Healthcare Provider Identity Suite
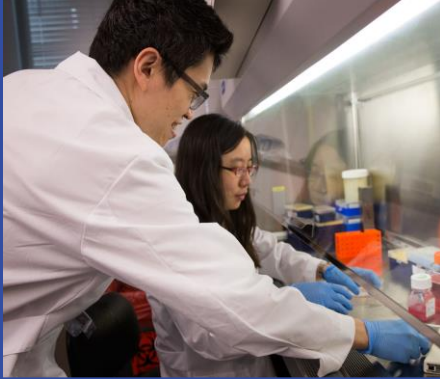
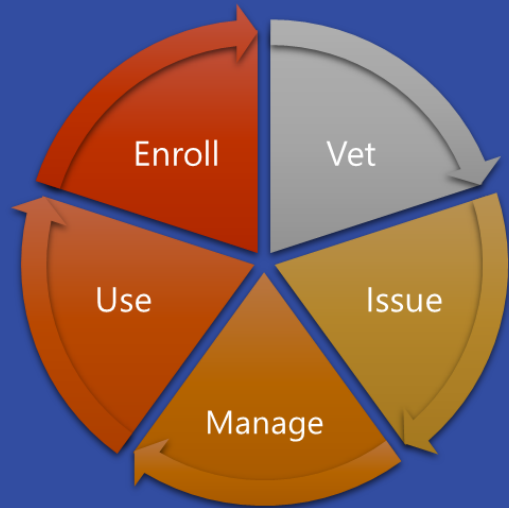**ALLIED IDENTITY**

The iChip® Healthcare Provider Identity Suite is designed to improve security through a unique multifactor management system, track payer assets, and improve emergency response. Allied Identity technology is based on international (ICAO) and federal (NIST & HL7) standards and is designed to have backward compatibility with many of the existing physical access systems installed today. Using a biometric enrollment system built on interoperable standards the iChip Suite can communicate with all background services e.g. Interpol. The suite uses sophisticated smart cards built on the iChip® microprocessor that exceeds all FIPS standards for Authentication and eSignatures.. The suite helps HR departments comply with CMS, Section 6201 of the Patient Protection and Affordable Care Act (PPACA) and the Medicare Modernization Act requirements to conduct background checks. Our system automatically comes with hooks to the Salamander Live Emergency Response Software and integrates with printers from Fargo, Zebra and Matica.

Benefits to the Healthcare Provider

- Eliminates ghost employees

- ID's can be instantly read on mobile devices in field without internet connectivity

- ID's have eSignature capabilities for asset check-in and out e.g. crash carts or ventilators.

- The ID holds training, certifications, Emergency Health Record file built on HL7 standards and other related data for instant verification.

- Can be tied to a secondary Uniform RFID tag (in buttons or epaulets) for high security assurance at gates.

- Integrates a vital EMS solution as part your governments national security system and plan

- Supports 7 types of Biometric modalities

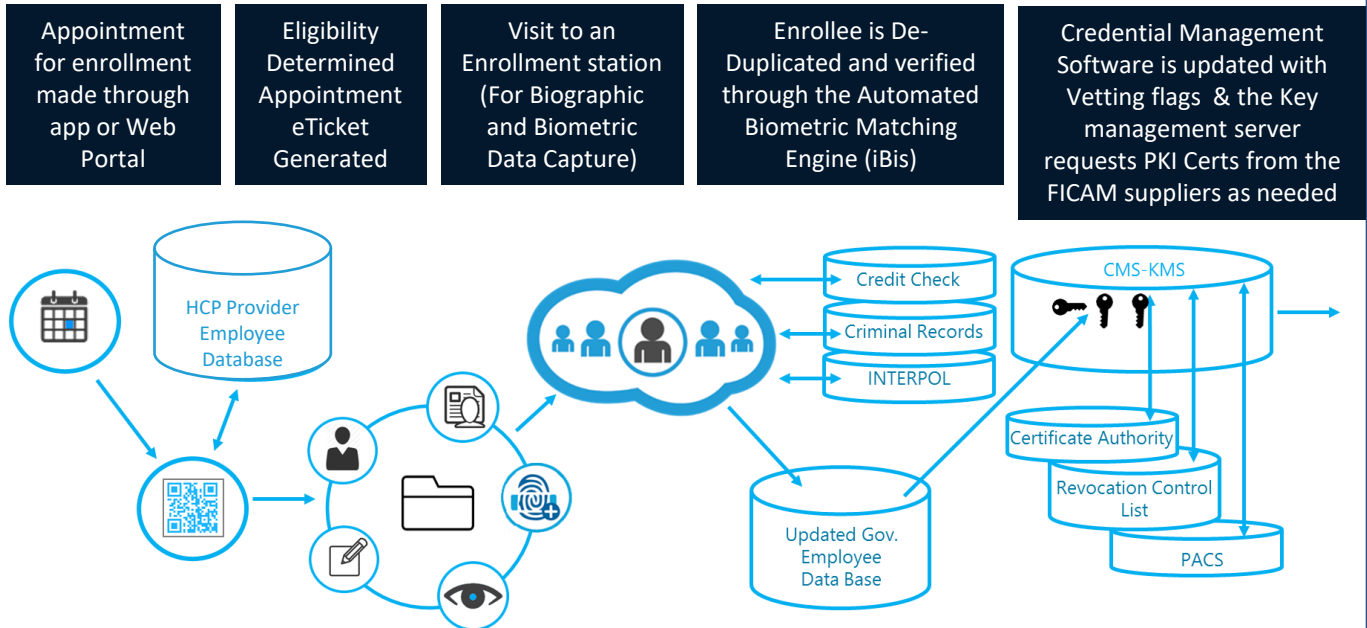- Integrates with PACS, Time and Attendance, HR and Single Sign-On Solutions

Enroll — Vet — Issue — Manage — Use

ALLIED IDENTITY®

Call us today +1 747-215-9200

Credential Part #	Card-File Type	Interfaces	Features
SASICNIICAOCL	ICAO 9304	ISO 14443-A/B	Authentication, eSignatures
SASICNIICAOCP	ICAO 9304	ISO 14443-A/B & Prox	Authentication, eSignatures
SASICJXPIV2CL	PIV II	ISO 14443-A/B	Authentication, eSignatures
SASICJXPIV2CP	PIV II	ISO 14443-A/B & Prox	Authentication, eSignatures
SASICJXPIV2DI	PIV II	ISO 7816 & 14443-A/B	Authentication, eSignatures, SSO
SASICJXPIV2DIP	PIV II	ISO 7816 & 14443-A/B + Prox	Authentication, eSignatures, SSO

Enroll & Vet

Appointment for enrollment made through app or Web Portal	Eligibility Determined Appointment eTicket Generated	Visit to an Enrollment station (For Biographic and Biometric Data Capture)	Enrollee is De-Duplicated and verified through the Automated Biometric Matching Engine (iBis)	Credential Management Software is updated with Vetting flags & the Key management server requests PKI Certs from the FICAM suppliers as needed

Issue & Manage

Appointment set for credential pick-up	Record is sent for Printing & Encoding	Enrollee is re-verified through Biometric Matching at Distribution and link verified to user's cell phone and provider assets	Credential management Software notified

www.alliedidentity.com