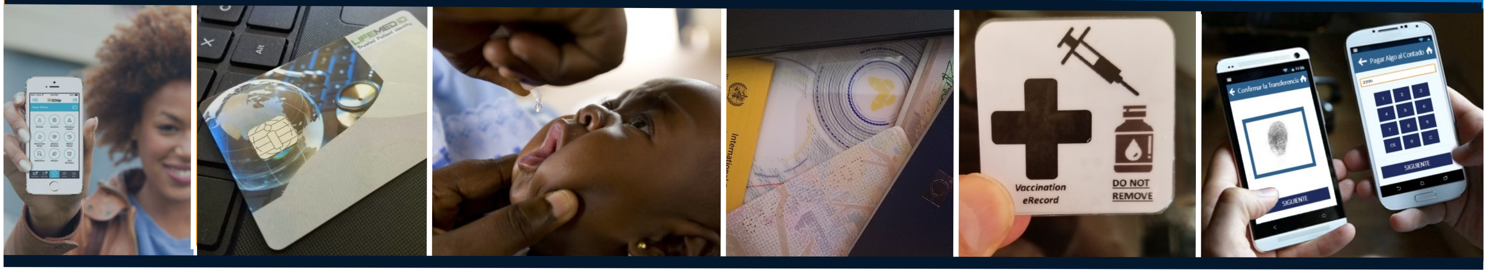
ALLIED IDENTITY

Platform Suite for Identity Ecosystems

Frictionless transactions through real identity



ALLIED IDENTITY

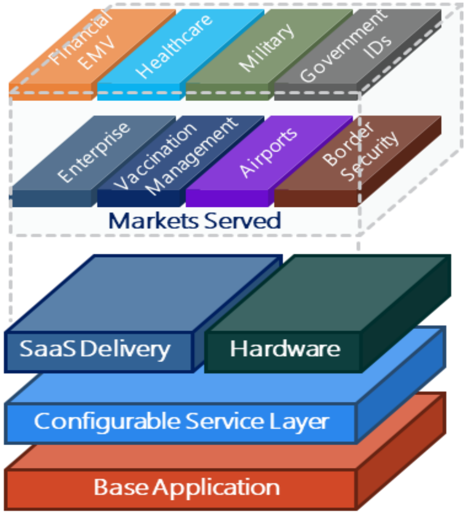
Platform Suite for Identity Ecosystems

Delivery Everywhere

The Allied Identity Platform Suite is a collection of software and hardware components that work together to enable every process step in an strong Identity Ecosystem. These components can fundamentally transform populations that are under-served or under-banked and have limited access to government services. We can deliver iChip based applications and credentials in a wide variety of formats including virtual cards. Our data management can be delivered ***On-Prem or via a SaaS Model***.

Our foundational technology enables end-to-end control of Digital Identity Systems:

- Proof of who you are through ***Authentication***
- Privacy of your data through ***Encryption***
- Enablement of your system through ***Authorization***
- Guarantee of your transaction integrity through ***eSignatures***
- Security is enabled through design from the start and enhanced by our strong Certified Trusted Silicon and the iChip Credential Operating System
- Our Credentials manage both an online and / or offline eWallet Transactions, when used with our AGL banking platform
- Compliance and reporting through the iChip real-time event management software



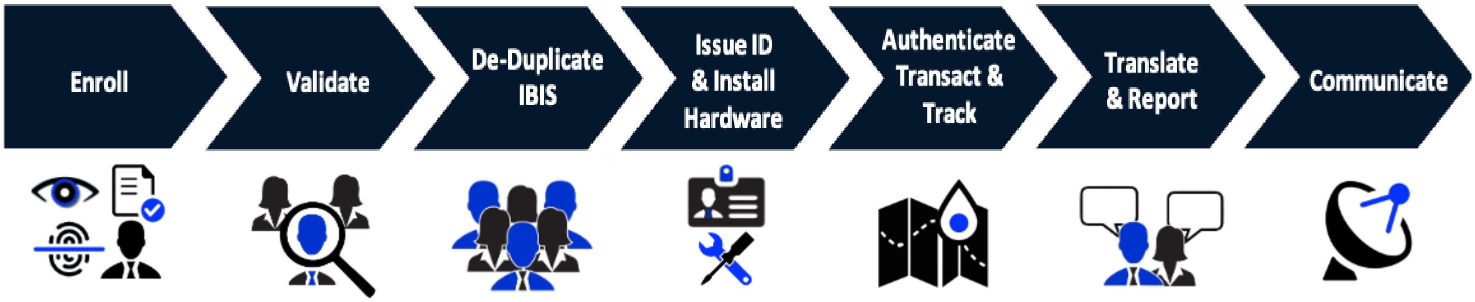
World Class Biometric and Biographic Collection and Deduplication

Unlike many solutions that store templates dedicated to a specific vendor's hardware, we make sure what is collected is usable across all standardized hardware devices. Then records are built on validated data that is tagged with the appropriate metadata for interoperability across department - ministry domains and third party authorities e.g. ICAO or Interpol.

Benefits:

- All platform components are integrated and support standards-based interoperability
- Modular Components that let the issuer mix and match based on needs
- Ease of use , Best in Class user interfaces and intuitive design
- High-performance / Low Cost
- Integrated and certified Authentication, Encryption and eSignature technology
- Simplified Credential Issuance
- Incorporated Identity Lifecycle management
- Secured Data Architecture with a Zero Trust Model that incorporates secured endpoints and micro-segmentation controls
- Workflow designs that incorporate optional independent field use for ruggedized environments e.g. remote biometric collection for a civil ID or voting application

