FALKEN Secure Networks RFID

HOSPITAL

PalmSecureID IN HEALTHCARE

Improving Identity Authentication, Patient Safety and Security

while Protecting Patient Privacy

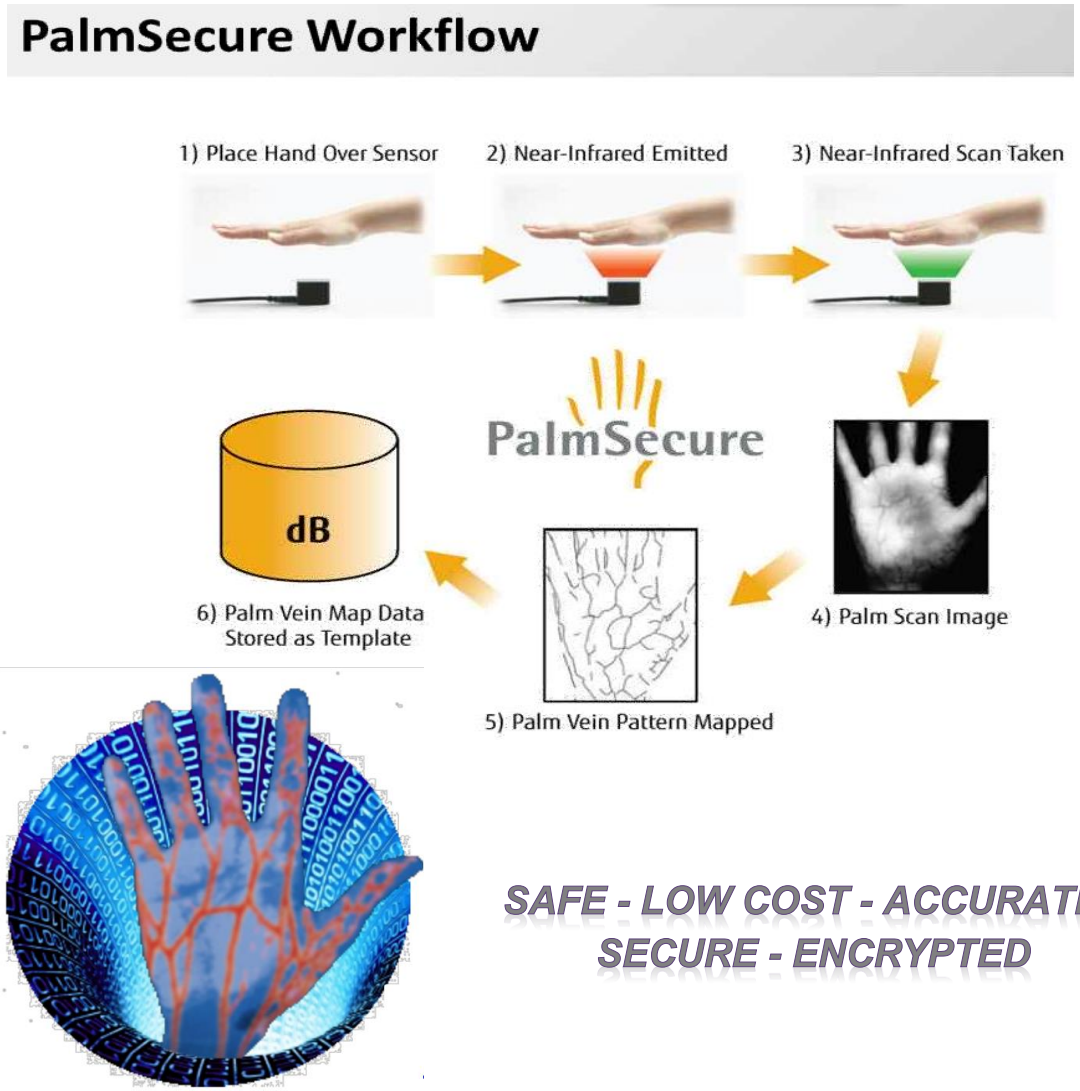
"The biggest problem we face in medical informatics is the identification of the patient," says Raymond D. Aller, MD, director of informatics in the Department of Pathology, University of Southern California, Los Angeles. "Our traditional identifiers are just not good enough. Every day, in every large city in the U.S., specimens are collected from the wrong patient, testing is run, and the patient is treated based on results that belong to someone else. These are preventable errors."

Clearly, patient identification relates directly to patient safety, which is a number-one priority for hospitals. Indeed, it is also the foundation of a viable Electronic Health Record (EHR) system. The World Health Organization Collaborating Centre for Patient Safety Solutions as well as the HITECH Act in the USA encourages the use of at least two identifiers to verify a patient's identity upon admission or transfer. In recent years, biometric technologies have emerged as solutions to not only protect medical records from being tampered with, but also to accurately identify patients. Until now, there has been no biometric technology that can achieve the highest levels of security and usability at a reasonable cost. Palm-vein recognition hits that sweet spot of biometrics between security, cost, accuracy and ease of use that make it an optimal physical and IT access control solution for health care organizations.

