjunction with ID2Surveilance. ID2Pass can be deployed without ID2Enrollment if all enrollments are processed through on-premises enrollment such as a visitor center.



4.1.2.1 Features and Benefits

- Contactless Access: The system employs a contactless approach for vehicles through express lanes, allowing for enhanced throughput without compromising security
- Express Lanes with High Speeds: Unencumbered travel is facilitated through express lanes, allowing for swift and efficient entry
- Facial Recognition for First and Second Row Passengers: Facial recognition technology is used to capture and verify the identity of both front and backseat passengers, enhancing security measures
- License Plate Checks (Optional): License plate checks can be optionally performed, adding an additional layer of identification and verification
- Maximized Throughput: The system is designed to maximize access control throughput ensuring efficiency while maintaining a high level of security
- Biometric Identification on the Move: The system enables expedited entry through biometric identification via facial recognition
- Enhanced Focus for Security Forces: By automating badge and identity validation, the system empowers security forces to focus on threat response and other critical tasks, improving overall security posture
- Optimized architecture to support high volume, distributed vehicle access point solutions Facial Recognition, License Plate Recognition, Watchlisting, etc.
- Syncs with ID2Access suite or external software and data repositories
- The ID2Pass identity repository uses NSS developed pre-processing algorithms to support visible and infrared spectrum imaging used to capture in-vehicle occupants

4.1.2.2 Use Cases

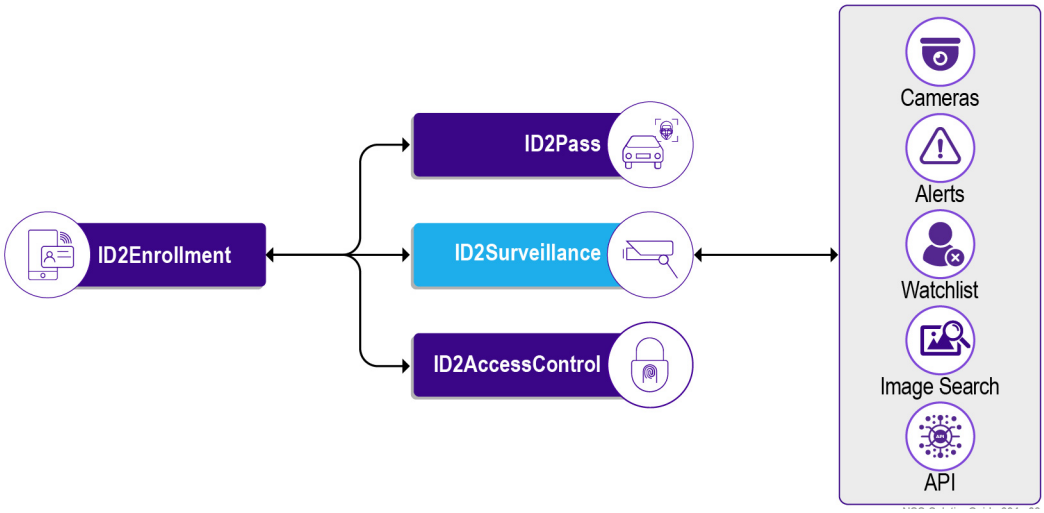
- High-throughput, identity-based vehicle access points
- Face detection through windshield
- Face identification
- Occupant detection and counting
- Occupant seat position detection
- External database support for adjudication/ Defense Biometric Identification System (DBIDS Integration)
- License plate recognition

4.1.3 ID2Surveillance – for Security Operations Centers and Local Guard Stations

ID2Surveillance is a comprehensive surveillance system that utilizes IDEMIA's best in class algorithms to monitor sensitive sites and identify the movement of individuals across the installation. ID2Surveillance employs video processing for real-time facial detection. Real-time passive, intelligent surveillance is used to monitor sensitive locations, enhancing security measures.

The diagram below illustrates the high-level concept of operation for ID2Surveillance. ID2Surveillance receives enrollment information from ID2Enrollment via the ID2Access server. ID2Surveillance is used for managing enrollments and processing face detect and face identification requests from ID2Pass. ID2Surveillance can be deployed independently and integrated into an existing application using the fully featured API. ID2Surveillance uses the ID2Access GUI for

configuration and alerting. The ID2Access GUI is used to visualize all the ID2Access Solution component in a single web view.



4.1.3.1 Features and Benefits

- Biometrically Enabled Alerts: The system provides biometrically enabled alerting on enrolled individuals for situational awareness
- Passive, Intelligent Surveillance: Passive, intelligent surveillance is employed, utilizing real-time facial detection to monitor sensitive locations. This enhances the security infrastructure by proactively identifying and alerting on individuals in monitored areas
- Data Analysis from Cameras: Deployed cameras gather data in real-time. This data provides guards with information on any enrolled person as they pass through Access Control Points (ACPs)
- Real-time video analytics offering supporting facial recognition workflows
- Configurable to enable recording of surveillance events
- Supports industry standard network camera feeds, webcams, and multi-spectral imaging devices
- Optimized NVIDIA architecture and algorithm to maintain near real time performance
- Capable of deployment on edge embedded devices or operation within a centralized system
- Fully featured API that supports integration with partner solutions

4.1.3.2 Use Cases

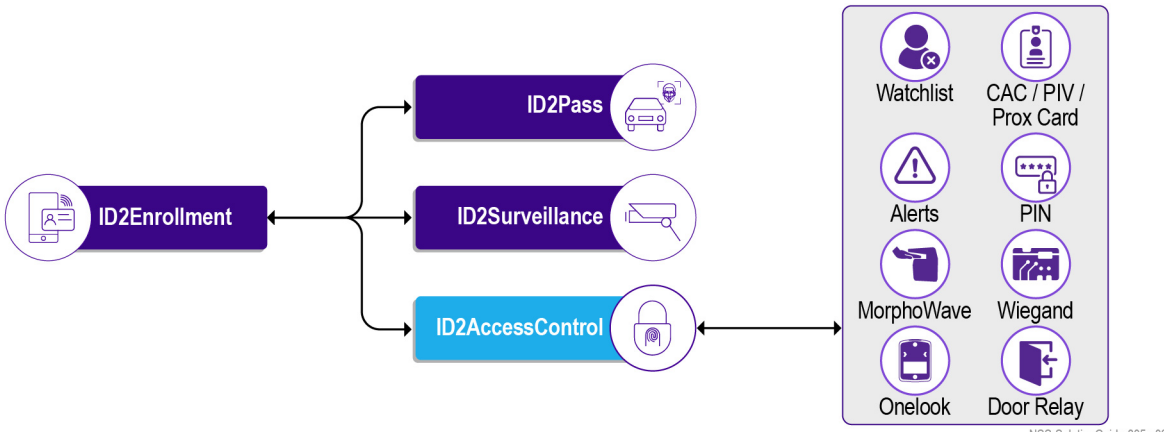
- Overt or covert surveillance
- Integration with existing camera infrastructure
- Watchlisting
- Enterprise deployments
- Embedded deployments for drones, and mobile edge compute, etc.
- Integration into existing systems via API

4.1.4 ID2AccessControl – For Security Operations Center and Local Enrollment

ID2AccessControl is a comprehensive biometric management platform containing a range of biometric capabilities. It connects biometric sensors into access points and matches acquired biometrics against the ID2AccessControl database. The platform monitors configured access points and generates reports on demand. It provides alerts for unknown persons or identities. ID2AccessControl is designed to provide an innovative and centralized approach to access control, leveraging biometric authentication and identity management. The platform allows for the granting or denial of access to a facility based on a centralized and connected matching system. This decision-making process is complemented by IDEMIA's multi-factored approach, which includes biometrics, CAC/PIV, proximity card, and Personal Identification Number (PIN).

