White paper

valantic bioLock™ for use with SAP® ERP - powered by Fujitsu PalmSecure

valantic bioLock™ for use with SAP ERP - powered by Fujitsu PalmSecure is an advanced security solution for Identity & Access Management (IAM). Enabled by Fujitsu PalmSecure readers, the solution is tightly embedded and natively integrated with SAP® ERP and the HANA platform. PalmSecure uses the physiological uniqueness of the vein structure in the palm of the human hand to reliably determine identity.

Contents

Background – Security

System security is an increasing challenge on many fronts, for public sector entities and enterprises in all lines of business. Systems are simultaneously under attack from outsiders and under threat of insider manipulations. Data is becoming increasingly valuable, whether it is private data pertaining to employees and customers, or intellectual property belonging to the organization. Data loss, often compounded by poor or absent encryption practices, can occur through many avenues including employee-owned devices, non-sanctioned applications, social media and more. Compliance with government regulations regarding data storage, governance and privacy are creating additional pressure on organizations. A data breach or financial loss due to insider fraud can cause severe damage through loss of reputation, stock market loss and other secondary effects. Implementing technological safeguards is becoming increasingly complex with the dramatic increase in networks, connections, devices and applications.

Enterprise Industry - Security Status

Many independent third-party sources of information allow us to take the pulse of system security across industries. These sources publish the results of their studies and surveys at regular intervals. Many clear, consistent patterns can be seen, spanning all types of organizational systems:

- Consistently high year over year levels of loss due to various forms of fraud are being reported across industries and geographies. Much of this involves IT systems.
- Data record breaches have reached alarming levels and seem to be accelerating. Breaches involving tens of millions of data records are frequent.
- On average, the cost of a system breach is in the millions, with individual outlier cases costing far more.
- Insider fraud is most likely to be perpetrated by long-standing, trusted management employees with no pattern of previous offenses. Detection of such incidents is generally extremely slow, and therefore very costly.
- The explosion in the numbers of connected devices, networks, IP addresses and data volumes is greatly expanding the number of threat vectors.

SAP ERP – Security Status

Despite an extensive landscape of security-related features, modules such as “Single Sign-On” (SSO), “Governance, Risk & Compliance” (GRC) and security industry “best practices”, users of SAP ERP systems continue to face major security challenges and suffer costly, publicized breaches. The reliance on password-based security mechanisms throughout the ecosystem enables circumvention of policies and rules. The most common way of circumventing security rules is the “borrowing” or voluntary sharing of passwords. In this way, Segregation of Duties and GRC risk policies are violated and unauthorized insider activities can occur.

Passwords unfortunately cannot identify a user as an individual human being, but simply as someone who knows a password. In other words, identity management as it is commonly known does nothing more than manage a set of password-based permissions, without knowing who is using these permissions, or whether they are legitimate users or impostors.

Adding layers of passwords, enforcing password creation and refresh rules, or passing along stored passwords automatically via SSO rarely increase security. The implementation of physiologically based identity and access management, with its ability to detect the human being behind the password, is a strong and viable option commercially available today, providing a significant step towards greater security.

Traditional Threat Vectors

Reviewing past SAP system security breaches and insider manipulation incidents reveals clear patterns. Threat vectors appear to recur in the following general areas of system activity:

- Activities involving outflow of funds, or the related requisitions, approvals, invoices, purchase orders, transfers, work-flow and more.
- Activities where inventory, raw materials, or work-in-process moves through the supply chain, including retail Point of Sale (POS).
- Activities where sensitive information is viewed or edited including Intellectual Property (IP), customer/vendor data, private employee data, pricing, confidential data, bills of materials and more.
- Activities involving high-level system management or administration such as code changes, global data management and more, usually done by power-users or “fire-fighters”.
- Activities that affect the system periphery such as log-on, physical access, time and attendance, or customer/vendor inquiries.

Threat Response with PalmSecure

Security in any system is generally improved by additional factors of authentication, as opposed to SSO which only achieves greater convenience. The factor of authentication offering the greatest incremental security gain is biometric user identification. This includes many modalities including iris, fingerprint, face, voice or vein recognition and more. Often these are mentioned interchangeably, however there are distinct categories and differences to be aware of.

Some features, like fingerprints or facial geometry, are superficial, visible and offer little privacy. The technologies they use are well known and used globally in law enforcement. Other features such as palm vein structures are hidden physiological characteristics detected by unpublicized technology. A hidden feature as used by PalmSecure is only readable by proprietary devices and is therefore vastly more private and secure. *Fujitsu PalmSecure* is by its nature more suited for enterprise SAP security, shielding its users’ privacy from intruders and law enforcement alike. It is also by far the most accurate modality available.