The Allied Identity Process

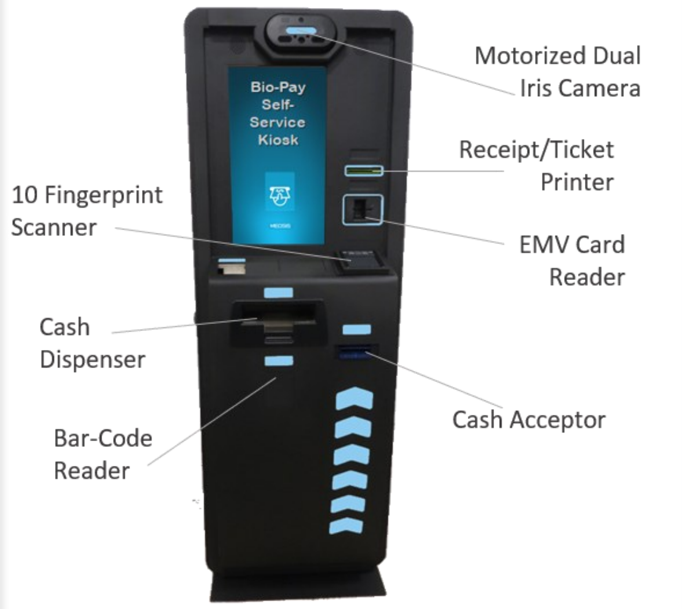


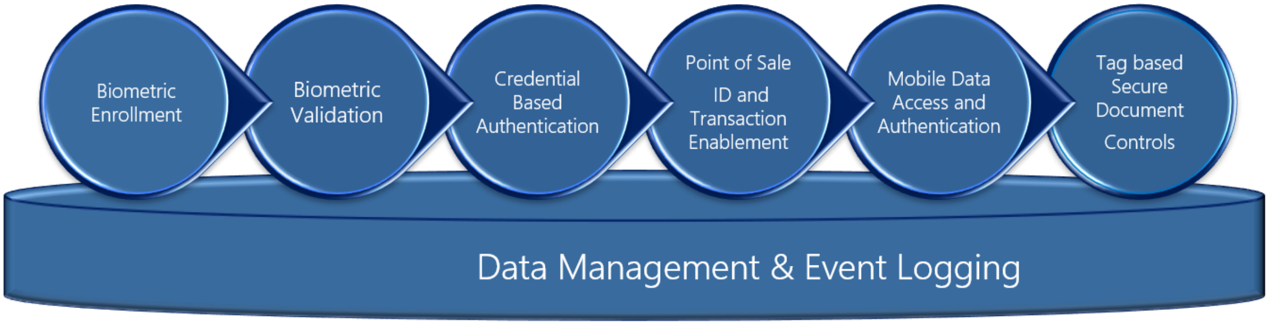
Components or Solutions, your Choice

The Allied Identity platform can work at all levels of an identity process with either a bespoke solution or a set of products that fill a need into an existing system. From strong enrollments that are biometrically cross modal and biographically accurate we can enroll large populations from mobile devices, web applications, Windows devices, portable jump kits and automated kiosks. All collection is interoperable & built to ICAO / ISO standards. Robust Validation includes biographic checking of employment, address and credit as well as family references.   We can also validate other credentials as a breeder document reference to the enrollment. We start this process with apps and mobile devices, specialty Windows-based devices or from a bespoke web application. All validations are interoperable & built to NIST SP-800, and ICAO / ISO standards.

We build Automated Biometric Information Systems (ABIS) that perform real-time matching of up to 6 different types of biometric modalities for populations up to 250 million in under .4 min per record. We use different biometric matchers for different populations and we always use the right matching algorithm for each modality type.

Bio-Pay Self Service Kiosk/ATM




Biometric Enrollment
Biometric Validation
Credential Based Authentication
Point of Sale ID and Transaction Enablement
Mobile Data Access and Authentication
Tag based Secure Document Controls
Data Management & Event Logging

iChip®

Credential Operating System for Identity Ecosystems

Credential Security and Secured Silicon

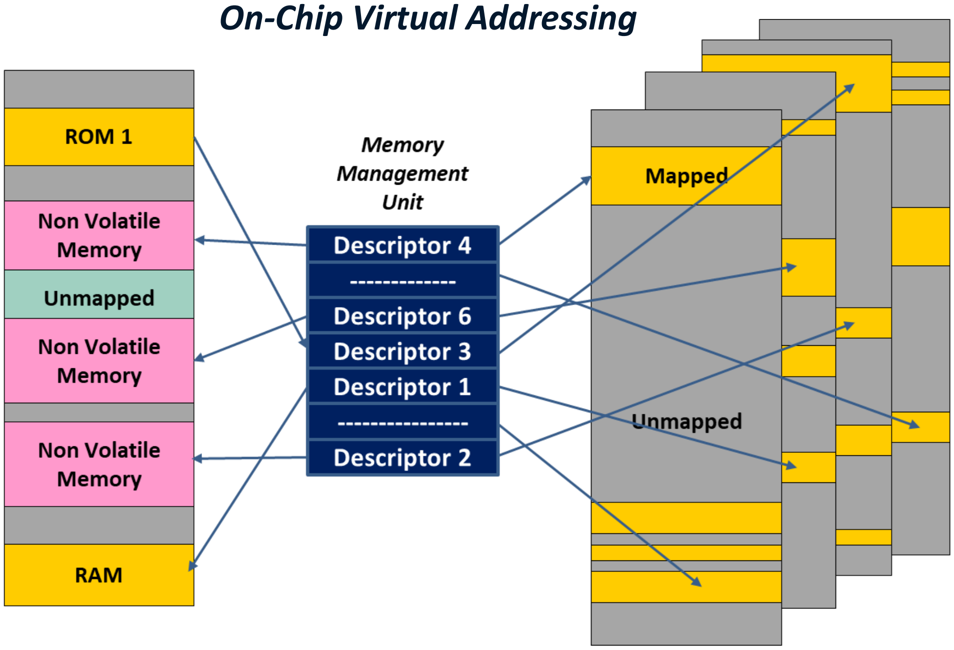
- High Security EAL5+ Silicon
- Support for Block-Chain Crypto Currencies (Hybrid Ledger Methodology)
- Multiple eSignature options
- Multiple Authentication options
- On-Chip Bio-Match options
- 5 form factors – Contact ID1 cards, Contactless ID1 Cards, Dual Interface ID1 cards, SIMS, NFC labels
- Multiple Part Numbers based on User Requirements
- NIST Certified Cryptography, tested to ICAO and EMV Certified + Visa, Discover and MasterCard

