valantic bioLock^{TM} for use with SAP® ERP – powered by Fujitsu PalmSecure

Demo scenario description for simulation software

FUJITSU and valantic have developed simulation software for evaluation and demonstration. This shows the live working functionality and benefits of valantic bioLock^{TM} for use with SAP® ERP – powered by Fujitsu PalmSecure within a simulated SAP environment. This document describes the sample security scenarios, and how to demonstrate them using the simulator software. A PalmSecure reader device is highly recommended but not essential.

Content

Introduction

This software has been developed to help customers and partners to understand and demonstrate the valantic bioLock for use with SAP ERM – powered by Fujitsu PalmSecure solution. valantic bioLock for use with SAP ERM – powered by Fujitsu PalmSecure combines the bioLock control and monitoring software which can control the log on as well as every function inside SAP with the PalmSecure biometric authentication to reconfirm the identity of the actual person. This would apply to any SAP function that is chosen to control and monitor.

This module has been developed in response to requests for an offline simulation system that can be used in a variety of environments including trade shows, where connectivity is often limited or entirely unavailable. Its purpose is also to enable a quick overview demonstration of the bioLock and PalmSecure system capabilities without requiring the user to possess any specialized SAP knowledge or training. It is designed to qualify a prospect's interest in moving on to a more detailed demonstration in the traditional sense.

The concept of developing an off-line way to demonstrate bioLock and PalmSecure with SAP posed a large challenge. SAP by its nature is an online transaction processing system; it is a very large set of programs which require the processing power of an organization's largest computers such as mainframe or mid-range computers, running on large databases such as Oracle, in order to extract the data required to demonstrate a given functionality. An SAP user typically connects with the host system via a PC-based thin client module, which is Windows-based software that communicates with the server.

Overview

To cope with this challenge, valantic bioLock for use with SAP ERM – powered by Fujitsu PalmSecure simulation software has been created as a stand-alone application which meets the needs outlined above:

- The PalmSecure components have been fully incorporated, in the sense that users can be enrolled and authenticated in a "live" mode, such as a trade show where a prospect wants to see that component in action. All enrollments and storage of templates are occurring locally, not in SAP.
- The bioLock components are incorporated, so that the demonstration can show the bioLock system interacting with PalmSecure to authenticate a user attempting an SAP activity. Although the user appears to be authenticating against the remote SAP host system, in fact they are authenticating against a local database.
- The SAP components, where SAP menus and screens are called up to log in and interact with bioLock and PalmSecure, are also simulated locally with screenshots. They appear to be calling a remote host database however, because by the definition of our challenge, they cannot occur online, they are actually occurring locally on an offline demonstration PC.

So, while we have met the challenge of providing an off-line demo capability, this brings with it certain limitations:

- The Quick Demo System is a very controlled application which has only limited capability to show SAP functionality. The demo is tightly scripted and does not allow for deviations. For example, once you arrive at a certain SAP screen, such "VA01 – Create a Sales Order", you cannot enter data in the fields, or search the database to populate the fields, etc. The point is to show how the access to that screen could be biometrically controlled using bioLock and PalmSecure, but to go no further.
- Certain functions seen on SAP menus are inactive. Choices were made while creating this application to only show a limited set of activities which are fraud-prone, in areas of HR, Finance, and so on.
- Certain Windows keyboard functionalities are disabled. For example, note that when a window is open, the "Minimize", "Resize" or "Close" functions are disabled. Screen navigation is tightly controlled.
- The application cannot be connected to an actual SAP host system but can only run in stand-alone mode.
- For the advanced user audience, this demo will only be a "teaser" and will require a follow-up demo against a live SAP system.

System Requirements

Supported Operating Systems:	Windows 7, Windows 8.1, Windows 10
Required Software:	valantic bioLock for use with SAP ERM – powered by Fujitsu PalmSecure simulation software and PalmSecure sensor drivers
Required biometric Device:	USB PalmSecure sensor or PalmSecure mouse with built-in M1E sensor*

*Please verify exact sensor requirements and operating environment. Only PalmSecure readers based on the M1E sensor are supported. M1E sensors are identified on the back by a product ID (KD03816). Older PalmSecure Devices using the M1 Sensor (identified on the back as product ID KD03231) are only compatible with Windows 7 and will not work with Windows 8 or higher. Laptops with integrated PalmSecure sensors (e.g. Fujitsu Stylistic) are not currently compatible, as the sensors do not perform 1:N identification but only 1:1 verification.

