Inform sheet
Fujitsu secured control and monitoring of SAP

Secured control and monitoring of SAP activities using biometric authentication with Fujitsu PalmSecure™ and bioLock™ software from realtime AG.

Identification Management

In our society of ubiquitous networks, where individuals can easily access their information anytime and anywhere, we are also faced with the risk that others can easily access the same information – anytime and anywhere. Because of this risk, personal identification technology that can distinguish between registered, legitimate users and imposters is generating increasing interest. Traditional knowledge-based (password) security is not meeting this challenge, whether a user is working on a dedicated device or especially when multiple users access SAP via a shared device such as a kiosk or cash register.

Fujitsu has developed a contactless palm vein authentication technology called Fujitsu PalmSecure™. Fujitsu PalmSecure technology uses the very complex vein pattern in the palm of your hand to ensure the safety of your information. Your palm vein pattern remains the same for your entire lifetime and is different on your left and right hand. More than five million reference points of the vein pattern are captured by the highly accurate PalmSecure sensor. Vein recognition technology is one of the most secured solutions because the authentication data is inside your body in your circulatory system, making it very difficult to forge. Smart cards, usernames or ID numbers can be stolen, to be copied or forgotten; biometric characteristics are unique and fixed to a person. This contactless, hygienic system offers maximum security as well as maximum precision.

Fujitsu PalmSecure™ and realtime bioLock™

Investing in biometric access, perimeter and layered security can best protect an organization's SAP data from insider financial fraud, privacy violations, industrial espionage, data loss or unauthorized access to intellectual property, while increasing regulatory compliance.

Protection for SAP

SAP is the market-leading ERP solution used by large organizations. The only biometric security program available that is seamlessly integrated and certified for SAP® and HANA is bioLock™ software from SAP Gold Partner realtime AG.

Combined with Fujitsu PalmSecure the approach for security is to control what happens within SAP not just at the moment of log-on but more especially after the user is in the system. SAP normally relies on role-based authorizations, Single Sign-On and GRC process protocols to prevent segregation of duties violations following a simple password-based log-on. Unfortunately, these techniques offer no protection against impostor's misuse of passwords that were stolen, guessed or voluntarily shared. Passwords alone cannot tie an SAP activity to a specific user to create accountability or to absolutely enforce a rule. Fortunately, dramatic security improvements in SAP are possible by implementing rigorous biometric re-authentication at granular level, which become user-specific checkpoints. Because those re-authentications are based on biometric identity management tied to user credentials ("who you are" security) instead of passwords ("what you know" security) or devices ("what you have" security), the results are indisputable audit trails and accountability.

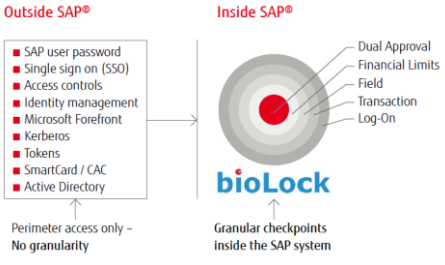
In addition to the fraud protection provided, this helps also to ensure compliance with various government regulations, which usually rely heavily on strong audit trails or logging of activities.

How it works

With bioLock, customizable security check-points can be established based on management policies and business rules on a user-by-user basis. These re-authentication checkpoints can be set at very granular levels if needed such as menu items, tables, transactions, info types, fields, field values, buttons or whenever a critical activity is performed within SAP. Actions such as exporting data, printing data, saving data, changing data and of course viewing data can all be controlled. This could protect anything involving sensitive or private data, large amounts of money, or any mission-critical information that would be of value to unauthorized parties if stolen. On a user by user basis, you are able to:

- Restrict access entirely to any given menu item or screen
- "Mask" sensitive fields of data in that screen so that those fields will not populate for a user with insufficient credentials
- Set threshold field values that cannot be exceeded
- Disable buttons for saving, printing or exporting
- Require presence of a second credentialed biometric user

Here is what we mean by granularity within the SAP system:



With bioLock, a given granular function (example: ME54N, Release Purchase Requisition) can be 100% "locked down", with the exception of named ("white-listed") users. Anyone else attempting the function will be rejected, and cannot gain access regardless of their pre-bioLock level of SAP authorization.

