White Paper – **GDPR Compliance**

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

Compliance with GDPR – effective May 2018 – is a serious challenge for users of SAP ERP. Key threat areas are where employee private data, or that of individual customers, is exposed during normal processing. These areas can be robustly secured with valantic bioLock™ for use with SAP® ERP - powered by Fujitsu PalmSecure, ensuring only authorized parties gain access to restricted data, on a continuous re-authentication basis.

PalmSecure data protection in action

Contents

Background – GDPR

The General Data Protection Regulation (GDPR) was adopted by the EU in April 2016 and will replace the current EU Data Protection Directive 95/46/EC.

The GDPR introduces new obligations to data processors and data controllers, including those based outside the EU. Given that infringement can lead to fines of up to 4% of annual worldwide turnover or €20 million, it is important for organizations to assess how GDPR will affect them and prioritize preparations to comply by May 2018.

Figure 1. Approaching GDPR Deadline – May 2018

What is the deadline?

- The legislation was passed in 2016 with an effective date of May 2018.

Who is affected?

The advent of GDPR legislation significantly "raises the bar" with regard to who is required to comply:

- Organizations of any size
- Organizations, regardless of location, that process personal data belonging to individuals or customers in Europe
- Any organizations, such as multi-national entities, that run world-wide instances of SAP ERP

What are the penalties?

Per Article 44, the fines are quite severe:

- Maximum € 20 million, or
- 4% of prior year global revenue (whichever is higher)
- Example: If revenue is € 100 million, fine is € 4 million

What are the requirements?

According to Article 25 of the legislation, system security must exist "by design, by default":

- This appears to favor a built-in technology solution
- This favors a software or system solution over procedures that can be circumvented
- A Data Protection Officer is required for organizations with more than 250 employees
- Formal notification of a breach to affected individuals must occur within 72 hours
- Article 44 forbids export of European private data outside the Eurozone
- Specific data protection techniques recommended include encryption, pseudonymizing, anonymizing
- Specifically targeted towards fingerprint and facial recognition biometrics

SAP ERP – GDPR 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 already face major security challenges and suffer damaging, costly breaches. They are also at risk of falling short of GDPR requirements and incurring hefty fines.

Reliance on password-based security mechanisms enables circumvention of policies. 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 access to GDPR-protected data can occur, such as editing, viewing or exporting.

Passwords cannot identify a user as an individual human being, but simply as someone who knows a password. In other words, traditional identity management 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. Solutions involving passwords will not qualify as "by design, by default".

Only a solution that cannot be procedurally circumvented will effectively ensure GDPR compliance. The implementation of palm vein recognition-based identity and access management, with its ability to detect the human individual behind the password, is a strong and viable option, commercially available today, providing a significant step towards closing GDPR compliance gaps.

GDPR threat vectors - SAP ERP

As GDPR legislation targets anything involving private, personally identifiable data, here are some key areas of SAP ERP data processing that are affected, backed by users' explicit consent:

- Log-On Access Management:
  - Logging on to SAP ERP and the HANA platform
  - Connecting to MS-Active Directory (AD)
- Peripheral Data Access:
  - Time & Attendance
  - Employee HR Self-Service
  - Physical Access Control
  - Individual Customer inquiries (CRM)
  - Medical / Patient information
- "Least Privilege" (Granular) Access:
  - HR employee information (both individual access and HR administration of individual data)
  - High-level actions involving HR data (e.g. SU01)
  - Power-user actions or queries related to individual employee or customer data
  - IT & security administration of any of the above
  - Granular access to GDPR-sensitive menus, screens, tables or fields
- Hardware access points could include:
  - Kiosks, shared PCs, tablets, turnstiles, cash registers, POS terminals, ATMs, smart cards and more

Figure 2. Key Compliance Areas – Customer, Patient or Employee Data

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 operational risk, leading to identity fraud. This helped give rise to current GDPR legislation in Europe, which specifically mentions only fingerprint and facial biometrics as areas needing privacy protection, while warning against biometric storage.

As seen in Figure 3, 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-steal 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, and proprietary algorithms which are not shared with law enforcement, is at the other extreme, answering to GDPR requirements for security to be built-in "by default, by design".**

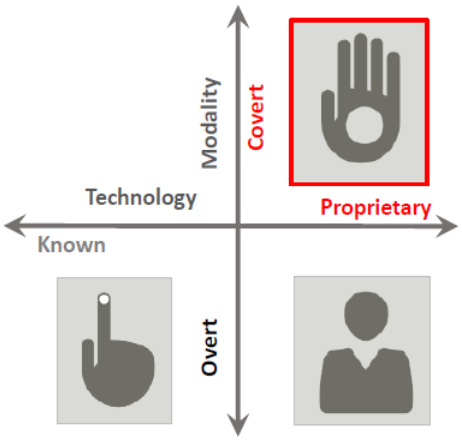

Figure 3. Security Technologies Differentiation

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. This initiates the multi-stage creation of the cryptographic signature or token 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.