Industry Standard Data Maps for Interoperability

- ICAO BAC/SAC
- EMV SDA, DDA & CDA
- PIV II with Salamander Containers
- EU DL
- HL7 – CCDA, EMR & PHR

iChip Credential Operating System
On-Chip Virtual Addressing

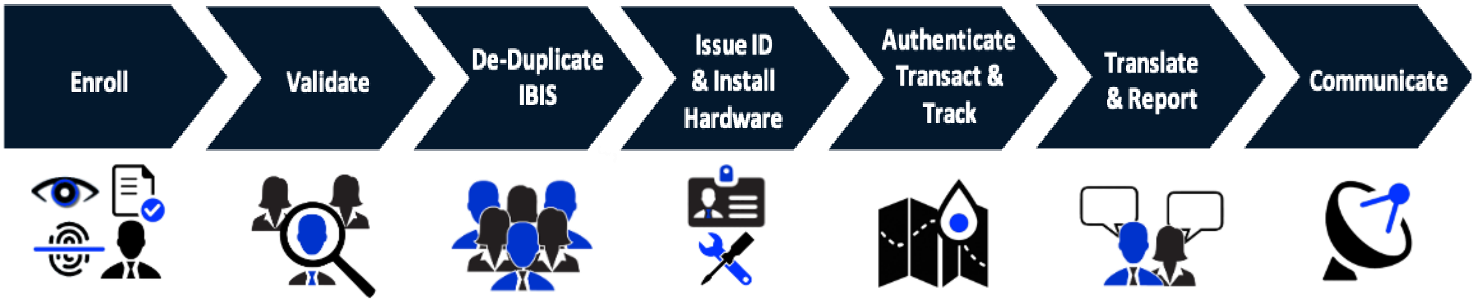
For security the iChip internal memory is remapped and encrypted on each clock cycle of the CPU. This prevents any possibility of hacks on the internally stored keys



Physical Addressing of Data **Virtual Addressing of Data**

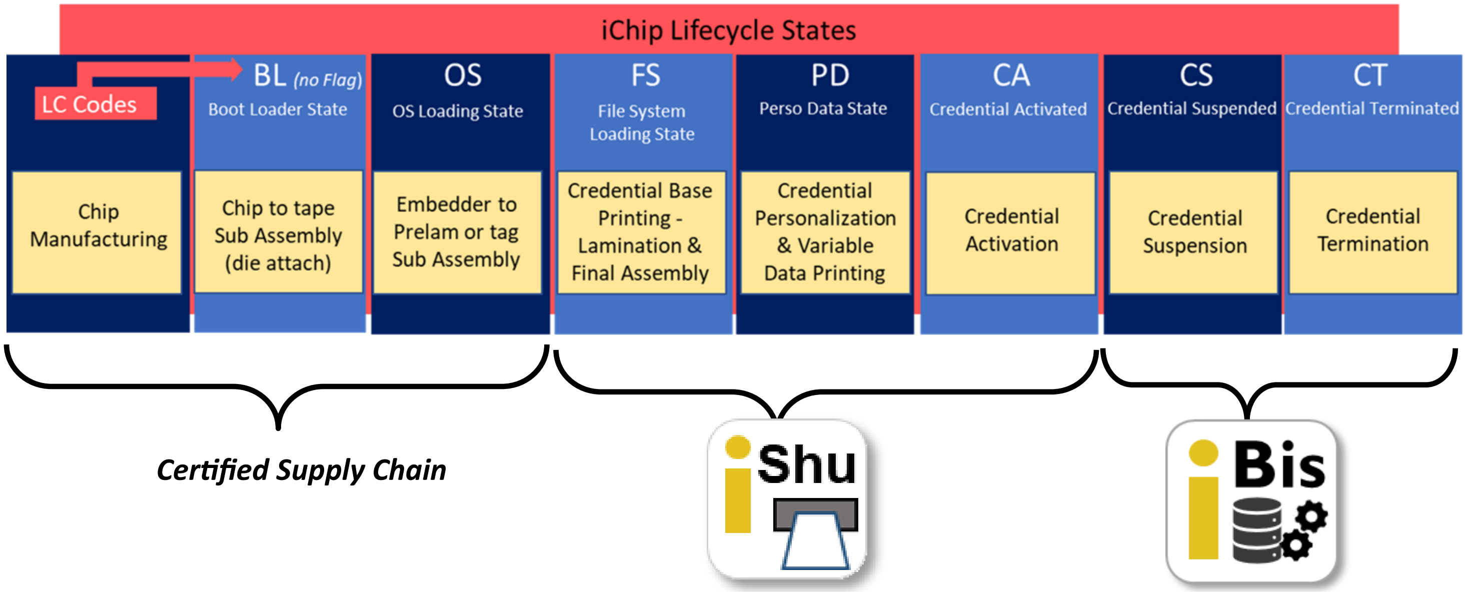
www.alliedidentity.com

The Allied Identity Process



Lifecycle and Key Management

The iChip® OS has an integrated lifecycle backbone that is based on real world environments. This design philosophy starts with the internal structure of the iChip Credential Operating system that has lifecycle states that are tied to events. These events are managed by the secured supply chain or the platform components (either the iBis or iShu software) and are bounded by keys from our Key Management Server (KMS). The access controls to change a Identity record are either authorized to key Supply Chain partners that are vetted and certified or are the responsibility of each country in larger Build Operate and Transfer type projects.

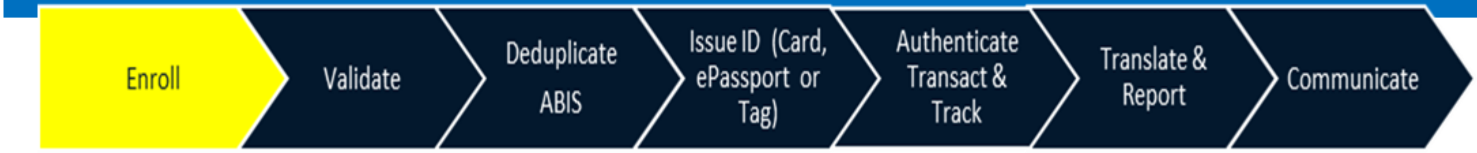


iChip Lifecycle States

LC Codes	BL *(no Flag)* Boot Loader State	OS OS Loading State	FS File System Loading State	PD Perso Data State	CA Credential Activated	CS Credential Suspended	CT Credential Terminated
Chip Manufacturing	Chip to tape Sub Assembly (die attach)	Embedder to Prelam or tag Sub Assembly	Credential Base Printing - Lamination & Final Assembly	Credential Personalization & Variable Data Printing	Credential Activation	Credential Suspension	Credential Termination

Certified Supply Chain

iReg®



Enroll

Validate

Deduplicate ABIS

Issue ID (Card, ePassport or Tag)