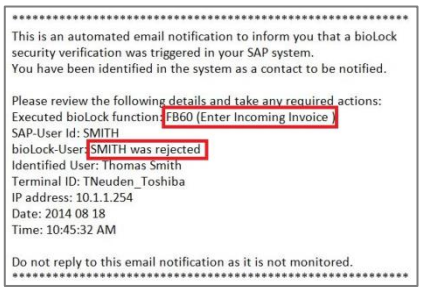
As examples, if an employee is transferring a large sum of money, or setting up a new vendor account, or opening a customer's file with all their personally identifiable information (PII) visible, these activities are critical enough to require biometric re-authentication.

This can accomplish several goals:

- Absolutely prevent a user from gaining access to unauthorized areas.
- Create true accountability for each user's actions.
- Enforce any segregation of duties, or checks and balances deemed necessary by the organization's GRC rules, business risk management or regulatory requirements.
- Generate a robust audit trail with notifications of user activities, including failed access attempts.
- Provide employers legal ammunition to pursue rogue employees.

Existing SAP security, roles and authorizations are unchanged – bioLock™ software complements and reinforces existing SAP security and GRC.

While log-on, standard transactions or info-types are protected by simple configuration, more advanced checkpoints can be set via ABAP code (z-transactions, field exits, enhancements, or modification to SAP code). Checkpoints are seamlessly and invisibly interposed into SAP business logic to trigger re-authentication. End-users have no access to checkpoint code. Tamper-proof log file information is available to auditing tools and can silently alert a supervisor to fraud attempts via email:

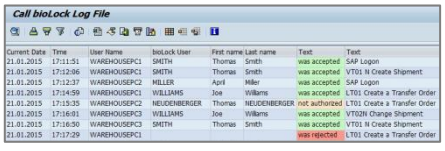


Auditors can now prove which person looked at the balance sheet, changed a purchase order, exported the customer list, edited a social security number or did a large wire transfer to a foreign country. Security is no longer a recommended set of protocols, but a strictly enforced procedure that prevents password-related fraud and user impersonation.

System administration

Employees can be enrolled into bioLock in a few minutes, with both palm templates stored and with the optional addition of a smart card. This establishes the reference bioLock template.
Additional information can be collected and stored with the bioLock user record (separate from the SAP user record), such as validity date range of the biometric template. Biometric access can be pre-set to expire on a given date, thus preventing "ghost workers" (former employees, contractors, temporary users). Biometric credentials are assigned to each user defining the scope of activities allowed or forbidden.

More options include restrictions on the user's nationality and the IP address range they should be accessing the SAP system from. Here is an example in the automatically generated log file of the results of users logging in:



Biometric scanning

Biometrics in the form of palm vein scanning is used at security checkpoints. The Fujitsu PalmSecure palm vein scanners are used, whether attached as a USB device, built into a Fujitsu mouse, attached to a kiosk or cash register. PalmSecure uses Fujitsu's proprietary extraction and matching algorithms.

When a palm vein scan is executed, the user's biometric data is encrypted for security. A user's privacy is therefore always protected and actual biometric images are never stored, thus alleviating privacy concerns.

An initial scan to enroll a user involves taking several readings to establish an average baseline. Once enrolled, a user experiences only a momentary interruption when asked to re-authenticate. The re-authentication process takes at most several seconds, depending on the speed of connection to the server. Regardless of the SAP user profile that appears to be signing on, bioLock will truly identify the actual user based on biometrics. Depending on whether users have the appropriate credentials, or how a given activity is restricted, they may be accepted or rejected.

How bioLock™ is licensed

The product is licensed in user tiers graduating up to an enterprise-wide license. In addition to the named users, benefits extend to the passive monitored users, who don't actually interact with the software yet are protected by it. In bioLock each protected function can be globally locked down, meaning only specifically credentialed users have access to that function, even if they are an administrator or other type of power user.

