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 a biometric security software solution for Identity & Access Management (IAM) which can easily be utilized for SAP® ERP systems and the HANA platform. Enabled by Fujitsu PalmSecure readers, the solution is tightly embedded and natively integrated with SAP ERP.

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 under attack from outsiders and simultaneously under threat from 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 can occur through many new avenues including employee-owned devices, non-sanctioned applications, social media and more. Compliance with government regulations about 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 many ripple 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 patterns can be consistently 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 cases costing far more.
- Insider fraud is most likely to be perpetrated by long-standing, trusted management employees with no pattern of previous offences. Detection of such incidents is generally extremely slow, and therefore very costly.
- Predictions from many industry sources indicate an imminent explosion in the numbers of connected devices, networks, IP addresses and data volumes, greatly increasing the number of threat vectors.

SAP ERP – Security Status

Despite an extensive landscape of security-related features, modules such as Single Sign-On (SSO) and Governance, Risk & Compliance (GRC), plus security industry "best practices", users of SAP ERP systems continue to face major security challenges and suffer damaging, costly 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 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 the 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 more layers of passwords, enforcing strong password creation and refresh rules, or passing along stored passwords automatically via SSO rarely increase security.

The implementation of biometrically based identity and access management, with its ability to detect the human individual behind the password, is a strong and viable option that is commercially available today, providing a significant step towards greater system 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, orders, transfers, work-flow and more.
- Activities where inventory, raw materials, 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 administrative and system management such as code changes, global data management and more, usually done by power-users or "fire-fighters".
- Activities that touch the system periphery such as log-on, physical access, time and attendance, or customer/vendor inquiries.

Threat Response with Biometric IAM

Security in any system is generally improved by moving to multiple factors of authentication. Some improvement projects such as SSO generally succeed in achieving greater convenience, but no increase in security. In fact SSO does not add any new factor of authentication.

The factor of authentication which offers the greatest incremental security gain is biometric user identification. Biometric identification includes many modalities including iris, fingerprint, face, voice or vein recognition and more. These different modalities vary in cost and provide widely varying benefits. The biometric capability provided through *Fujitsu PalmSecure* palm vein readers is by far the most accurate modality available. Along with bioLock software embedded within SAP ERP, it provides an exceptionally robust additional security factor of biometrically based Identity and Access Management (IAM).

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 1. Comparison of biometric modalities. Source: Fujitsu

A Biometric 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 biometric identity and access management made possible by valantic bioLock™ for use with SAP® ERP - 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 biometric 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 biometrically authenticated administrators – a "biometric firewall". This allows a high degree of administrative control while enabling easy roll-back of unwanted configurations.

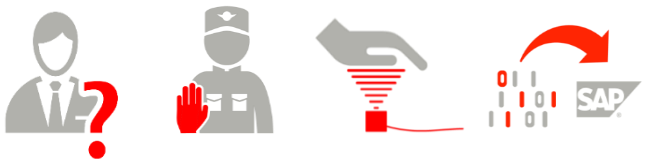

Figure 2. The Biometric Challenge & Response

How Does It Work?

Based on know-how 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 biometric 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 authentication process takes just several seconds.

Threat Protection Levels

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

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

These are 1:1 verifications with biometrics plus smart card or other information. Devices could be kiosks, shared PCs.

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

These are 1:N identifications using biometrics.

- Advanced Granular System Access:
  - Granular checkpoints within the SAP ERP system.
  - Control access to menus, screens, tables, fields, buttons.
  - transactions, custom checkpoints, workflow, data masking, threshold values, dual approval
  - Silent alerts, tamper-proof logging, logging only

These are 1:N identifications using biometrics.

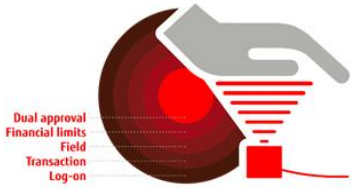

Figure 3. Examples of granular access levels

Privacy Considerations

The storage and processing of biometric data is viewed very differently by various countries. Whereas European privacy laws generally prohibit or discourage centralized storage of biometric data, other jurisdictions actively use such central databases. For example, law enforcement use of Automated Fingerprint Identification System (AFIS) biometric data is widespread. To understand this privacy issue, one must first understand what storage of biometric data really means.

To create a biometric template, a multi-stage process is initiated, starting with the actual image being extracted, from which unique numerical values are measured, which are then further processed by encryption. This process cannot be reversed back to a biometric image, meaning that the final template cannot be considered as private biometric data any longer, but only a unique mathematical or cryptographic construct. Therefore, any security system which deals only with encrypted templates as described, cannot be equated with systems such as AFIS which store the actual source images.

Biometric modalities also differ in that some are standardized, others are not. Fingerprints, for example, are subject to ISO and other standards. PalmSecure templates use a proprietary format, which is further protected by private encryption keys unique to each developer. PalmSecure biometric templates are therefore highly secure, not involved with law enforcement databases, and protect the users' privacy to a higher degree than other modalities.

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 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) 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 at hand - PalmSecure enables simple and reliable biometric user identification:

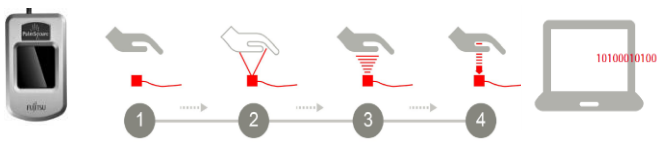

Figure 4. Fujitsu PalmSecure authentication steps

The only reliable forms of personal authentication are based on biometric characteristics. The veins in the palm of the human hand are especially well-suited for biometric authentication. Palm vein patterns are unique to each person – even twins have different patterns. Fujitsu PalmSecure is the most precise, versatile and convenient biometric technology of its kind on the market:

- Maximum security: veins are concealed under the skin, and 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 biometric 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 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 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.

About valantic

Founded over 30 years ago, valantic (formaly 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 SAP Extended Business Member, valantic provides consulting plus market-leading "Made in Germany" security software, based on SAP NetWeaver.

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

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited in Japan and other countries. PalmSecure is a trademark of Fujitsu Limited. SAP and its logos are trademarks or registered trademarks of SAP SE in Germany and in other countries. bioLock is a trademark of valantic ERP systems AG. All other trademarks mentioned herein are the property of their respective owners.