The vein pattern in your palm is
totally unique to you.
No one else in the world can match it.

FALKEN Secure Networks RFID

PALMSECURE ID is FSN's industry-leading hardware and software integration based on Fujitsu's unique Palm Vein Scanning technology. Like Fingerprints and Iris eye patterns, each vein pattern in the palm of the hand is unique to each individual including those born as twins. The right palm is different from the left. It is hygienic, contactless, more accurate and less invasive than fingerprinting and iris scanning with authentication response speeds less than 2 seconds. This offers a highly reliable, contactless, biometric authentication solution that is non-intrusive and easy to use in a small cube-sensor form factor which is normally encapsulated with hand guide and LED verification of a palm read and match. PalmSecure™ technology has been deployed worldwide in a wide range of vertical markets, including security, financial/banking, healthcare, commercial enterprises and educational facilities. Additional applications include physical access control, logical access control, retail POS systems, ATMs, kiosks, time and attendance management systems, visitor ID management and other industry-specific biometric applications.



SAFE - LOW COST - ACCURATE - SECURE - ENCRYPTED

FALKEN Secure Networks RFID

- Contactless palm vein authentication is fast, hygienic and non-invasive
- No biometric footprint or residual trace left behind after authentication
- Advanced biometric authentication algorithm produces a high level of accuracy with low FAR (false accept rate) and FRR (false reject rate)
- Fast and easy enrollment for all users with virtually no registration failure
- Robust biometric controller can be mounted remotely in secure area
- Encrypted template repository
- Compact design with flexible integration for easy installation into existing access control systems via Wiegand or IP interfaces

Technology Validation:

- Over 190 Hospitals in the US are now using the PalmSecureID technology for patient registration.
- Over 50 USA School Districts are now using PalmSecure for lunch lines.
- Financial institutions in both Japan and Brazil are now using PalmSecureID for ATM authorizations. These and similar products are in use by the US Navy; US Army; the State Of Pennsylvania and private sector

clients. In March 2013, Unibank was announced as the first European bank to implement PalmSecure, initially in its Papillon mobile payment systems at various retailers.

ID Requirements for Healthcare

The Patient wants to:

- Have assurance that his/her privacy is being protected
- Get quick access to the correct patient records and current benefit information (and then see the right medical practitioner)

The Medical Staff want to:

- Easily and accurately identify patients, and get to their patient records as fast and convenient as possible
- Enhance patient privacy and improve convenience during a visit

The Hospital wants to:

- Reduce organizational expenses and administrative tasks
- Improve patient services through enhancement of secured information sharing capabilities

The Funder wants to:

- Assist with combating healthcare insurance and billing fraud
- Reduce phantom billing by ensuring the correct patient is present during service

ID Challenge –Actual Case Study

- Patients in the Harris County Hospital District's database: **3,428,925**
- Times two or more patients share the same last and first names: **249,213**
- Times five or more patients share the same last and first names: **76,354**
- Times two or more patients share the same last and first names, and date of birth: **69,807**
- Number of patients named Maria Garcia: **2,488**
- Number of Maria Garcia's sharing the same date of birth: **231**

The Health Insurance Portability and Accountability Act (HIPAA) in the USA mandates that all healthcare organizations need to effectively meet a set of administrative, technical, and physical safeguards in order to protect the privacy of patient information. Canada has similar regulations under the PIPEDA privacy and regulations covering the safeguarding of personally identifiable information. Furthermore, HIPAA compliance mandates incorporation of minimum 'two-factor' authentication for authorized employees to access protected health information. Basic password management no longer satisfies this requirement. Violating the HIPAA carries severe civil and criminal penalties including fines up to $250K and/or imprisonment up to 10 years for knowingly misuse of individually identifiable health information. Moreover, hospitals and healthcare facilities need accurate verification of patients' identification in order to protect them from medical identity theft and insurance fraud, as well as to streamline outpatient registration processes.

FSN's PalmSecureID for healthcare solution utilizes best-in-class biometric technologies based on Fujitsu's award winning Palm Scanning and our software to secure access to patient data. Using FSN's solution, doctors, nurses, and other hospital employees register their biometric palm vein pattern, to a

smartcard. For example, to access a patient's electronic medical chart, they simply insert their smartcard and place their palm just above the sensor, which is attached to the PC. The biometric sensor converts the palm vein image into a digital record that is then associated with a given patient's medical records. Only doctors and other personnel authorized to treat a given patient can access that patient's records.