Example: If 500 named employees out of 3,500 are empowered to execute SAP financial functions, the other 3,000 users are specifically excluded from financial functions and would not be able to do any finance activities, (even with an administrator, DDIC or "firefighter" password), unless they have a biometric credential. Although the 3,000 users are passive, bioLock protects and monitors the entire SAP system against

unauthorized activity by any passive user. This would apply to any SAP function that you choose to control. Former employees, auditors, consultants and potential intruders will also be shut out.

Therefore, although the software license fee appears to cover only the named users, in reality the cost of ownership should be viewed as spread over the entire protected SAP user base whether named or passive users. In addition to the initial license fee, an annual maintenance covers support, bug fixes, new versions and documentation.

Implementation

The software is installed via transports into its own namespace in SAP. Current SAP versions including HANA are supported, plus limited functionality in older SAP versions. The bioLock software resides in the SAP system protected behind a "biometric firewall", which means after installation it can only be accessed with dual verification of two trusted biometric users ("dual authentication").

Users can be enrolled into bioLock in a few minutes, optionally capturing some of the user profile information from SAP (SU01) or Excel upload, if available. A biometric scanner at each named user's workstation or shared device is required. Secure, remote enrollment of users and installation of bioLock client software is supported.

Establishing a bioLock user does not override or change existing SAP security settings or GRC. Instead, bioLock overlays and reinforces existing security. Use is extremely intuitive so there is no training or learning curve, users simply respond when prompted. Administration of bioLock uses skill-sets that are usually already "in-house" such as Basis Administration, SAP Security, ABAP or HANA.

Features and benefits

Main features	Benefits
Highest security level	
■ Data underneath your skin – hidden inside your body ■ Highly complex vein pattern – more than 5 million reference points ■ Encryption of vein templates via EAS, unique encryption key single for every project/ customer ■ Lowest false acceptance rate (FAR): < 0.00008 and false rejection rate (FRR): ~ 0.01 compared with other biometric technologies	■ No data theft – no latent biometric images left behind ■ No copying of palm pattern ■ Easily practicable for users, hygienic, high user acceptance ■ BSI certification allows usage of PalmSecure in high secure areas ■ Accepted at ISO certification ■ SAP certification of bioLock software since 2002, developed by SAP Gold Partner realtime ■ Easy integration into existing infrastructure ■ Flexibility to use with many devices such as PCs, tablets, kiosks, cash registers and more ■ Administered with in-house SAP skill sets (Basis Administration, SAP Security, ABAP, HANA).
Control and monitoring	
■ The verification performed uses palm vein biometrics, as opposed to relying on passwords which are easily compromised. Although passwords do continue to be used because they are required by SAP, they are only the first step in verifying a user's identity and are followed up with the second factor biometric authentication which is indisputable. The biometric verification is done after the password log-on, (as opposed to before password log-on with typical Single Sign-On systems) thus protecting this process internally within SAP. ■ The biometric sample that is taken at the moment of signing on is compared to a stored "reference template", which is the template originally stored for that user at the time of their enrollment into the system. This original enrollment was done under very controlled conditions, and the reference template is therefore considered to be authoritative. It makes sense therefore to store that reference template very securely. In the case of bioLock, the reference template is stored within SAP, behind a biometrically secured "firewall", and not in an application residing outside SAP (such as is customary with Single Sign-On systems). ■ Some systems capture biometric images and store them, whereas bioLock never stores any actual images. Instead, the relevant data points are extracted by the palm vein scanner, converted to numerical values using Fujitsu algorithms and encrypted before being sent to SAP for comparison with reference templates. ■ Not all systems are created equal in terms of their matching and identification algorithms. In the case of bioLock, powerful 1:N identification matches are standard, combined with 1:1 verification in cases where an additional user information field is provided, for optimal speed and accuracy. ■ Logging of activities, including errors and violations, are securely logged in a tamper-proof way that is accessible to third-party audit tools on a "read-only" basis. Violations can be transmitted to supervisory levels via silent e-mailed alerts in real time. ■ Generally, Single Sign-On (SSO) systems greatly increase convenience, but decrease security. Password credentials are automatically passed on, giving a false sense of security, because	■ Usage of the same technology for every kind of identity management/access management within an organization. Wide range of usage: ■ Enforce GRC policies by setting up appropriate biometric user credentials and checkpoints to match GRC rules. Prevent fraudulent users from violating Segregation of Duties via password theft or sharing. ■ Financial Fraud - With bioLock the risk of insider fraud can be mitigated, by controlling Procure to Pay activities such as requisitions, purchase orders, wire transfers, journal entries and more. This is done with the multi-level control checkpoints including maximum field values, dual authentication or outright blocking of features. ■ Inventory Shrinkage - The ability of employees to release inventory, ship goods, create customers, write off goods, issue credits and such can be prevented or controlled by requiring biometric authentication at every step in the supply chain. ■ Time & Attendance - The bioLock system can use its biometric identification capability to indisputably determine the identity of an employee clocking in or out at work. This eliminates payroll fraud opportunities such as "buddy punching" or abuse of clock-in passwords, resulting in major payroll cost savings. Data is seamlessly integrated with SAP payroll. ■ Point of Sale (POS) - In a retail environment, it is possible to control every cash register transaction by requiring biometric authentication, thus reducing inventory shrinkage. Despite employees' sharing of POS devices or generic logon, true identity management is assured. ■ Access to information - By requiring biometric log-on and/or re-authentication, access to viewing or changing sensitive information can be controlled and monitored. Sensitive data might include customer records or Personally Identifiable Information (PII), health care records, HR or personnel data, high-level financial data, company secrets, intellectual property (IP), engineering drawings, etc.