All use cases support IDEMIA biometric collection devices, such as the MorphoWave and OneLook. MorphoWave provides PIV-certified fingerprint collection that matches against existing contact fingerprint enrollments with built-in Proximity card reading for PIV cards.

The diagram below illustrates the high-level concept of operations for ID2AccessControl. ID2AccessControl retrieves enrollments from ID2Enrollment. It can be installed alone as a complement to existing access control systems. The ID2Access GUI is used to visualize all the ID2Access Solution components in a single web view.



4.1.4.1 Features and Benefits

- Real-time Situational Awareness: Dashboards provide real-time situational awareness of personnel and visitors on the installation
- Bottleneck Reduction: The system is effective in reducing or eliminating bottlenecks at various points, including pedestrian gates, lobbies, visitor centers, and high-access facilities, thereby expediting commute times for personnel
- Multi-Biometric Support: The solution supports multiple biometric modalities, including fingerprint, facial, and iris recognition, providing flexibility and adaptability
- Integration with PACS: Seamless integration with Physical Access Control Systems enhances overall access management
- Blacklists: Blacklists are used to indicate known individuals for which access should be restricted adding an extra layer of security

- Identity-Based Alerting: Identity-based alerting is enabled through real-time biometric matching
- Contactless Reading of CAC and PIV Cards: The system supports contactless reading of CAC and PIV cards, enhancing security with two-factor authentication (2FA)
- Touchless “Wave” Fingerprint Readers: Touchless “wave” fingerprint readers with built-in credential-based authentication secure sensitive locations
- Wiegand Interface Integration: Integration with Wiegand interfaces facilitates compatibility with various access control devices
- EBTS Support (Import/Export): Support for EBTS allows for the import and export of biometric data
- Augments the existing access control systems by providing centralized biometric authentication and identity management at defined physical access points
- Third-party capture devices can be integrated
- The ID2AccessControl product serves as the core integration interface to orchestrate the features within the other products of the ID2Access solution

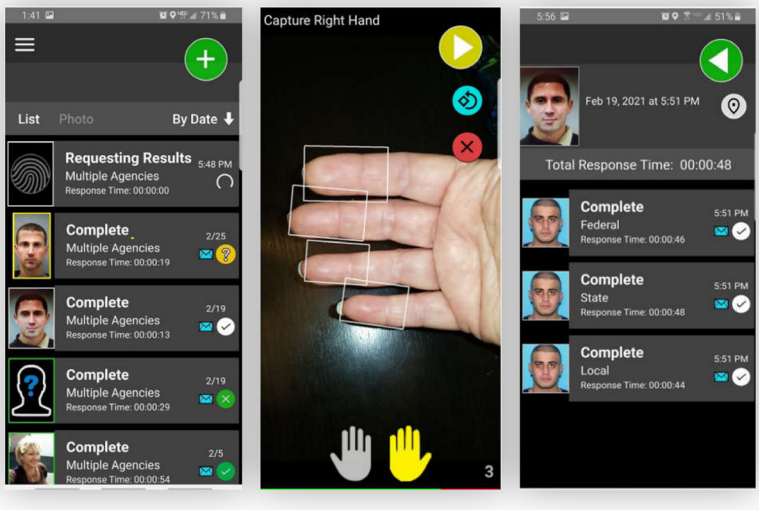
4.1.4.2 Use Cases

All use cases support IDEMIA biometric devices, such as MorphoWave and OneLook.

- Pedestrian access points
- Multi-factor authentication for finger, face, iris, CAC/PIV/Proximity card, and PIN
- Wiegand integration into PACS
- Direct door control (via Relay)

4.2 Mobile Biometric Check

Mobile Biometric Check (MBC) is an advanced mobile application to support law enforcement, border patrol, and fraud investigation officers conduct identification checks on the go. Officers can use their smartphone camera to verify a person’s identity by matching their fingerprints or face against an authorized central law enforcement database. IDEMIA’s industry-leading face and finger identification system quickly returns search results for officer review.



MBC uses cutting-edge contactless technology to automatically detect and capture facial images and fingerprints for rapid identification. This addition of advanced biometric capabilities to their smartphone help keeps officers safe when making identifications in the field. With MBC, law enforcement, border patrol, fraud investigators, and military personnel can make informed decisions by identifying individuals based on facial images and/or fingerprints.

MBC uses the camera within a mobile device to capture high quality fingerprint images. The capture process does not require the subject to touch the device in any way. Subjects simply place their hand approximately 6 inches in front of the device screen. The MBC application automatically detects an individual's fingerprints and provides a visual indication plus a tactile vibration when the capture process has completed. The images are captured in a completely contactless manner. MBC operators are provided the option to view the captured images prior to submitting them for search.

Immediately following the successful capture of a subject's biometrics, MBC transmits them for search. MBC provides operators with a list of searches along with their status within the main screen of the app. Search results can be sorted by date and displayed in either a detailed list or as thumbnail images. Upon receiving the results of a search, the device vibrates and displays the search details. Positive identifications are updated to display an individual's mugshot (when available) as well other details about the subject. The information that is displayed can be configured to meet an agency's specifications.

The MBC application can be configured to authenticate users via an existing user database, such as Active Directory. Users are required to enter a username and password prior to accessing the application. All search submissions and responses are handled via an HTTPS exchange and are EBTS and NIST compliant. The MBC application is publicly available on the Apple App Store and Google Play Store. Preconfigured versions of the MBC application can be made available to support distribution via an agency's private app store.

4.2.1 Features and Benefits

- Configurable for use with databases across multiple levels such as local, state, federal, etc.
- Pairs with IDEMIA's industry-leading face and finger identification systems and algorithms
- Response time in seconds for face and fingerprint recognition results
- Can be configured to read any ISO 18013-5 compliant mobile ID
- Automatic, contactless detection and capture of facial images and fingerprints in the field
- Secure submission of captured biometrics against multiple databases and agencies
- Easy-to-use safe operation and collection of biometrics
- Available on existing mobile devices to reduce cost and increase accessibility
- Available on the App Store and Google Play and can be distributed and managed by an organizations' existing mobile device management system

4.2.2 Use Cases

- Law enforcement can easily identify individuals that may not have an ID or present fraudulent identification documentation or are impaired or unresponsive
- Contactless technology is ideal for use with subjects in hands-up or handcuffed position.
- One-hand operation, leaving the other hand free to facilitate officer safety

4.3 Handheld Biometric Collection

IDEMIA provides a handheld biometric collection for MBC, described above, and a similar device for the tactical operational environment.

We provide complete mobile flat and rolled enrollment, verification, and booking. This FBI Appendix F Certified FAP 50 Mobile 10-Print Scanner, AFIS-compliant scanner provides mobility, performance, and compact form factor. Light-emitting sensor (LES) technology delivers fixed and mobile FBI certified fingerprint imaging in an exceptionally durable, lightweight scanner. LES-based biometric solutions provide picture-perfect image quality in both direct and indirect sunlight and are resistant to finger contaminants such as grease, oil, water, dust and chemicals

Small enough to fit in a shirt pocket and built for law enforcement, military, border control and national ID programs. It resists latent fingerprints, dirt, cold, heat, bright lights, and direct sunlight. There are no silicone membranes or light sources to replace. Each unit can operate for hours using power provided by a smartphone or other mobile device. Available in embedded or standalone versions.

4.3.1 Features and Benefits

- Contactless biometric capture for face and fingerprint using phone camera
- Built-in capture devices for iris and friction-ridge fingerprints
- Contact smart card reader
- Import/Export of EBTS-compliant files
- Onboard and remote matching
- Rapid dry finger capture
- No need to clean latent prints in high-volume situations
- Unaffected by extreme temperatures, direct sunlight, or bright artificial lights
- Compact, lightweight, and rugged
- Rejects common spoofing attacks
- Emits no bright lights during scans
- Meets or exceedsU.S.military durability specifications
- Faster in-device charging
- Compatible with IDEMIA applications such as Mobile Biometrics Check and Universal Enrollment
- Integrates with the Samsung S20 Tactical device

4.3.2 Use Cases

- Law enforcement, military, border control and national ID programs
- On-the-go environments
- Embedded or stand-alone

4.4 VisionPass and VisionPass SP

IDEMIA's VisionPass and VisionPass SP are access control devices employing facial recognition and 3D face modeling to provide the highest levels of security and anti-spoof capabilities.