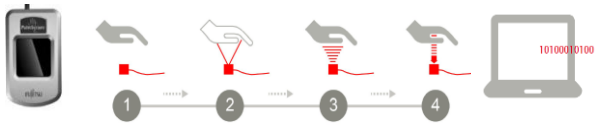

Figure 4. PalmSecure signature – a cryptographic construct

PalmSecure Compliance with GDPR

As noted, some biometric security modalities cannot easily comply with the spirit of GDPR legislation, as they store individual biometric data and images, and do not protect private data "by default, by design". In many cases, private information is represented in easily accessible formats which make them high-risk targets. Sharing of such data by enterprises with global law enforcement entities takes the data outside any original protective sphere and replicates it far and wide. GDPR suggestions to "pseudonymize" data, protecting such data by substituting the real owner's name with a nickname, offers only weak protection. Encryption is a suggested technique, without offering any technical guidelines. Anonymized data is recognized as entirely safe, without clearly defining how to attain it.

Fujitsu goes beyond the bulk of GDPR requirements due to the extensive transformation that occurs in the creation of the PalmSecure signature. An encrypted, unrecognizable signature is created which carries no identifiers tying it to an individual. Within the data, no recognizable personal data can be found. There is no way to reverse the enterprise-specific cryptographic process used. There is no backward path to establish information about the individual. As such, Fujitsu PalmSecure is an ideal choice for users of SAP ERP needing to protect the GDPR-affected data within their system.

Transparent, seamless SAP integration

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 standard security.

In fact, the identity and access management made possible 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 security factor is seamlessly introduced at configurable points as required to protect individuals'

right to privacy. Configurations are stored in a dedicated SAP ERP system namespace, itself accessible only to PalmSecure authenticated administrators. This allows a high degree of risk-based administrative control while enabling easy roll-back of unwanted configurations.

Fujitsu PalmSecure

Security is always at hand - PalmSecure enables simple and reliable palm vein user identification, the most reliable form of personal authentication. The veins in the palm are especially well-suited for authentication. Palm vein patterns are unique to each person – even twins have different patterns. Fujitsu PalmSecure is the most precise, versatile and convenient technology of its kind on the market:

- 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 information is ever shared with law enforcement, would be useless to any third party. Advanced encryption is used throughout to ensure legitimacy of 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 and more.
- Maximum SAP system accessibility: Users can enjoy secure GDPR-compliant access to SAP ERP system data using devices such as PCs, tablets, kiosks, POS/Cash registers, banking ATMs and more.

How does it work?

Based on knowledge gained by *valantic* over 3,500 SAP ERP project lifecycles, specialized code and techniques 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 requester has been identified or verified using a PalmSecure reader device. Verification/identification is not enough, the user's bioLock access authorizations are also checked, before allowing the process to proceed, while logging results in the background. (Please note, these bioLock authorizations are supplemental to standard SAP system authorizations). The entire process takes just several seconds.

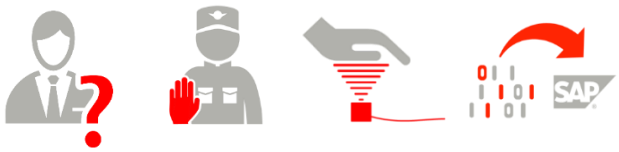

Figure 5. PalmSecure Challenge & Response

GDPR Use Case Example

SAP Self-Serve Kiosk, incorporating PalmSecure sensor

- Connected to SAP ERP
- Integrated PalmSecure OEM sensor (M1E or F Pro)
- Simplified GUI interface using GuiXT, Fiori, limited user access
- User authentication without transmitting any personal data

Examples: Preventing Leakage of Sensitive Information:

- **HR self-service**: vacation requests, status, paychecks, overtime, schedule changes, sick leave, time & attendance
- **Customer inquiries**: Billing, orders, complaints, bank balance, retail checkout, service desk
- **Logistics**: Workplace accidents, safety equipment requests
- **Healthcare**: Medical profile, appointment scheduling, doctor visits, insurance information

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