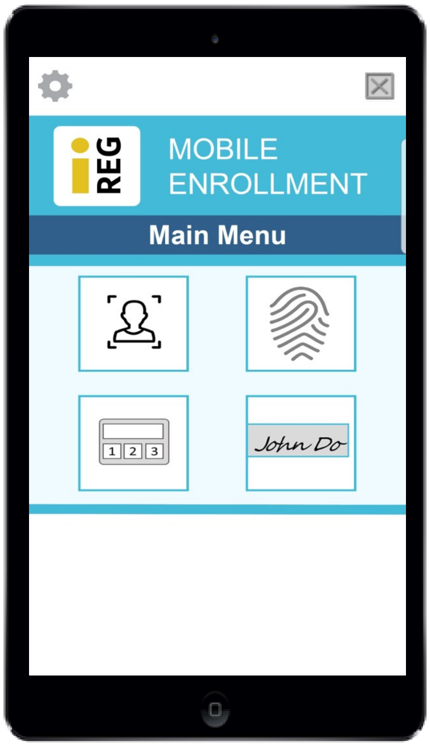
Authenticate Transact & Track

Translate & Report

Communicate

Overview

This general-purpose tool enables the registration of participants via an Android platform. After each collection, the data is pushed to a cloud-based Automated Biometric Information System (ABIS). If the system is in a off-comms mode , it will store and forward when it re-syncs with the ABIS. The iBis ABIS / Database and AI rules engine handles optional 3rd party candidate proofing, screening to pre-set filters and real-time deduplication. We have built an optional vaccination tracking enrollment and update mechanism into the system as well.



iReg Captures and Enrolls

- Breeder document Information
- A wide selection of Biographic Data following the ICAO and or the AAMVA/ISO standards to be used for candidate screening and/or in credential production
- Biometric Modalities formatted to the ICAO 9303 standards

Benefits

- All platform components are integrated and support standards-based interoperability
- Ease of use , Best in Class user interfaces and intuitive design
- High-performance / Low Cost
- Integrated and certified Authentication, Encryption and eSignature technology
- Secured Data Architecture with a Zero Trust Model that incorporates secured endpoints and micro-segmentation controls
- Workflow design that incorporates optional independent field use for ruggedized environments e.g. remote biometric collection for

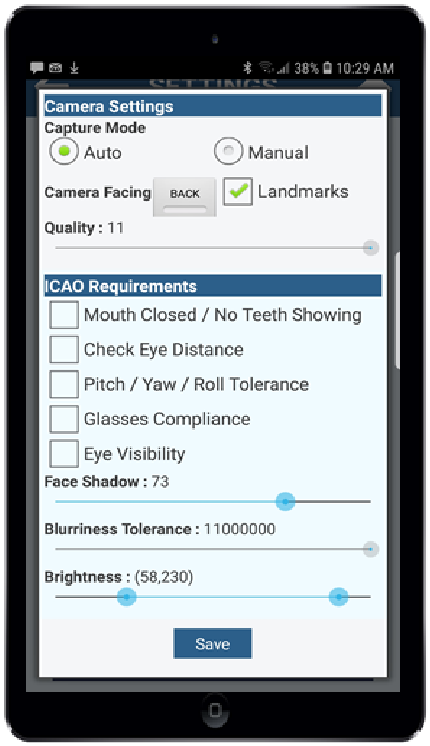
Biometric Modalities supported

- Face
- Finger
- Iris
- Signature
- PIN

Flexible options

The iReg solution lets the user capture the data and biometrics as their ecosystem requires. A wide variety of options can be specifically tailored and branded for the end user.

The current system builds records on validated data that is tagged with the appropriate metadata for interoperability across department - ministry domains and third party authorities.



38% 10:29 AM

Camera Settings

Capture Mode

● Auto ○ Manual

Camera Facing BACK ☑ Landmarks

Quality : 11

ICAO Requirements

□ Mouth Closed / No Teeth Showing

□ Check Eye Distance

□ Pitch / Yaw / Roll Tolerance

□ Glasses Compliance

□ Eye Visibility

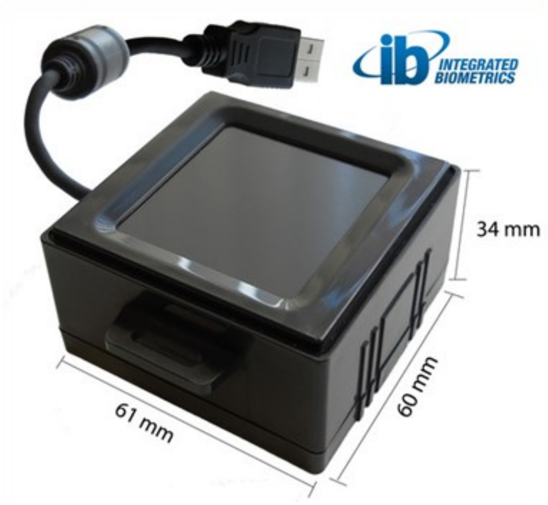
Face Shadow : 73

Blurriness Tolerance : 11000000

Brightness : (58,230)

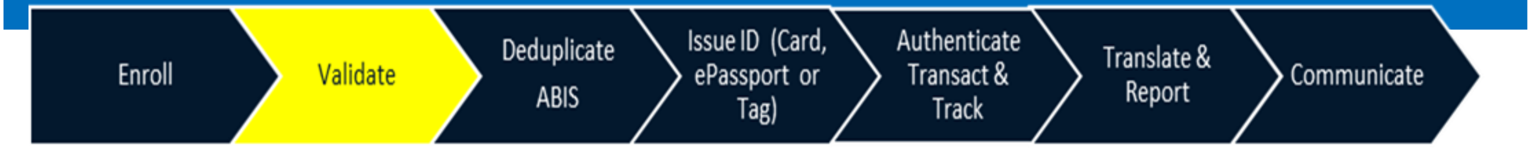
Hardware Agnostic

Use any Android device with Nougat or above that supports external ports and you are enabled. We currently support the Integrated Biometrics and Greenbit live scan fingerprint scanners and will add others on request. External cameras are supported if your chosen hardware supports this option.