The SP version provides accurate and fair matching results in less than one second, for all users, in any lighting. This improves the user experience while maintaining a high level of security. VisionPass SP is a sleek and compact terminal developed to ease integration into various environments. With an eco-friendly design it offers automatic deep-sleep mode capability, significantly reducing power consumption. Integrating the latest cybersecurity standard, VisionPass SP embeds a secure-by-default configuration to enforce security in the field to prevent cyber-attacks.

VisionPass SP has been developed with customers and end-users in mind, to meet both security and convenience requirements. Furthermore, VisionPass SP has succeeded in reducing our environmental impact, with a greener design and energy saving.

4.4.1 Features and Benefits

- Multi-optic setup includes InfraRed, Visible Light, and 3D cameras
- Multifactor authentication with built-in RFID readers for Biometric Data, Card, PIN Code, or QR Code
- Robust and reliable device that thwarts all kinds of spoofing attempts
- A sleek and compact terminal with an eco-friendly design that provides accurate and fair matching results
- Secure DevOps and Pen tested
  - Secure booting and authenticity checks
  - Crypto chip to secure sensitive data
  - Trigger alarms in case of tampering
  - Adjustable capture area to confirm the intention of user who are trying to gain access
  - Embedded anti-spoofing capability
  - Secure communication with a network and door controller over new Open Supervised Device Protocol (OSDP)
- Provides secure and convenient access for even the most critical environments and customers
- Ensures accurate matching with fast results and throughput
- Independent of environmental factors such as lighting conditions or face masks

4.4.2 Use Cases

- Facial recognition for access control
- Multi-factor authentication with facial recognition and PIV/CAC

4.5 MorphoWave XP and SP

To protect their premises, organizations require access control solutions that are efficient, fast, and convenient. A contactless fingerprint scanner provides an optimum answer in high throughput workplaces. IDEMIA's MorphoWave™ contactless fingerprint solution scans and verifies 4 fingerprints in less than 1 second, through a fully touchless hand wave gesture.

Two versions of the MorphoWave™ contactless fingerprint scanner are available:

- MorphoWave XP: an extended Performance biometric reader for the most demanding projects; up to 100K user records in 1:n mode, up to 60 people per minute, with a large color tactile screen for user interaction, and time and attendances use cases
- MorphoWave SP: all of the essentials of MorphoWave technology with a Simplified Profile up to 10K user records, and a simplified user interface via multicolor LED indicators

Embedded with IDEMIA's latest advances in the use of AI, these two ergonomic biometric readers work efficiently with wet, dry, dirty hands or even damaged fingerprints. In addition, the card reader of MorphoWave natively supports HID Prox, iClass, MIFARE, DESFire, and mobile access control solutions. It is also capable of scanning printed QR codes for visitor management.

Already integrated with more than 25 of the industry's leading access control systems, MorphoWave technology has become the benchmark in frictionless access control. This advanced fingerprint solution range secures high traffic access points in the world's largest financial institutions, critical infrastructure facilities, universities and healthcare organizations.

4.5.1 Features and Benefits

- Touchless 3D fingerprint technology
- FBI Image Quality Specifications (IQS) certified sensor
- Simultaneously scans all 4 fingers
- True frictionless access control
- High speed acquisition and matching with a wave of the hand
- 20% more accurate than competing contactless systems
- Convenient, secure, versatile, easy deployments with high throughput

4.5.2 Use Cases

- Used by financial services, marquee event arenas, universities, and government facilities worldwide.
- Addresses the increased interest contactless fingerprinting

Chapter 5: Augmented Vision

Augmented Vision is a video analytics solution that helps survey and protect buildings, infrastructure, and areas of interest by making sense of all available data. It employs the best of IDEMIA's technologies to provide comprehensive security and awareness.

An immense volume of videos and images exist today due to the prevalence of Closed Circuit Television (CCTV) streams, smartphones, and more. Augmented Vision protects areas of interest in real time. It can help prevent security incidents in highly frequented secured areas, bases, and governmental spaces but also to ensure frictionless access to restricted areas for authorized personnel, all while protecting citizens' privacy with the highest level of data protection.

Augmented Vision also analyzes massive amounts of video streams and photos to help find subjects and objects of interest in post-event investigations. Augmented Vision is designed to make sense of all available video and image data, allowing operators to quickly create leads to solve crimes.

It provides an Identity Matching Software solution for efficient real-time and post-event video analytics utilizing COTS hardware. Augmented Vision manages 5 billion biometric records worldwide, is top-rated by NIST across multiple biometrics, and has a 99.9% true alert rate. Augmented Vision solution is built to scale with customer needs, providing seamless security whether you're protecting a single building or an entire enterprise.

5.1 Features

- Facial recognition
- Pedestrian detection
- Vehicle detection
- Color filters
- Object linking/association
- Meta tagging
- Event Analytics
- Parallel processing
- Collaboration
- Geo tracking
- License plate recognition
- Event prioritization
- Hybrid deployments
- Embedded compute
- Scalability
- Designed for CCTVs
- Proprietary Neural Networks
- Versatile plug-in ability

5.1.1 Real-time Video Analytics

- Identify and track high-risk and vulnerable persons of interest across multiple cameras
- Extract and capture faces of pedestrians, motorists, license plates, vehicles, and other video data
- Trigger live alerts for awareness across the entire area of operation
- Real time video analytics - This solution monitors CCTV cameras and alerts security staff if necessary. The identification of persons of interest is based on biometric and non-biometric attributes (e.g., face, silhouettes, vehicles and objects of interest)

5.1.2 Edge-embedded Computing

- Designed for ease-of-use and fast deployment on the NVIDIA Jetson computer platform
- Provides full system capabilities in a high performance, low-power computing package
- Allows for standalone and hybrid deployments to accommodate all customer use cases and environments
- Video analysis at the point of capture - This video processing solution is built on the world's leading embedded Artificial Intelligence Edge computing platform

5.1.3 Post-event Video Processing

- Automatically recognizes, records, and classifies persons and objects of interest
- Improves suspect or person-of-interest traceability and detects interpersonal associations
- Allows a single workstation and analyst to process large scale cases quickly and efficiently
- Post-event video analytics- IDEMIA's video analytics tools and algorithms help investigators find and qualify information from video sources faster using automated technology

5.1.4 Small Deployment Option

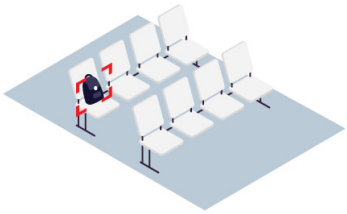
Augmented Vision gives you the flexibility of small deployments, built on the NVIDIA Jetson (Embedded ARM64 Device + GPU and SoC), for covert investigations and for distributed solutions where infrastructure is sparse and communications are limited. This Edge Embedded appliance is a high-performance, low-power computing device, optimized for IDEMIA's next generation video analytics and computer vision solutions.

Augmented Vision can be used as a standalone or as a hybrid solution and is therefore compatible with all existing cameras. It can be installed rapidly for quick and easy deployment. The Edge Embedded solution supports diverse operations – from multiple cameras and high person throughput to single camera deployments and covert or isolated applications.