On a voluntary basis, Patients initially enroll at an enrollment station or a self-serve kiosk in the Emergency ward. On subsequent visits, a simple palm scan authenticates the patient for health plan, medical treatment and payment processes. Paper form completion and processing is eliminated.

- Eliminates fraud and identity theft
- Reduces registration time
- Enhances patient safety by significantly reducing the risk of misidentification
- Enables immediate identification of patients already in our database

PalmSecureID utilizes a hygienic, non-contact palm vein authentication scanner. It can be used to secure access to patient data or to restrict access to specific laboratories, operating rooms, etc. to authorized personnel only. Doctors can log into the system in sterile areas without having to completely remove their gloves.
In addition to complying with HIPAA data privacy regulations, PalmSecureID allows the optimization of treatment procedures, preventing errors and reducing paperwork. The risks of medical negligence and malpractice lawsuits are also significantly reduced, enabling healthcare facilities to benefit from lowered insurance costs.

PalmSecureID offers a high-performance, reliable, and user-friendly platform, dedicated to meeting the need for positive identification and effectively countering the growth of identity theft and forgery. Operating as stand-alone systems or as part of a network, the PalmSecureID platform is an extremely strong multi-factor identification server, integrating palm vein authentication .This truly 'best-of-breed' solution combines an unmatched level of performance in terms of accuracy and one-to-one(template on smartcard) and/or one-to-many matching (palm template on secure centralized server) with exceptional ease of use, fully complying with US and European biometric standards.

The combination of smart card plus palm vein authentication provides the highest level of security for all concerned. Even if the card or ID is stolen, the account remains secure since authentication also requires biometric identification.

Palm vein technology can be implemented in both 1:1 and 1:N matching environments. Biometric Palm Vein Templates are encrypted, digitized versions of the scanned palm. These templates can be stored on a Smartcard ID card to enable authentication to take place without transmitting data over a network, or in a secure, networked centralized database …..or both.

Match to palm template stored on card

This is a two-factor security (something you have(card) and something you are(palm vein match). It may be further enhanced to a three factor security with addition of a PIN Code or Password(something you know).

- Integral secure and privacy-enhancing smart card solution
- Biometric template stored on card
- No security issues compared to matching on server or database
- Safeguards user privacy and prevents data intrusion
- Operating in an embedded environment offers increased security
- Highly accurate and fast
- Easier and cheaper to install in existing infrastructure

The PalmSecure technology offers up to three factors of authentication in a single unit installation, as well as a bonus capability of an alternate factor of authentication via registration of the user's second hand. As a result, system administrators are enabled to require biometric authentication for all ingress points and layer additional factors of authentication as needed, specifically in mission-critical areas. For example, a customer needing to enter the front door to the building would do so via biometric authentication. The same customer needing access to a mission-critical or highly restricted area would then need to biometrically authenticate and provide up to two more factors of authentication, including key-pad code and/or RFID smart card. The application of this comprehensive, multi-factor technology allows Healthcare institutions to flexibly meet security demands as required and support various compliance regulations.

- "This new technology helps protect patient information and taxpayer dollars."
- "It reduces the possibility of medical identity theft and helps ensure that patients are appropriately billed for the care they receive."

Tim Tindle. *Executive Vice President and Chief Information Officer*
Harris County Hospital District

Carolinas HealthCare System

Case Study: Carolinas HealthCare System

Charlotte, North Carolina

- 4000+ licensed beds
- 15 hospitals, 15 ambulatory care centers, and over 200 physicians offices
- >1,800,000 patients enrolled in the biometric database
- >5 ,000 authentications / day

Patient Safety

- Ensure the right care is given to the right patient

Patient Protection

- Protects against identity theft and insurance card sharing

Improved Customer Service

- Accelerates registrations / decreases patient wait time

EMR/EHR Integrity

- Puts a stop to duplicate medical records

Emergency Support

- Access medical records for unconscious patients (1:N search)

- "There is great importance in properly identifying the patient.
- If there is a main benefit from the system, it will be in helping us avoid patient errors."
- "Carolinas HealthCare System uses this technology to ensure that the right care is provided to the right person." **Dr. Roger Ray, MD.,** Executive Vice President *and Chief Medical Officer*

PalmSecure™ is family of robust front-end biometric authentication solutions for healthcare data and identity management. PalmSecure™ solutions help healthcare providers and payers:

- Protect patient records while assisting with HIPAA regulatory compliance
- Improve patient services through enhancement of secured information sharing capabilities
- Reduce organizational expenses and administrative tasks
- Assist with combating healthcare insurance and billing fraud
- Streamline operations by integrating with existing software program
- Easily and accurately identify patients, clinicians and employees using advanced non-intrusive biometric technology

Patient PalmSecureID Kiosk

The Med-Serv 50/60 free-standing patient registration platform combines years of Fujitsu experience in delivering self-service kiosks. The Med-Serv provides users with a simplified alternative to registration that delivers an enriched patient experience.