Watson Mini 2 fingerprint livescan device from Integrated Biometrics

iCheck®



Enroll

Validate

Deduplicate ABIS

Issue ID (Card, ePassport or Tag)

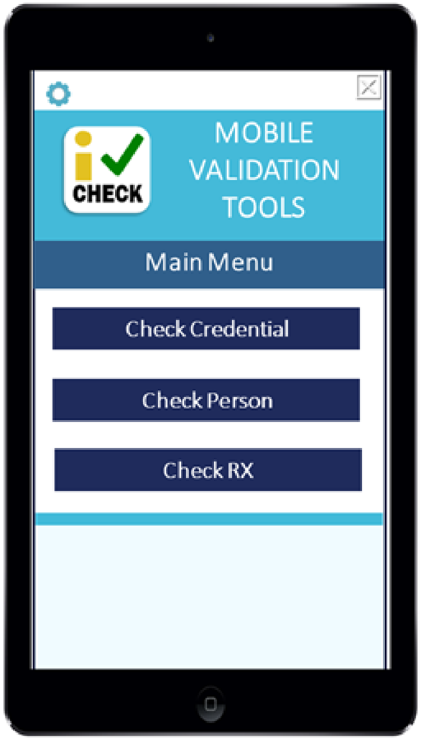
Authenticate Transact & Track

Translate & Report

Communicate

Overview

iCheck® validates people, as well as authenticates a wide variety of credentials including ICAO MRTDs. The App can read prescription drug containers or other dispensed bar-coded items via an Android-based platform. This platform includes mobile phones and selected payment terminals. The program works in conjunction with a number of external servers to authenticate government issued keys found in passports or government IDs, doctor eSignatures and drug formularies.



iCheck verifies

- The person is who they say they are through Biometric Matching
- Confirms that their credential is real and has been issued to them via eSignatures (Binding)
- Drug container Bar-codes and does a lookup against a specified database
- That the drugs dispensed are within date code and have been dispensed by a certified supply chain

Benefits

- All platform components are integrated and support standards-based interoperability
- Ease of use , Best in Class user interfaces and intuitive design
- Integrated and certified Authentication, Encryption and eSignature technology
- Secured Data Architecture with a Zero Trust Model that incorporates secured endpoints and micro-segmentation controls
- Workflow design that incorporates optional independent field use for ruggedized environments   e.g. remote biometric matching for a civil ID or voting application

Biometric & Validation Modalities supported

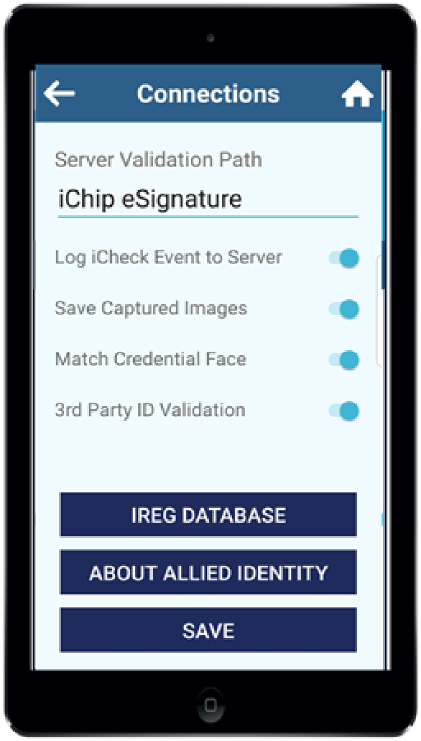
- Face
- Finger
- Iris
- Signature
- PIN

www.alliedidentity.com

Actionable Information through Biometric Matching and Credential Validation

In many environments, falsified or out of date credentials enable drivers, citizens or visitors to move unimpeded in places they should not be. The iCheck app enables Governments and NGOs to accurately identify people with a few touches of a button. *Passports, Drivers Licenses, Commercial Vehicle Registrations, Insurance Validity* as well as *Vaccination Records* can all be verified. The system can read all ICAO compliant MRTDs (Machine Readable Travel Documents) with BAC (Basic Access Control) and /or SAC (Supplemental Access Control with PACE 1) and many country's National IDs for use in border control systems.

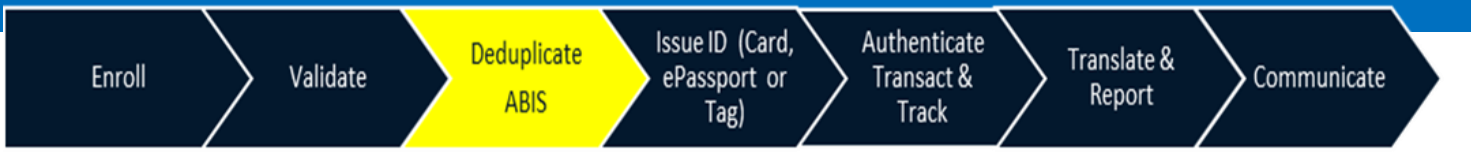
The program can easily be modified to be used as a portable time clock with event logging and geolocation of each participant.



Server Validation Path
iChip eSignature

Log iCheck Event to Server ●
Save Captured Images ●
Match Credential Face ●
3rd Party ID Validation ●

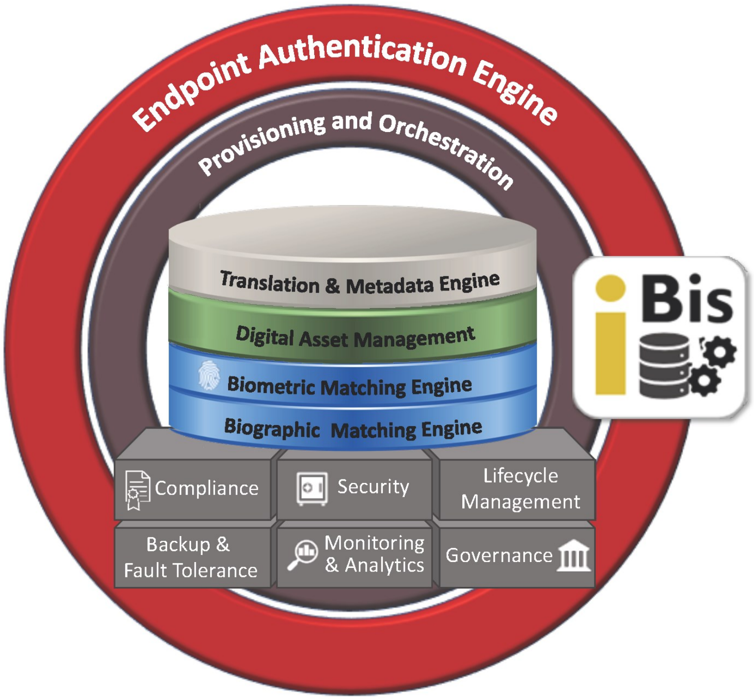
iBis®


Enroll
Validate
Deduplicate ABIS
Issue ID (Card, ePassport or Tag)
Authenticate Transact & Track
Translate & Report
Communicate