5.2 Benefits

Detect and identify a person of interest

Secure access for authorized personnel



Detect suspicious objects and alert

Detect and recognize a person and identify clothes using a color filter

Detect and warn of an intrusion

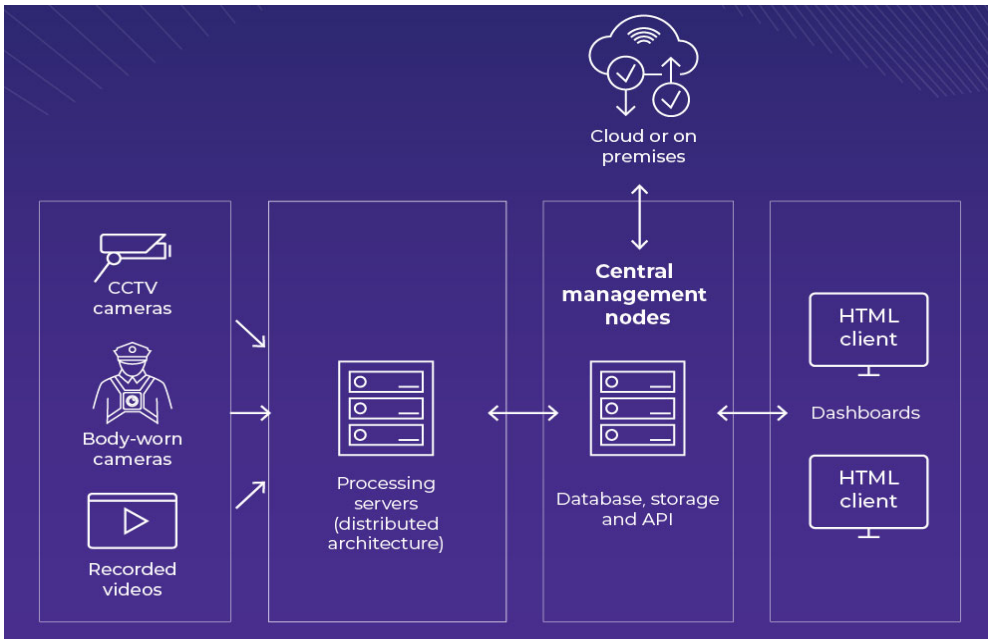
Speed up post-event investigations

5.3 Use Cases

- Prevent security incidents in highly frequented areas, bases, and governmental spaces
- Frictionless access to restricted areas for authorized personnel, while protecting citizens' privacy with the highest level of data protection
- Survey and protect buildings, infrastructure, and areas of interest in real-time or post event
- Commercial and federal clients and in our own ID2Surveillance.
- Government/Public Sector
- Airports and Public transportation
- Corporate and commercial
- Stadiums and arenas
- Gaming and entertainment

5.4 How does Augmented Vision work?

Augmented Vision analyzes scenes in the processing service from a CCTV camera's field of view (an image or recorded video), live and/or post-event. Data is then converted into mathematical models and analyzed with respect to known object types e.g. faces, people, vehicles, license plates etc. and compared (where applicable) to a client's database. The results of this analysis are presented to the operator in various dashboards.



5.4.1 Allocate

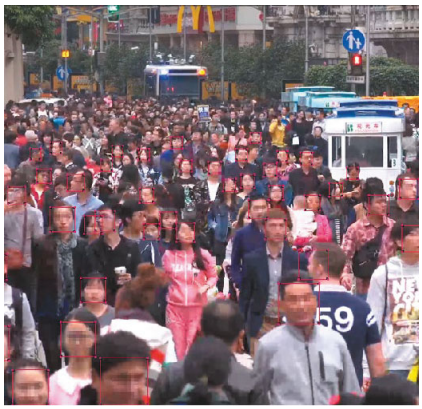
Previously, it would have taken multiple people and weeks of work to view 500 hours of video footage to study half a million faces. Augmented Vision can complete this in almost a day on a small workstation system with one single officer.

5.4.2 Investigate

When investigating a suspect you need to leverage all sources, including processing and analyzing a large variety and quantity of video and image formats.

Once Augmented Vision has been fed the video and image data, it recognizes, records, and classifies persons and objects of interest such as silhouettes, faces, vehicles and license plates. This automatically improves suspect traceability and enhances associations that were previously unknown.

5.4.3 Transition video production to actionable intelligence



In highly frequented public or private spaces, the use of CCTV cameras can help spot potential threats, preventing situations from escalating and ultimately keeping people safe. However, it is not always easy to understand the complexity of many CCTV streams simultaneously collected over many hours. Determining your key persons of interest (POI) is important, but how do you survey everything at the same time to make sense of momentary events?

Augmented Vision performs live monitoring across thousands of CCTV cameras, differentiating between individuals based on biometric and non-biometric features to identify potential POI and automatically alert security staff upon a match. This allows officers more time to follow up on actionable intelligence, rather than reviewing endless video streams.

Augmented Vision can identify high risk and vulnerable individuals while following POI across multiple cameras and alert officers about targeted events of interest by identifying license plates, faces, silhouettes and more.

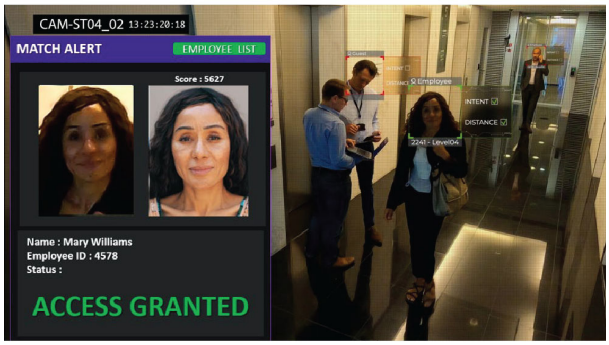
Examples of events analytics

- Intruder detection
- People counting
- Mask detection
- license plate
- vehicle identification
- soft biometrics data such as gender and age

5.4.4 Solve

With Augmented Vision, you do not have to spend endless hours watching video footage or looking at images. This cutting-edge tool identifies normal background noise in a scene and detects, extracts and classifies pedestrians, faces, vehicles and license plates, identifying potential clues faster and more effectively. As a result, you maximize resources to obtain actionable intelligence faster.

5.4.5 Authorize



Augmented Vision can be easily integrated with any existing access control software, leveraging IP cameras to manage access facilities. Facial data is pushed either from server to server or from server to door controller, allowing Augmented Vision to fit all ecosystems. This technology can easily identify visitors and collaborators at a distance, creating a seamless biometric identification experience. IDEMIA's advanced algorithms, enable in-motion recognition while ensuring the highest accuracy.

Using facial recognition means that no direct contact is needed with the equipment, a hygienic alternative to other systems available on the market. The strength of the solution resides in its ability to analyze the entire situation around access points. It is capable of enabling group access and detecting suspicious behaviors. It increases security by spotting attempts at tailgating and then locking a door when an unauthorized person is identified in the field of view.

Chapter 6: Enterprise Identity

NSS Enterprise Identity solutions include Identity proofing and enrollment services powered by the world's most widely-used, accurate biometric matching service – MBSS – enabling identity intelligence for the homeland, defense, and intelligence markets.

NSS offers enrollment capabilities tailored for the validation of numerous document types including state issued IDs, CAC/PIV credentials, Trusted Traveler IDs, U.S. Immigration Credentials, Passports, and Industry issued credentials containing a barcode. Our solutions have comprehensive document capture and identity proofing and verification in both mobile platforms and fixed registration locations. These solutions:

- Deliver scalable, agile, top-performing match results to our nation's most sensitive missions
- Support diverse biometric modalities: Face, Fingerprint, Iris, Palm, Pedestrian, Tattoo
- Fuse biometric, biographic, credential, and digital views of identity for unparalleled match results in the most challenging operational settings
- Leverage cutting edge, machine learning algorithms that match when others can't
- Provide proven reliability - 60% of U.S. Federal biometric systems of record

NSS enterprise identity clients support large scale MBSS deployments for FBI, DOD, DOS, and members of the IC.