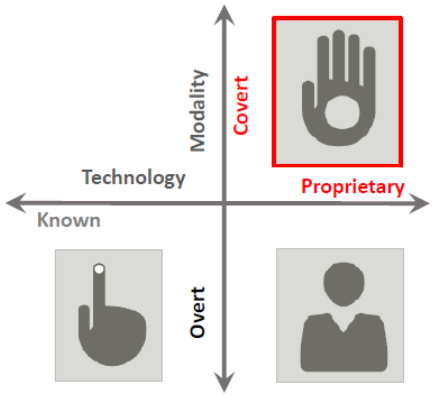

Figure 1. Security Technologies Quadrant

PalmSecure Challenge & Response

Due to the complexity of the current security landscape within SAP ERP systems and the HANA platform, any proposed solution would have to consist of an entirely supplemental overlay, which operates seamlessly, invisibly and independently of existing security.

In fact, the identity and access management enabled by valantic bioLock™ for use with SAP - powered by Fujitsu PalmSecure fulfills that requirement. No changes whatsoever are made to existing security systems, settings or configurations. The user will not know that anything has changed until a supplemental security checkpoint is encountered.

By activating bioLock, this additional palm vein security factor is seamlessly introduced at configurable points. Configurations are stored in a separate, dedicated, SAP ERP system database namespace, which is itself accessible only to administrators authenticated with PalmSecure. This allows a high degree of administrative control while enabling easy roll-back of unwanted configurations.

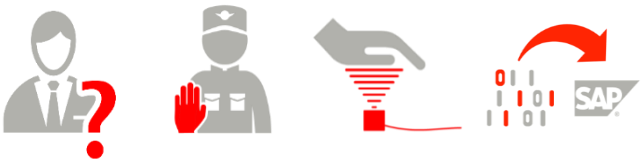

Figure 2. The PalmSecure Challenge & Response

How Does It Work?

Based on knowledge gained over 3,500 SAP ERP project lifecycles, techniques and specialized code were developed that enable bioLock software to intercept SAP ERP transaction commands. This means that when a transaction encounters a bioLock checkpoint while it is executing, the transaction is paused until the requestor has been identified or verified using a PalmSecure palm vein reader device.

Verification and/or identification is not enough, the user's bioLock access authorizations are also checked, before allowing the process to proceed, while logging the result in the background. (Please note, these bioLock authorizations are supplementary to standard SAP system authorizations). The entire process takes just several seconds.

Threat Protection Levels in SAP ERP

Added security may be needed at one or more of these levels:

- Peripheral Access:
  - Customer or Vendor inquiries
  - Time & Attendance
  - Employee Self-Service
  - Informational requests
  - Physical Access Control

  These are **1:1 verifications** with PalmSecure, optional smart card or other information. Devices can be kiosks, shared PCs and more.

- Log-On Access Management:
  - Log on to SAP ERP and the HANA platform
  - Connect to Microsoft Active Directory (AD)

  These are **1:N identifications** using PalmSecure.

- Advanced "Least Privilege" System Access:
  - Granular checkpoints within the SAP ERP system.
  - Control access to menu options, screens, tables, fields, buttons.
  - Control transactions, custom checkpoints, workflows, data masking, threshold field values, dual approvals ("4 eyes").
  - Silent alerts, tamper-proof logging, optional "logging only".

  These are **1:N identifications** using PalmSecure.

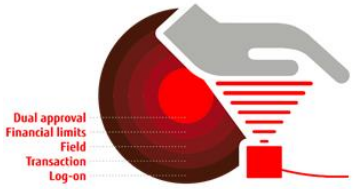

Figure 3. Examples of granular access levels

Privacy Considerations

Public attitudes toward superficial biometrics such as fingerprints are driven by decades of conditioning through law enforcement scenarios, which are reinforced by the entertainment industry. Facial recognition is now following. The recent explosion of fingerprint and facial recognition on mobile telephones confirms these beliefs. Users consciously choose convenience, balanced against fear of the low level of security. Everyone believes that fingerprints cannot be separated from police work. Intuitively, users know that hacking and spoofing are an on-going risk, leading to identity fraud. This helped give rise to current GDPR legislation in Europe, which specifically mentions fingerprint and facial biometrics as needing privacy protection, while warning against biometric storage.

As seen in Figure 1, clear distinctions exist between modalities using visible characteristics versus ones using hidden identifiers. On the technology side, some modalities work with documented, publicly accessible methods, others are proprietary with high barriers to data theft. The fingerprint world (now expanding to include superficial "palm prints"), with its standardized data structures (ISO/ANSI/NIST), easy-to-copy images, comparatively high error rates and global police sharing, represents one end of the spectrum, with high risk to personal privacy. **Palm vein technology,** using invisible, subsurface markers with higher accuracy, advanced private-key cryptography, hashing, proprietary algorithms, non-storage of images and no sharing with law enforcement, **is at the other extreme, strongly answering GDPR requirements for security to be built-in "by default, by design".**

PalmSecure allows users to securely sign enterprise system activities without jeopardizing personal data. Identifying an individual is just the first of multiple steps leading to creation of a PalmSecure "signature". When a user holds their hand over a PalmSecure sensor, a process involving infrared scanning of millions of data points with a special camera detects uniqueness in the palm vein structure hidden below the surface, without storing an image. This initiates the multi-stage creation of the cryptographic signature that is sent on to other systems for matching or signing purposes. This signature, despite containing no confidential data, metadata or personally identifiable data needing protection, is still AES encrypted with an enterprise-specific private key unknown to either Fujitsu, law enforcement or other parties, and thus poses an extremely high barrier to attempted unauthorized use.