Overview

iBis® is a complete civil ID management system that stores, deduplicates, matches and manages validated identities with their associated breeder documents. The software is more than an industrial strength Automated Biometric Information System (ABIS). Aside from the blazing fast biometric matching the iBis system also deduplicates biographic data with AI enhanced accuracy. Our system is designed for processing multiple parallel endpoint authentications and transactions to enable a wide variety of requests. The software distributes external requests between the corresponding services. iBis's authentication server can be performing heavy algorithmic digital authentication functions at the same time that the image processing executes parallel biometric matching from multiple extracted templates while the biographic data processor can generate weighted decisions based on preset rules that take into account:

- Data entry errors
- Misspellings, transpositions, variants, accents, hyphenations
- Natural name variations e.g. diminutives, nicknames, aliases
- Cultural name anomalies and practices
- Other Multiple name spellings due to language translation

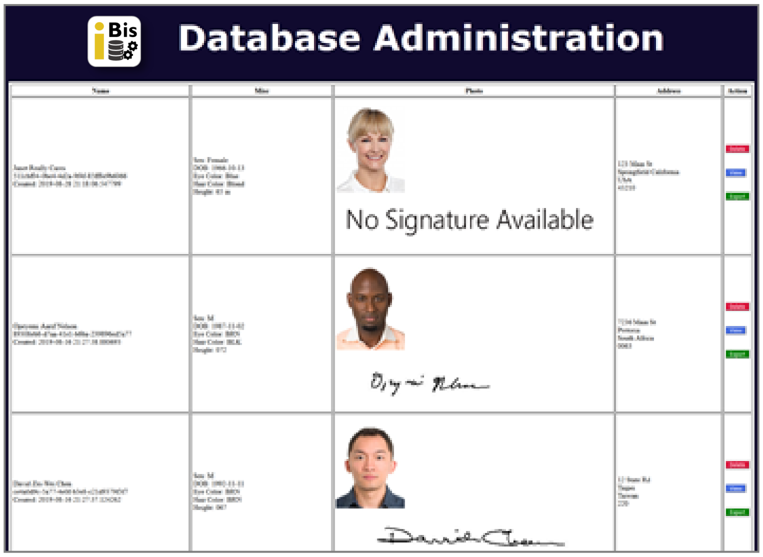

Endpoint Authentication Engine
Provisioning and Orchestration
Translation & Metadata Engine
Digital Asset Management
Biometric Matching Engine
Biographic Matching Engine
Compliance
Security
Lifecycle Management
Backup & Fault Tolerance
Monitoring & Analytics
Governance
iBis

The classic name matching challenge has now been solved with artificial intelligence based adjudication. This is the only system that has a programable event log built in for full audit capability. The system can be integrated with a nationwide electronic master patient index and an EMV certified benefits distribution system.

Every record created and managed is considered an asset in our system. iBis is built with a sophisticated tracking system that creates and uses metadata for each component of a record e.g. A facial image. All records are optionally anonymized, stored encrypted and accessed through a PKI authenticated tunnel after authentication and authorization.

Valuable Insights through big-data dashboards

- Population Movements
- Vaccination efficacy against disease vectors
- Haji Participants
- Voter Participation
- Airport Incident management
- Insurance Participation
- Familiar relations information



Database Administration

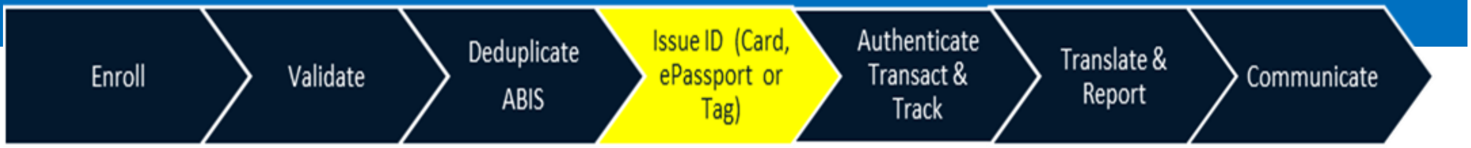
Biometric & validation modalities supported

- Face
- Finger
- Iris
- Signature
- PIN

Features and Benefits

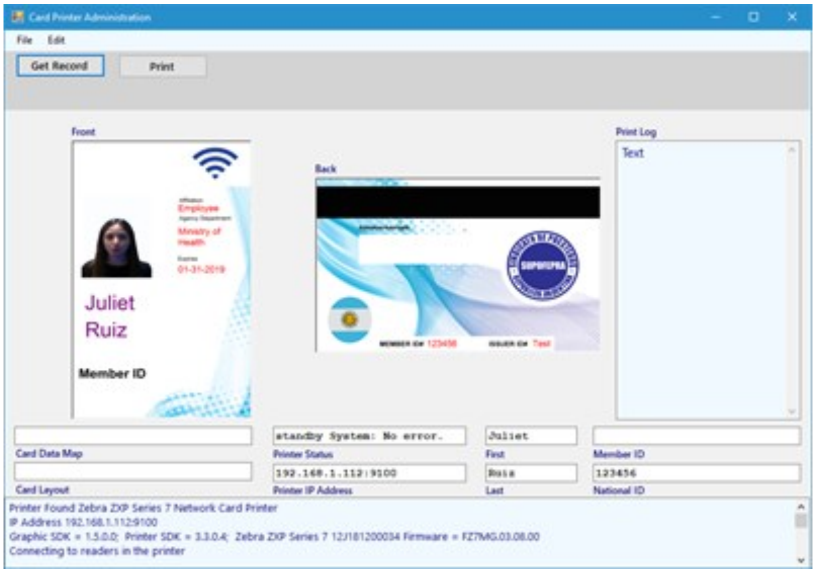
- ***Full biometric standards support*** iBis enables the use of ANSI/NIST-ITL-1, ISO/IEC 19794-2, ISO/IEC 19794-5 and ISO/IEC 19794-6 biometric standard templates.
- Face images can be optionally confirmed compliant with ICAO requirements if your system does not Use iReg as the upfront capture software
- NIST MINEX-compliant fingerprint engine, NIST IREX proven iris engine.
- iBis is designed to support standards-based data exchanges e.g. MIRTH to HL7-FHIR to support interoperability
- Available as on-premise implementation and/or as cloud service.
- Fully scalable iBis can store biometric and demographic information for an unlimited number of persons
- Fault tolerant design with 24/7 full availability
- Integrated authentication services for rapid endpoint service requests
- Optional watchlist interfaces for 3rd party validations e.g. PEPs or Interpol

iShu®


Enroll
Validate
Deduplicate ABIS
Issue ID (Card, ePassport or Tag)
Authenticate Transact & Track
Translate & Report
Communicate

Overview

iShu® has been designed for the creation of ID Credentials personalized with a registrant's biographic and biometric data via a Windows 10 based Platform. This is an installed application that drives specific printers at the client's location and pulls data through a secured network connection to an ABIS.