6.1 Identity Proofing

Through the NSS Identity Proofing Platform, identity documents are scanned and validated through embedded security features, verified via reach back into credential issuance systems of record (e.g., driver's license, CAC, and Personal Identity Verification [PIV]), and aligned to a real-world identity through third-party data aggregation platforms, such as federal or state government databases or public records. This feature validates not only the identification credential but the holder of the credential as well. The IAL2 compliant document and identity verification can be performed remotely via desktop and mobile applications or in-person via a self-serve kiosk reducing identification document issues.

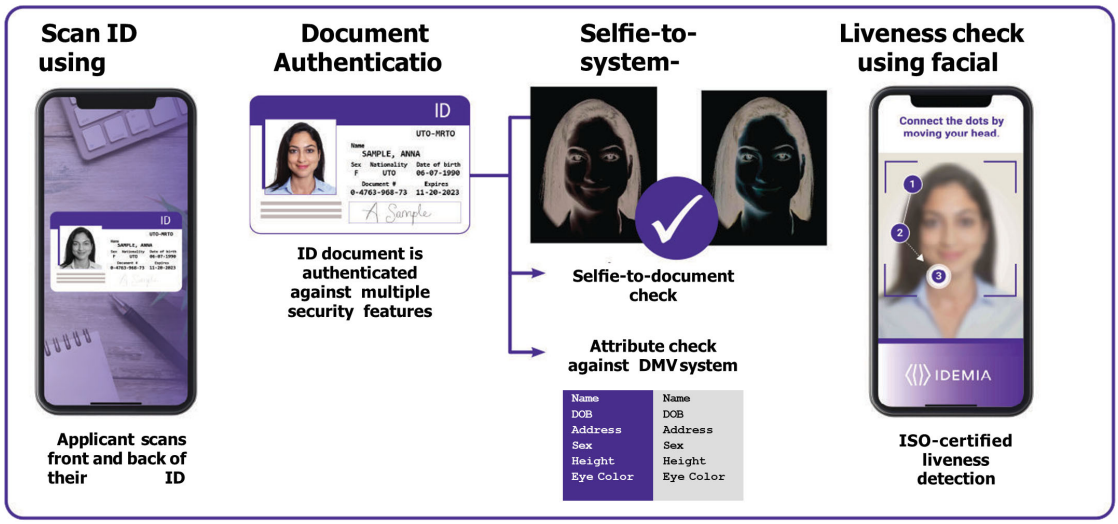
The NSS Identity Proofing Platform is a powerful identity verification service for secure, seamless enrollee identity verification. The platform combines validation and verification with data collection to not only improve remote identity proofing and vetting process efficiency, but also to allow organizations to gain higher assurance in an individual's identity. It is the first step in a robust, reliable identity management process. In alignment with NIST 800-63A IAL 2 and FIPS 201-2 remote identity-proofing principles, the platform currently has the following validation and verification services:

- Identity Resolution – Verifies that the identity claimed by the enrollee is accurate and exists in the real world by comparing it to identity documents provided, or to an issuing authority's system of record
- I-9 Document Authentication – Verifies the I-9 document presented by the enrollee to support his/her identity claim is genuine
- Enrollee Verification – Verifies that the enrollee is the person with the claimed identity using biometric matching combined with liveness detection
- Validation against Issuing Authority Records – Verifies that the presented identity evidence corresponds to the records of the organization that issued that evidence

6.1.1 ID&V

IDEMIA's Identity and Verification (ID&V) solution is a powerful digital identity verification service using document authentication and photo/data comparison against authoritative government records. It offers government agencies the means to securely verify an individual's identity. ID&V allows Relying Parties with customer-facing online services to verify a user's identity by validating their submitted identity documents.

As shown below, customers can complete transactions online, reducing the need for in-person office visits or manual processing of identity documents, without sacrificing identity security. For the person whose identity is being verified, the process is as easy as taking and uploading photos of their identity document (e.g., a driver's license) and a selfie.



The power of the solution lies in IDEMIA's ability to verify identity attributes and face images against government-held data, thanks to our longstanding relationships with state and federal government agencies—without storing or retaining personal data in the cloud. Additionally, the solution can easily be configured to draw on alternate data sources for enhanced identity assurance.

The solution addresses the vulnerabilities created by existing password and knowledge-based authentication methods and can be configured to a desired level of certainty, from secure to ultra-secure, depending on the sensitivity of the transaction.

6.1.1.1 Features and Benefits

- Document verification and Claimed identity verification captures a picture of the user's identity documents to verify their validity. Users may submit multiple identity documents to increase the Level of Assurance (LOA) of their identity
- Issuer verification confirms that the issuer or other authoritative sources validate the user's identity and documents
- User verification has face matching with liveness detection features verifying that the user interacting with the service is a real person and that the user's identity corresponds to the one supported by the document
- Global coverage supports over 500 different ID documents for over 195 countries. It manages multi-modal biometrics checks and connection to various trusted databases and AML/CFT watchlists
- Omnichannel customer journey enables enterprises to onboard customers through a variety of different channels: in branch, assisted by agents equipped with trusted devices, or remotely using smartphones and web platforms
- A single API unifies all ID verification processes, connecting to internal or external sources. It enables enterprises to swiftly integrate the solution and add complementary checks when needs arise (e. g.,new use cases, evolving regulations, etc.)

6.1.1.2 Use Cases

Anywhere identity proofing is needed, for example: Government Agencies, NASA, and DOT.

6.1.2 IdentoGO

IdentoGO provides a wide range of identity-related services with our primary service being the secure capture and transmission of electronic fingerprints for employment, certification, licensing and other verification purposes – in professional and convenient locations.

The IdentoGO solution is a mobile handheld solution that offers organizations a means to perform in-person identity proofing and enrollment for its workforce. The IdentoGO service can be used in conjunction with the ID2Secure platform to meet current and future emerging and evolving requirements for identity management. For the remote proofing capability,

the IdentoGO service can be used for exception handling as needed. For ID2Secure the IdentoGO service can deliver NIST 800-63A LOA3 service for identity enrollment/assurance.

If you've recently applied for a job, adopted a child, traveled through TSA PreCheck® or any number of standard day-to-day situations requiring fingerprint identification, chances are the process was simplified and secured by IdentoGO.

6.1.2.1 Features and Benefits

- Security – Our employees undergo comprehensive background checks and an extensive (and recurring) security training to provide you with the highest level of security
- Speed – Our enrollment agents are trained to ensure your paperwork is in order and fingerprints are captured quickly so that you can get on your way. All IdentoGO Centers are equipped with Live Scan systems to ensure quality fingerprints. Results are returned in a matter of days rather than weeks
- Accuracy – IdentoGO Centers benefit from the latest technologies developed by IDEMIA for speed and precision. Our staff is measured on their accuracy to ensure maximum efficiency and convenience
- Convenience – Set your online appointment by selecting a date, time and location that best suits your schedule. We are constantly adding new locations to our already abundant IdentoGO Centers
- Professionalism – Our staff receives on-going training to manage the entire process with professionalism from the moment your appointment is booked

6.1.2.2 Use Cases

- Digital fingerprinting services for a wide variety of state agencies, programs, and industries
- Commercial service partnerships for dynamic, security-minded individuals and business
- Consumer Services - Livescan Fingerprinting, photo services, Fingerprint cards, and Personal History Checks
- Government facility access capturing, verifying, and documenting an individual's identity for access to military bases and secure facilities
- Law enforcement identity verification and documentation book-and-release, e.g., suspects apprehended in remote locations, and when a suspect is unable to come to a jail to be booked
- Health and human services vetting performing the background check at the time of the home inspection in case of vetting for foster care or adoption, reducing the number of visits and time to process
- Institutions requiring fast, high-volume background checks such as schools having the tablet on site to perform background checks on teachers when they interview for a position, or parents on the day of a school trip
- State agencies where tablet offers an easy way for individuals to get cleared for various jobs, and to authenticate identities for issuance of driver licenses through the Department of Motor Vehicles (DMV)