The Med-Serv platform provides an interface that lets patients check in, update their profile and insurance, order prescription refills, and settle account balances without waiting in line. The Med-Serv platform gathers patient information via keyboard, credit card, or the Fujitsu PalmSecure biometric technology.

- Install in Emergency Reception
- Implemented at over twenty healthcare systems 65+ hospitals and 300+ physicians offices in the United States
- PalmSecure™ patient registration is fast, convenient and secure Patients use this self-service system to quickly, conveniently and accurately establish identity review and edit personal information
- Hospital staff utilize the 'Administrator Console' feature to monitor system and update records
- Integrates to the Hospital's existing platforms

PalmSecure Self-Serve KIOSK

Benefits for Funders and Patients

Ensure benefits are provided to covered patients only

- Biometric authentication provides positive patient identification
- Facilitate accurate authorization and claims adjudication
- Reduce cross border "health tourism"

Reduce costs associated with fraudulent claims

- Eliminate opportunity to share benefit cards
- Reduce phantom billing by ensuring patient is present during service
- Minimize up-coding by "time stamping" patient arrival and departure

Manage operational costs

- Eliminate duplicate enrollees
- Improve billing accuracy

Protect patients' health and financial well-being

- Ensure patient is present when prescriptions are filled
- Protect patients against medical identity theft
- Slow the increase of health care cost

Benefits for Healthcare

Promotes patient safety

- Ensure positive patient identification
- Identify non-responsive patients for emergency treatment

Mitigate financial risks

- Protect patients against medical identity theft
- Prevent benefit card sharing to reduce insurance fraud

Help meet Meaningful Use criteria

- Protect patient privacy with non-contact non-traceable authentication
- Meet or exceed two-factor authentication criteria

Improves patient and employee satisfaction

- Streamline patient registration and reduce check-in time
- Minimize error-prone data entry and searching for the right person

Reduce Costs

- Reduce effort and costs associated with password resets
- Integrate with EMPI, EMR and patient registration systems

Promotes operational efficiencies

- Reduce duplicate medical records to ensure EHR integrity
- Enhance clinician and employee productivity via SSO

PalmSecureID software and Patient kiosk can be flexibly configured to:

- Integrate with existing healthcare systems
- prompt patients registering for any information updates such as insurance or health plan validity dates, current prescription and over the counter drugs being taken. Research suggests that over 50% of patients have at least one medication discrepancy upon admission to hospital, with many discrepancies carrying the potential to cause adverse health effects.
- automatically verify patient data by sending a verification request to the appropriate insurance company
- Scan a 1D or 2D barcode on an appointment letter from the patient's general physician
- record and set alerts regarding patient wait times for assessment and wait times for admission
- limit which staff have access to a specific patients health records
- other management reports

FALKEN Secure Networks RFID

THE SOFTWARE- FSN PalmSecureID

The FSN-PalmSecure™ software is affordable and rapidly deployed.

Stand-alone solutions or interoperable with existing systems and hardware.

A proprietary algorithm takes the scanned palm image, converts it into a digitized biometric template, and then matches it against a database of pre-registered templates. If a perfect match is found, your identity is verified. The PalmSecure technology false accept rate(FAR) is just 0.00008 percent with an exceptional false rejection rate (FRR) of 0.01 percent. Authentication response time is less than two seconds. The network and power connectivity interface is PoE or USB 2.0. For Privacy and Identity theft protection, an encrypted template repository in the SQL Database is included.

Totally Mobile:

It isn't just about the perimeter, its about the whole facility, inside or out. Use the FSN PalmSecureID software anywhere. It can be fixed to a door, a turnstile, a gate or deployed in the field or even *in* a field!

Real Time:

Information in real time is everything. The ability to *know* there is a problem and have that knowledge available to everyone in the organization, *as it happens,* is priceless. Stop trouble in it's tracks and do it *now.*

Highly Secure:

Your information is secure and encrypted. We do it well enough for our Military customers and conform to the highest commercial protection standards. We also read drivers licenses, passports, TWIC cards, CAC cards or any form of ID *you* decide is OK.

Link Locations:

Link together all your locations into one common operating picture. It doesn't matter if it's two facilities or twenty you can see all activity in real time and receive security alerts from any location our PalmSecure software is active in.

- ### *Open Architecture:*

FSN software application module use Postgres database which is a database which is free and downloadable on the internet and now very similar in functionality and speed with MySQL It has an export function (CSV format) to enable the export of data to use for reporting.

CONTACT

FALKEN Secure Networks Inc

647-930-7373 (CANADA)

sales@falkensecurenetworks.com

Support Service & Training