Card Data Map:
Card Layout:
Printer Status: standby System: No error.
Printer IP Address: 192.168.1.112:9100
First: Juliet
Last: Ruiz
Member ID:
National ID: 123456

```
Printer Found Zebra ZXP Series 7 Network Card Printer
IP Address 192.168.1.112:9100
Graphic SDK = 1.5.0.0; Printer SDK = 3.3.0.4; Zebra ZXP Series 7 12J181200034 Firmware = FZ7MG.03.08.00
Connecting to readers in the printer
```

iShu verifies

(when used with the iBis)

- That the person has been deduplicated before creating a credential
- Confirms that this is the only credential that has been created via the lifecycle manager

The iShu software

- Encodes the credential's internal chip with the profile and data selected into ICAO format with all relevant Metatags
- Loads all private and public keys for eSignatures and Authentication
- Prints specific field information as specified around each profile
- Changes the lifecycle state of the chip in the credential
- Sends a message to the ABIS that the credential has been personalized

Benefits

- All platform components are integrated and support standards-based interoperability
- Ease of use , Best in Class user interfaces and intuitive design
- Scalable to any printer that supports NFC encoding and windows print drivers
- Secured Data Architecture with a Zero Trust Model that incorporates secured endpoints and micro-segmentation controls

Security:

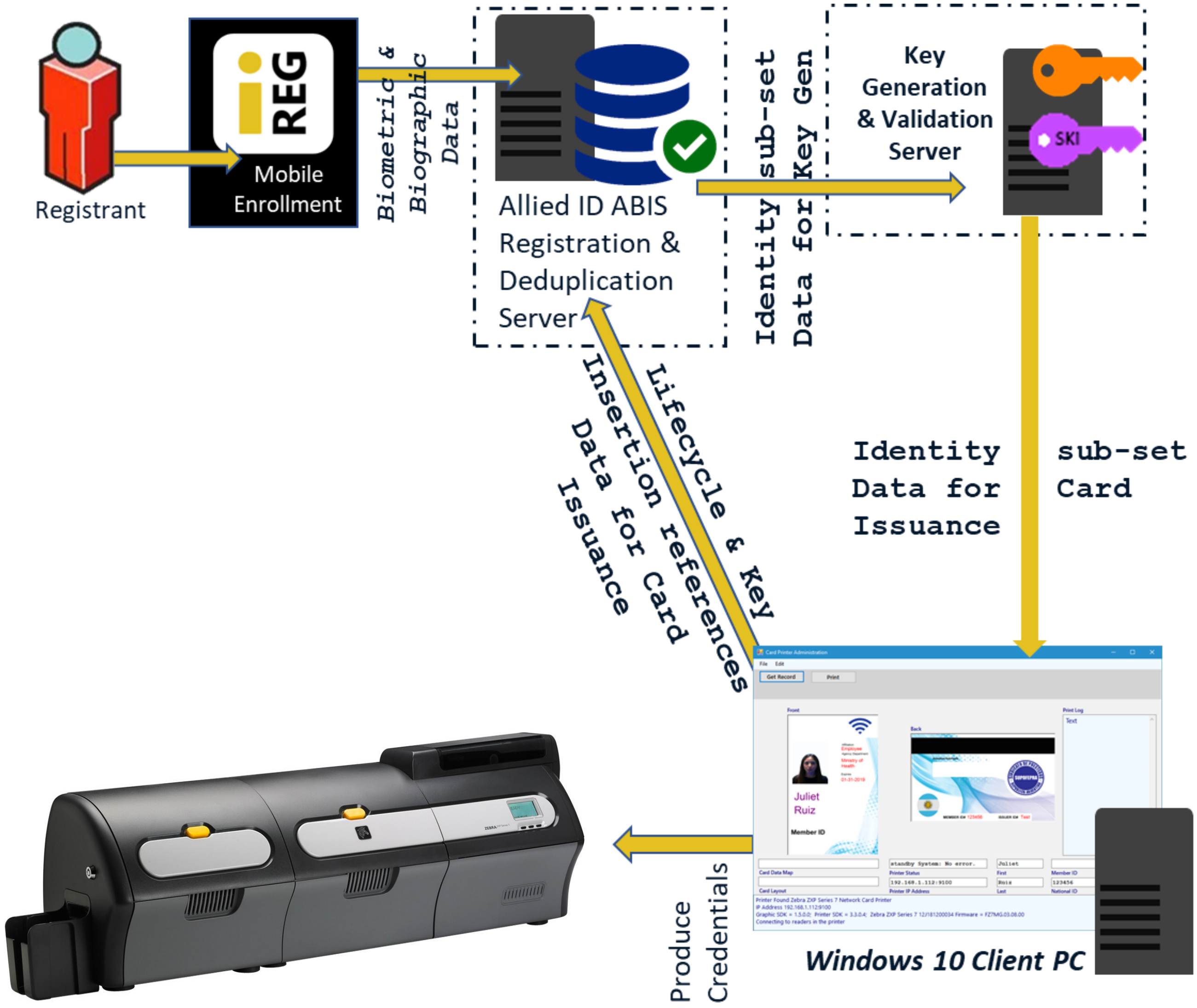
- Access rights are set by the issuer
- All data stored or/in transit is encrypted with AES 256
- Device Authentication is multi-tiered and based on SHA2

Requirements

- Windows 10
- Printers must support NFC and Wi-Fi

Hardware Agnostic

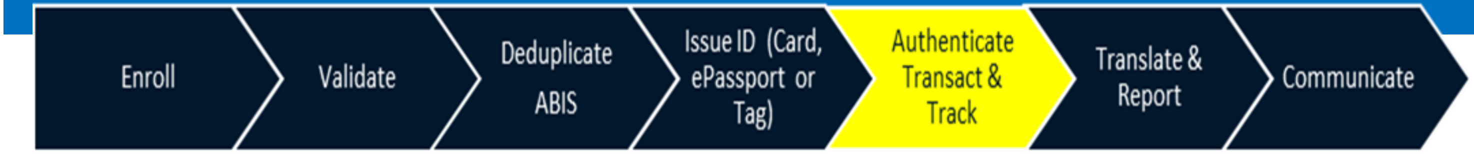
Use any card printer that supports Windows print drivers and Wi-Fi plus NFC encoding. We currently support Zebra and Matica units and will add others on request.