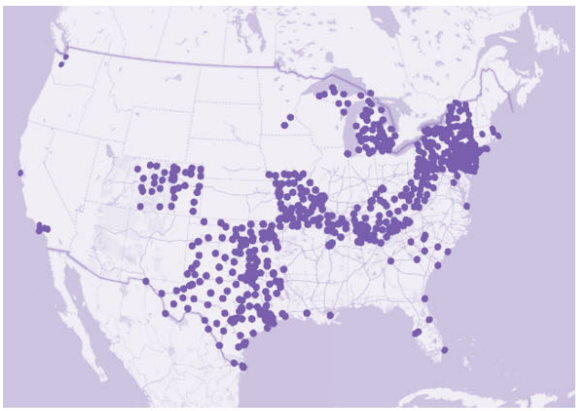
6.2 Enrollment Services

IDEMIA provides a wealth of enrollments services for your convenience.

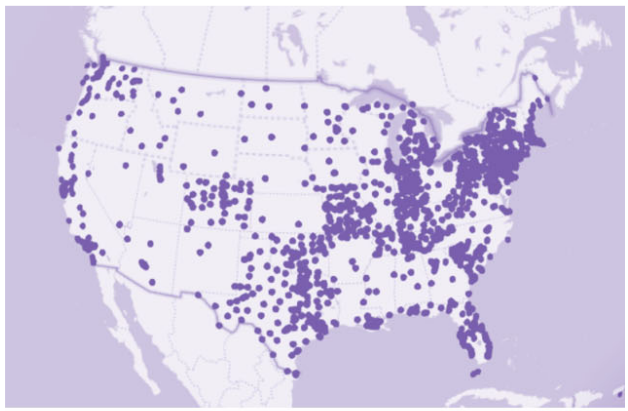
These include:

- Mobile enrollment to enable systems such as TSA PreCheck®
- The Universal Enrollment Platform (UEP) solution that delivers a complete high-performance fingerprinting solution combined with high availability and reliability
- The next generation cloud-based product CARES that delivers end-to-end fingerprint transaction and background check processing
- An enrollment tablet that enables multi-biometric capture from anywhere, at any time, bringing the functionality of the DMV front office to alternate locations

IDEMIA has an extensive nationwide enrollment center footprint



UEP Today: 600+



UE Potential: 1400+

Includes UEP, UES, and SEP Networks

6.2.1 Mobile Enrollment Capabilities

With TSA PreCheck®, you can breeze through airport and railway security. Keep your shoes, jacket and belt on; your laptop in its case; compliant liquids in your bag; and enjoy a better overall airport security travel experience. This allows low-risk travelers to experience faster, more efficient screening at participating U.S. airport checkpoints for domestic and departing the U.S. for international travel. IDEMIA Enrollment Trucks allow TSA PreCheck enrollment anywhere.

- IDEMIA Mobile Enrollment Trucks are on the move, providing TSA PreCheck enrollment services
- These trucks enable 1,000+ mobile fingerprinting sessions for state and federal customers annually
- IDEMIA utilizes a pool of 100+ employees who perform these enrollment events
- Events range from less than 20 applicants to well over 1,000

ADA-compliant locations are available.

6.2.1.1 Features and Benefits

- Enrollment Trucks
- Mobile fingerprinting
- Professional, trained Staff
- Convenient, accurate, fast, and secure biometric collection
- Mobile access to IdentoGO services through mobile enrollment trucks

6.2.1.2 Use Cases

Anywhere mobile enrollment is needed such as:

- Airports
- Railways

6.2.2 Universal Enrollment Platform

IDEMIA Universal Enrollment Platform (UEP) solution provides our customers with a complete high-performance fingerprinting solution combined with high availability and reliability. Based on active contract performance metrics across more than 30 state and federal programs and Transportation Security Administration (TSA), we meet 99.5% system availability and exceed this requirement on all of our current state and federal Enrollment Programs.

Universal Enrollment is an advanced, end-to-end managed enrollment solution that enables the capture of biometrics, documents, information, and payment for the delivery of mission-critical services for agencies nationwide. UEP incorporates features that integrate with and support agency licensing and employment workflows to enable seamless operations that yield quicker turnaround times and enhanced customer service.

For Physical Infrastructure recovery, our UEP solution is available (24x7x365) with components running in a distributed fashion across multiple Amazon Web Services (AWS) availability zones (data centers) with persistent data replicated across AWS Regions. Within a region, software components are “active-active,” meaning traffic is simultaneously processed by multiple AWS data centers. The resulting solution can withstand a full outage of a single AWS data center within a region without the need to invoke contingency plans.

Our next generation, advanced technology platform brings applicants the latest solution for data integrity, data security, fingerprint image quality, data storage, and program metric reports. Unlike other industry vendors, we commit an entire team to each program to ensure a successful deployment and ongoing support throughout the program.

6.2.2.1 Features and Benefits

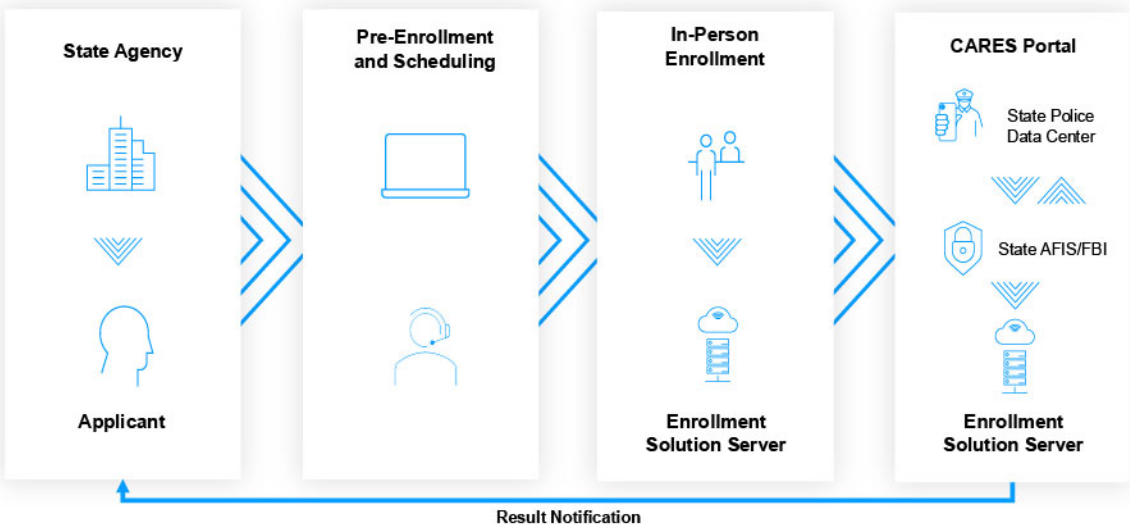
- End-to-End Managed Service
- Online self-service where applicant enters biographic info, schedules an appointment, takes payment (when applicable), and can check status
- In-person enrollment where an enrollment agent collects & verifies applicant identity, capture biometrics, and collects payment (when applicable)
- Optional call center support where applicants can speak to a Customer Service Representative who can enter pre-enrollment details on their behalf by phone
- Administrative portal & help desk to access monthly reports that provide insights and trends on the quality of prints captured where data is further broken down by age of applicant, gender, enrollment center location, and more
- Speed with results delivered back to authorized entity in hours as opposed to days or weeks
- Industry leading quality experiences a 99.5% acceptance rate on submissions to the FBI
- Service code technology allows for the most accurate intake (pre-enrollment) by locking in the correct reason for fingerprinting, account, fee, and other unique data requirements by utilizing a unique six-character service code
- Accuracy & Convenience with an API to fully integrate their systems of record with UEP, allowing for accurate applicant enrollment and a convenient customer journey
- Next generation portable, solutions, including our enrollment tablet and kiosk devices