Main features	Benefits
if the password has been compromised then the fraudulent user can still impersonate the true user, even in multiple applications.	■ Pure Logging - If desired, bioLock can be used to simply monitor and log specified activities within SAP, without preventing activities or alerting employees to the monitoring. ■ Physical Access - Currently in development, this capability will tie SAP PM (Plant Maintenance) assets such as building entrances to the SAP HR data and bioLock controls, so that access to physical assets can be controlled and monitored through biometric identity management.

More information

Fujitsu OPTIMIZATION Services

In addition to PalmSecure, Fujitsu provides a range of platform solutions. They combine reliable Fujitsu products with the best in services, know-how and worldwide partnerships.

Dynamic Infrastructures
With the Fujitsu Dynamic Infrastructures approach, Fujitsu offers a full portfolio of IT products, solutions and services, ranging from clients to datacenter solutions, Managed Infrastructure and Infrastructure as a Service. How much you benefit from Fujitsu technologies and services depends on the level of cooperation you choose. This takes IT flexibility and efficiency to the next level.

Computing products
www.fujitsu.com/global/services/computing/
- PRIMERGY: Industrial standard server
- SPARC Enterprise: UNIX server
- PRIMEQUEST: Mission-critical IA server
- ETERNUS: Storage system
- BS2000 mainframes

Software
www.fujitsu.com/software/
- Interstage: Application infrastructure software
- Systemwalker: System management software

More information

To learn more about Fujitsu secured control and monitoring of SAP please contact your Fujitsu sales representative, Fujitsu business partner, or visit our website.
http://palmsecurebiolock.com/

Fujitsu green policy innovation

Fujitsu Green Policy Innovation is our worldwide project for reducing burdens on the environment. Using our global know-how, we aim to resolve issues of environmental energy efficiency through IT. Please find further information at:
www.fujitsu.com/global/about/environment/

About realtime

Established in Europe over 30 years ago by former senior SAP® managers, realtime is a certified SAP® Software Gold partner specializing in biometric security and identity management software systems. Their bioLock™ software is the only biometric software system natively embedded and certified by SAP®. A wide variety of global corporations in many industry verticals, plus government entities are served by realtime software.

Copyright

Disclaimer

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.fujitsu.com/palmsecure