System Requirements

SAP ERP

- SAP 4.7 to ECC 6.0, SAP Basis rel. 6.x & higher
- Same O/S as SAP ERP, database Oracle, DB2, MS-SQL, HANA
- R/3, NetWeaver, SAP Portal, SAP GUI ver. 710 or higher

FUJITSU PalmSecure Sensors

- Fujitsu PalmSecure (based on the M1E or F Pro sensors)
- Drivers, runtime as per Fujitsu PalmSecure SDK
- Developer and/or project-specific private key encryption
- PalmSecure SDK V33 compatible

PC Clients

- Windows 7 SP1 (x86 and x64)
- Windows 8.1 Update (x86 and x64)
- Windows 10 (x86 and x64)
- Mac OS X

Integration – Other PalmSecure Solutions

valantic bioLock™ for use with SAP - powered by Fujitsu PalmSecure has an additional advantage: It can be combined with other solutions in the Fujitsu PalmSecure family, such as ID Access, ID Match with RFID smart cards, Single Sign-On (SSO), Workplace Protect and more. This can help solve complex security upgrade challenges involving compound use cases, such as protecting both logical and physical access.

Fujitsu PalmSecure

Security is always in the palm of your hand - PalmSecure enables simple and reliable user identification:

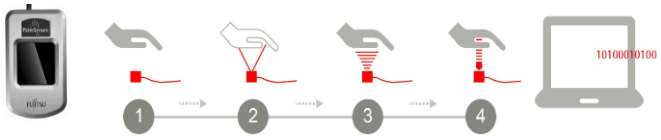

Figure 4. PalmSecure cryptographic authentication

The only reliable forms of identity authentication are based on physiological characteristics. The veins in the palm of the human hand are especially well-suited, being highly complex structures unique to each person and offering many detailed recognition points.

As such they are far superior to traditional systems such as fingerprints or facial recognition. Fujitsu PalmSecure combines the highest privacy protection and the highest accuracy ratings, while never sharing data with law enforcement.

- Maximum security: Veins are concealed under the skin. The identification is literally "live" and forgery-proof, because it requires hemoglobin to be flowing through the user's veins.
- Maximum accuracy: With a false acceptance rate (FAR) of less than 0.00008 percent, Fujitsu PalmSecure is the most precise authentication system available.
- Maximum performance: The initial user enrollment process is complete in just ten seconds. Verification of an enrolled user takes just a few seconds – faster than any password solution.
- Maximum acceptance: The technology is touch-free and thus very hygienic. The hand is simply held over the sensor – which makes PalmSecure very intuitive to use.
- Maximum privacy: No biometric images are stored and therefore cannot be shared with law enforcement. Advanced encryption is used throughout processing.
- Maximum versatility: The technology can be used in a wide range of business use case in SAP ERP systems, including time & attendance, HR self-service, physical access, perimeter access control, granular transactional checkpoints, enforcing GRC rules, preventing Segregation of Duties (SoD) conflicts, GDPR violations and more.
- Maximum SAP system accessibility: With **valantic bioLock™ for use with SAP - powered by Fujitsu PalmSecure**, users can easily enjoy secure access to SAP ERP system data using varied devices such as PCs, tablets, kiosks, POS/Cash registers, banking ATMs and more.

False Acceptance Rate (FAR)
& False Rejection Rate Comparison (FRR)

Authentication Method	FAR (%) =	If FRR (%) =
Face recognition	~ 1.3	~ 2.6
Voice pattern	~ 0.01	~ 0.3
Fingerprint	~ 0.001	~ 0.1
Finger vein	~ 0.0001	~ 0.01
Iris/Retina	~ 0.0001	~ 0.01
Fujitsu Palm vein	**< 0.00008**	~ 0.01

Figure 5. Comparison of security modalities. Source: Fujitsu

About valantic

Founded over 30 years ago, *valantic* (formerly *realtime*) is an established IT service provider with deep experience gained over 3,500 SAP project lifecycles. Part of the SAP® PartnerEdge® ecosystem, an SAP Gold Partner and an SAP Extended Business Member, *valantic* provides consulting plus market-leading "Made in Germany" security software, based on SAP NetWeaver. *valantic* offers 600 IT experts at 15 locations in Europe, plus International Sales, Marketing and support based in the US.

Contact
FUJITSU
Mies-van-der-Rohe-Str. 8, 80807 Munich, Germany
Phone: +49 89 62060 -1183
E-mail: thomas.bengs@ts.fujitsu.com
Website: www.palmsecurebiolock.com