6.2.2.2 Use Cases

- Scan, verify, validate, and store information from Applicant IDs
- Professional and customer-centric organizations that provide applicants with superior customer service
- Simplify the pre-enrollment process for Applicants, allowing them to create or modify existing appointments on mobile devices, lowering no-show rates
- Reduce the number of unwanted calls into the state and user agencies and giving applicants the ability to track their own status
- Convert and digitally submit more than 100,000 paper fingerprint cards annually in support of numerous statewide networks
- Standardized list of authorized government-issued document options for Applicants to present at our IdentoGO Enrollment Centers prior to fingerprint capture

6.3 Civil Adjudication and Response Solution (CARES)

CARES is the next generation cloud-based product that enables end-to-end fingerprint transaction and background check processing. The CARES powerful and configurable workflow engine accepts transactions from multiple sources to facilitate background check processing. It has an end-to-end transaction and background check processing solution with powerful and configurable transaction workflow engine.



How does CARES work?

- Integrates with UEP to submit fingerprint records to state and/or federal agencies
- Receives, adjudicates, and consolidates results based on customized workflows
- Web portal access for authorized users to search and review applicant Criminal History Record Information (CHRI) for hiring and licensing decisions

6.3.1 Features and Benefits

- Enables record management and results processing in a configurable manner
- Reduces effort on users by offering the automation of search results for adjudication decisions and missed actions/activities by delivering notifications to agency staff
- Ensures that users can quickly identify and manage records requiring intervention
- Shares applicant data with 3rd party state applications
- Cloud-based deployment for advanced security, remote access, and reliable continuity
- Maximized security and interoperability of results processing
- Customizable and configurable workflows to meet all customer use cases and requirements
- Reduces dependence on local infrastructure
- Advanced reporting including integration with QuickSight reporting capabilities

6.3.2 Use Cases

- Applicant Look-up - State agent checking on an auto-adjudication result that an applicant or an agency point of contact queried them for the status
- Template PDF Creation - Integrator or business user able to make custom configurations to a PDF template for an applicant adjudication result letter
- Notes -State Agent making notes, mainly used for auditing purposes
- Rapback Summary -When an arrest has occurred following the initial background check, the state or FBI would issue rapsheet information to CARES which would trigger a notification to the agency point of contact
- Reporting Portal - State agent has been tasked with reviewing or verifying expected volumes and turn around times are being met
- Agency Management -State agent wants to confirm an agency has been set up correctly or may need to edit information pertaining to an existing agency
- User Management – Is a tool built for users with elevated access to manage which users have access to CARES and which applicant records those users have access to based on their assigned ORI/RFP combinations

6.4 IDEMIA Enrollment Tablet

The IDEMIA Enrollment Tablet enables multi-biometric capture from anywhere, at any time, bringing the functionality of the front office to alternate locations.

These IdentoGo tablets are equipped with built-in cellular data support, allowing for operation in remote/low technology locations. Additionally, mobile enrollment agents are equipped with mobile telephones that can be utilized to tether the tablets to transmit applicant records when necessary. Finally, if necessary, the IdentoGo tablets can temporarily store thousands of applicant records until such time as a reliable network connection is available. The data on the tablet is fully encrypted, both at rest, as well as in transit, thereby protecting the Personally Identifiable Information (PII) of the applicant.

The Enrollment Tablet includes a FAP-50 FBI fingerprint sensor capable of capturing multiple finger impressions as flats or rolls. Additional features include a tablet stand with tile/swivel capability for easy ergonomic use and the ability to scan/process identification documents such as drivers' licenses, and passports.

These tablets are issued to all IDEMIA mobile enrollment agents, providing fast, convenient, and efficient capture and processing of enrollment services data from applicants in the field. This approach allows for the IdentoGo network to address all requirements for capture and processing of applicant data in remote areas through scheduled enrollment events.

The Enrollment Tablet is an industry-changing, portable, biometric capture and identity proofing solution. Originally designed for TSA to modernize in-person background checks, the Tablet can capture ten-print fingerprints (flats and rolls), capture high-quality face photos and identity document images, read, write, and authenticate smartcards with both contact and contactless readers, and collect credit card payments as a full point-of-sale (POS) solution. This solution has been used to enroll over 1.1 million federal and state background check applicants, in addition to the TSA enrollment programs for TSA PreCheck, the Hazardous Materials Endorsement Threat Assessment Program (HAZMAT), Transportation Worker Identification Credential (TWIC®), and the Flight Training Security Program (FTSP).

6.4.1 Features and Benefits

- Customize workflows to meet any use case
- Capture ten-print fingerprints (flats and rolls)
- Take high-quality face photos and identity document images
- Read, write, and authenticate smartcards with both contact and contactless readers
- Collect credit card payments as a full point-of-sale solution
- Portable and light-weight, with user-friendly workflows
- Compact form factor and weight enables maximum mobility for examiners and clerks
- Remote operability allows users to work offline, then upload and merge applicant records later
- Efficient and flexible setup brings all the functionality you need, wherever you need it
- Secure, portable, and efficient

6.4.2 Use Cases

- Mobile biometric collection in alternate locations
- Delayed integration of collected biometrics

Chapter 7: Secure Credentialing

With NSS's secure credentialing solutions, you can manage and produce PIV compliant credentials for issuance within the agencies, or provide the capability to use proprietary, currently issued credentials. Secure credentialing supports clients in DOS and DOD and any agency that needs or has digital or physical credentials.

7.1 ID2Secure

ID2Secure is a truly modular solution that offers a complete set of Federal Identity, Credential, and Access Management (FICAM) capabilities that customers can choose from to arrive at an HSPD-12 solution that meets their needs. This framework enables flexibility for organizations to adjust for changes in requirements while allowing them to modernize and maintain their ICAM integration with cloud-friendly and mobile-friendly technologies.

The ID2Secure solution includes a robust platform built on modern integration approaches and leverages industry standard Business Process Model Notation (BPMN) workflow capabilities, known as IDEMIA Identity Integration services. These services include comprehensive capabilities to integrate with external systems, allowing for support of the ICAM workflows required for an Identity Management System (IDMS) Technology Refresh Project (TRP) solution.

ID2Secure is cloud-based for easy deployment and is interoperable. The solution uses Commercial Off-the-Shelf (COTS) credentialing products that are based on Federal Information Processing Standards (FIPS) 201-3 and open standards.

7.1.1 Features and Benefits

- Single turn-key solution that meets all regulations and requirements
- Highly modular platform, with interoperability between system components
- Personalized to grant varying levels of access to facilities and information systems
- Shorter path to updates with fewer touchpoints
- Leverages IDEMIA's PIV credentials
- In-person, re-enrollment
- Mobile IAL2 enrollment
- 1,600 enrollment locations nation wide
- Supervised Remote In-Person Proofing (SRIP)
- Identity document verification against over 4,000 global identity documents

7.1.2 Use Cases

- Secure new enrollment or re-enrollment
- Embedded in a variety of solutions
- Mobile enrollment
- In-person enrollment

7.1.3 Credential Management Service

IDEMIA offers the Credential Management Service (CMS) integrated within ID2Secure to deliver the functional capability to manage credentials such as PIV cards, associated with identities managed within ID2Secure. The CMS issues and manages credentials to meet Authenticator Assurance Level (AAL) 1-3 based on NIST 800-63B guidelines. CMS integrates with Enrollment services and DOD solution components to manage the credential lifecycle. The solution offers lifecycle management capabilities that can be used by credential holders via the self-service portal, by visiting a self-service kiosk, or visiting a CMS issuance/helpdesk station in person. It prevents vendor lock-in and makes transitioning to any other CMS an easily achievable task.