Registrant
iREG
Mobile Enrollment
Biometric & Biographic Data
Allied ID ABIS Registration & Deduplication Server
Identity sub-set Data for Key Gen
Key Generation & Validation Server
SKI
Identity sub-set Data for Card Issuance
Lifecycle & Key Insertion references Data for Card Issuance
Produce Credentials
Windows 10 Client PC

Zebra ZXP 7 Pro with Laminator

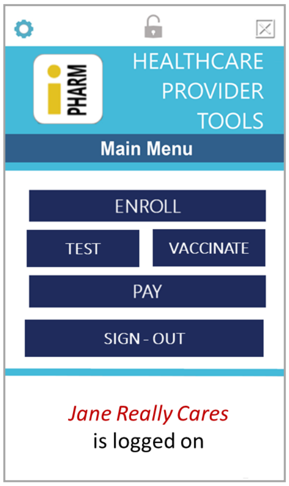
www.alliedidentity.com

iPharm®

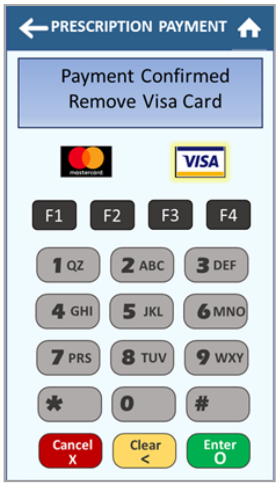

Enroll
Validate
Deduplicate ABIS
Issue ID (Card, ePassport or Tag)
Authenticate Transact & Track
Translate & Report
Communicate

Overview

iPharm® is a general-purpose demonstration tool that shows how a secured, auditable transaction can be done with registered participants via an Android-based Platform. This includes mobile phones and selected payment terminals. The data is partitioned and then pushed to our partner gateways for financial processing and to specified databases for verification of co-pays, drug dispensing data repositories for opioid and or vaccination tracking and each subscriber's Electronic Health Record. The application currently demonstrates the dispensing of controlled substances such as opioids or vaccinations and can be modified as a bespoke application for the sale of both controlled and unregulated items.



Jane Really Cares
is logged on



Payment Confirmed
Remove Visa Card

The System Captures and verifies:

- Each participant in the transaction flow
- This is configurable for each customer and can be done through a wide variety of Biographic and/or Biometric data

Validation Methods Supported:

One or all of these can be used:

- iChip Credential
- Face
- Finger
- Signature
- PIN

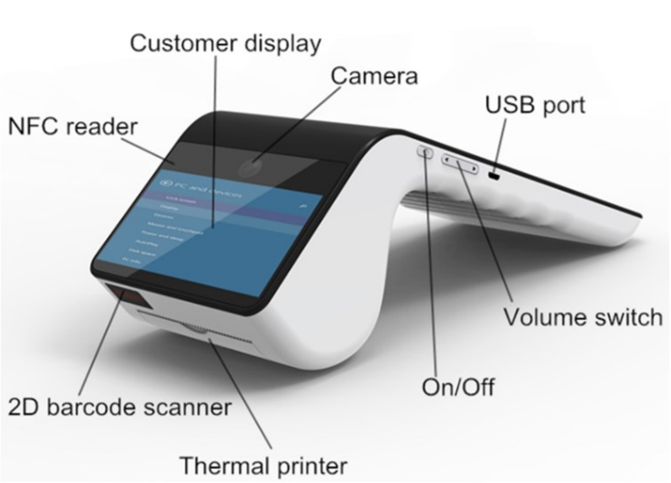
Security:

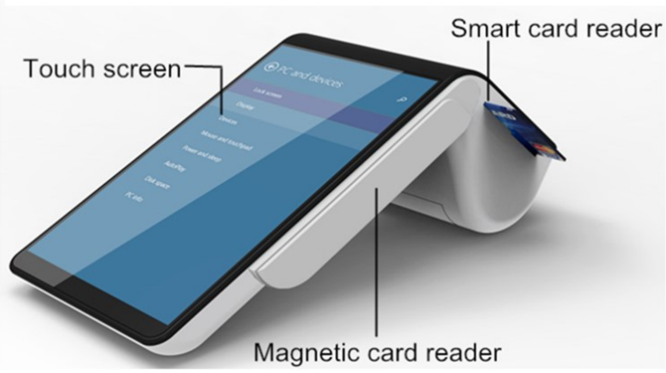
- Access rights are set by the user

Benefits

- The fully deployed product can be certified to EMV and PCI requirements based on the deployed architecture
- All biometric components are integrated and support standards-based interoperability
- Ease of use , Best in Class user interfaces and intuitive design
- The terminal comes standard with an NFC interface , EMV 7816 contact card reader, receipt printer and Bar-Code Scanner
- Magnetic stripe reader is optional not a fixed cost
- Secured Data Architecture with a Zero Trust Model that incorporates secured endpoints and micro-segmentation controls

iChip Payment Terminal and Functions





ID Verification
& Biometric
Matching

Credit – Debit
ACH-CC & Cash

Geo
Location
and
Fencing

Benefits
Calculation
of Coverage
Inc. Co-Pays

SKUs for
HSA and
personal
Account
Reporting

IVCP
Dispensing
and Reporting

Healthcare
Transaction
Transport to
Cloud & Payers

E-mail
option for
receipts

Appointment
Setting and
Reminders

ALLIED IDENTITY

291 S La Cienega Blvd #107
Beverly Hills, CA 90211
+1 (747) 215-9200
www.alliedidentity.com