CMS manages the lifecycle of PIV card certificates, derived credentials, alternate tokens, and FIDO2 passkeys. This solution includes the capability to issue and manage the lifecycle of various types of credentials such as PIV, PIV-I, Alternate Tokens, and a range of other physical devices that requires issuance of credentials to represent its identity.

Each of the credential types managed within the CMS is associated with a Credential Profile that defines all elements that are required for issuance, such as certificate details, layout (if printing is required), issuance process, PIN settings, etc. The credential profiles are then associated with the business processes that are configured to manage various types of person identities, organizations, and types of credentials. Separate profiles can also be created to support the PIV, PIV-I, and Alternate Tokens as required, as well as future credential types.

7.2 Vetting

NSS solutions support initial vetting of installation population group members against authoritative data sources. Our vetting uses abstracted interfaces to major data sources, including the FBI NGI; NCIC; state and local law enforcement systems, such as AFIS and DMV databases; and other authoritative data sources. Additionally, we interface to data aggregators, such as Lexis/Nexis, Experian, and Socure, with the ability to integrate with additional 3RD party authoritative data sources.

Our solution is integrated with similar aggregation servers for vetting data. The additional use of ID2Access as an IMESA enables connections between installation security, authoritative national databases, and commercial data aggregators. We provide solutions for the majority of state and local criminal justice systems and law enforcement organizations. Combining this with being the leading provider of state driver credentials in the U.S., we can perform identity verification, data exchanges, and vetting through both our idFabric solution and the American Association of Motor Vehicle Administrators (AAMVA).

7.2.1 Use Cases

Anywhere there is a need to vet credentials to authoritative law enforcement databases including but not limited to: National Crime Information Center Person Files, Interstate Identification Index, National Law Enforcement Telecommunications System, and Commercial criminal background screening.

7.3 Physical Credentials

IDEMIA provides solutions for the nation's driver's licenses, passports, passport cards, and government identification cards. These physical cards, or their digital equivalent, demand the highest level of security because they connect to your driving record, travel history, and for most government agencies, can grant access to high-security buildings or documents. IDEMIA is the proven partner of state and federal agencies because our seamless and convenient identification solutions make a security promise to each resident.

If you have a federal issued PIV smart card or CAC credential, odds are you're using an IDEMIA issued badge. IDEMIA has been the leader in providing federal credentials for over 15 years. IDEMIA's ID-ONE PIV® credential is used in more than 125 federal agencies in North America. Our identity solutions not only ensure that PIV smartcards and CAC credentials are in compliance with current guidelines and technical specifications, but we make it our goal to exceed the latest government standards. Each smartcard credential is personalized, up-to-date, and fast.

7.3.1 Features and Benefits

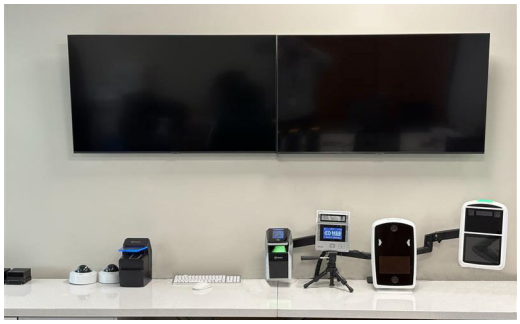
- Used for UHF RFID polycarbonate U.S. Federal Secure Credentials, including the ID-One PIV® smart card, and U.S. Passport Book
- Complete life-cycle operational support and quality assurance for secure credentials – including design, color management, operations, maintenance, repair, and upgrades
- Interoperable and compatible with legacy systems and current commercially available card management systems
- Flexible to grant varying permission levels to facilities and information systems
- 5X faster than existing cards, bringing FICAM compliant Physical Access Control under 1 second
- Single secure authentication card solution provides an easy way to control security for both physical and logical access
- Converged credential for controlling both buildings and IT assets without proprietary technology or customization

7.3.2 Use Cases

- PIV/CAC Cards
- Passports
- Federal Credentials

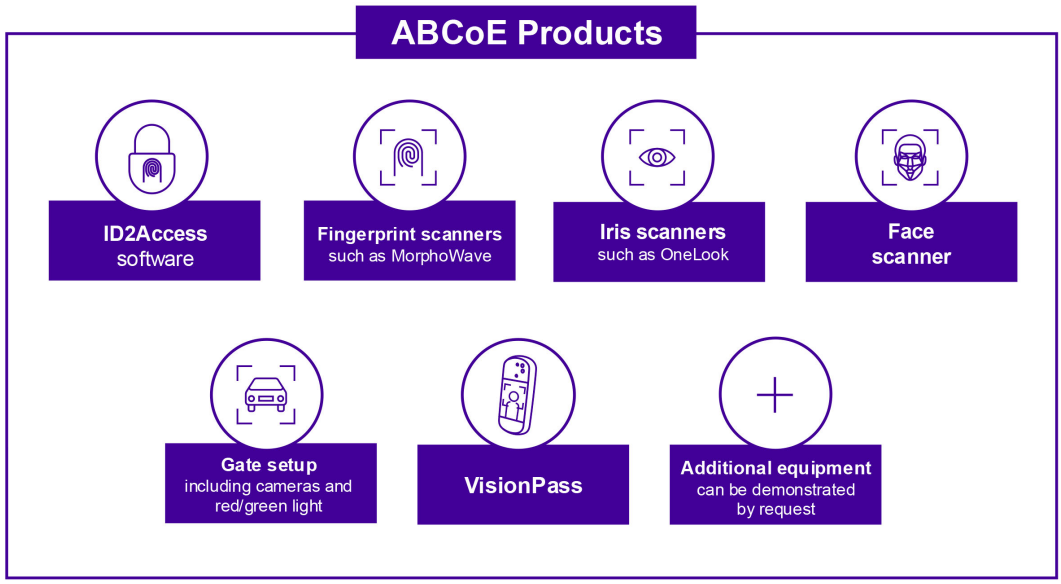
Chapter 8: Applied Biometrics Center of Excellence

The NSS Applied Center of Biometric Excellence, located in Morgantown, WV, provides a physical location where you can come to interact with and learn about our biometric solutions. You can experience how biometrics go from a concept to a practical solution - to see how biometrics are applied. This includes enrolling your face and fingerprint into the ID2Access system that facilitates access control and provides alerts and monitoring within the ABCoE. You can see the software in action by identifying passengers traveling through our ID2Pass demonstration lane and by walking through the facility to see ID2Surveillance providing real-time identification, as well as access to certain areas within the building.



Additionally, you can interact with a variety of access control devices using various biometric modalities such as face, finger, and iris in action and how these devices are applied in the field. Our Subject Matter Experts (SMEs) can provide on-demand demonstrations of Augmented Vision so that investigative agents are able to see how the software can make their lives easier in solving complex cases.

The ABCoE allows you to observe and understand how biometrics are applied in the field in a practical sense. Not just as a concept but in a way that improves the lives of those who use these solutions.



8.1 Features

- Primary hub for the cutting edge of NSS R&D and Engineering
- R&D for biometric access control solutions
- Operability of solutions across 5G networks
- MBIS cloud support and customization
- MBSS cloud support
- MBIS and MBSS Scaling Patterns
- Experience center for IDEMIA Solutions
- North American Augmented Vision expertise
- Seat of ID2Access Product Development
- Partnership with West Virginia University biometric lab

8.2 Benefits

- Wealth of engineering talent
- Physical interaction with devices
- Real-world demonstrations
- On the fly demos
- Access to SMEs
- Works in any weather