NOTE - What you do NOT require:

- Network, WIFI or other wireless connection
- SAP GUI
- Access to host SAP system
- bioLock software (PC client or SAP transports)

Important Note regarding Licensing:
As the bioLock OFFLINE DEMO is a simulation that uses depictions of other software interacted with, there are no licensing implications. Neither bioLock nor SAP are actually installed, instead simulated screens and screenshots of activities are packaged into the application. The only product which is installed and used as it would be in any normal commercial setting is the PalmSecure scanner. You must ensure that you are compliant with Fujitsu licensing requirements.

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

Installation
Pre-requisite:
You must have your Fujitsu PalmSecure scanner of the correct type installed on the demonstration PC before installing the bioLock OFFLINE DEMO. If the device is unplugged or not yet installed, you cannot use the demo software and an error message will pop up indicated that no device is connected!

Emergency User Operation – without a device:
For the case that you have forgotten your device, or do not have one, you can imitate the demo by using the emergency user "sapall". Log in using "sapall" and "password". You will see that the authentication request window will come up and you will even see a simulated palm image. The demo will be less effective but still useful.

Now you have the choice between selecting "a" on the keyboard for pretending to accept a valid template or to click "s" for rejecting the attempt. You can do the entire demo without the PalmSecure device however this should only be used for emergencies as the customer will be far more impressed by enrolling themselves with the actual PalmSecure device.

You can also change the name of the emergency user if required. Go to the bioLock_Demo directory and open the bioLock.txt file. You will see the emergency users defined as "sapall" or "SAPALL". You can rename any of them to your own name or your customer's name. Do not add a 3rd user as a 3rd user would not be recognized! Also remember that once an emergency user is changed to "Chris" you would not be able to use biometrics for user "Chris" as the system would default to key entry!

The full bioLock Control and Monitoring Software can control the log on as well as every function inside SAP using the PalmSecure to reconfirm the identity of the actual person. You will learn the details in the detailed description.

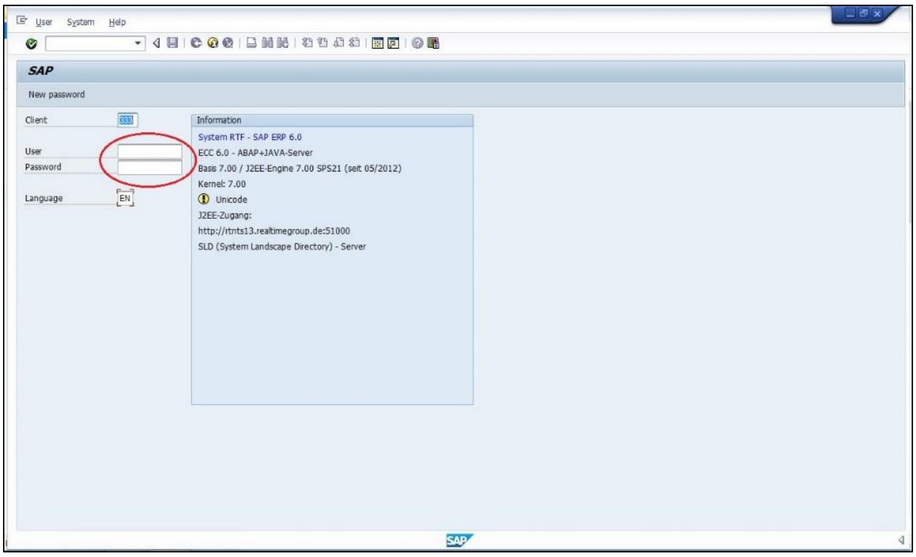
In the demo software the 'minimize' and 'X out' functionality are not enabled. To close the software you need to use the back button (or use Alt/Tab to switch to another application).

Enrollment
Enroll the FIRST user with a biometric template. Note: You only need to do this ONCE per demo computer!
The first time you start the demo system on any computer you need to enroll the first user with a Palm Vein template:

From the first SAP Logon Screen, log in with user "admin" and password "password". This user is the only one that can access the system without PALM VERIFICATION. Note that this user can ONLY access the bioLock menu for enrollment.

Deleting Templates
All biometric templates are stored in the bioLock_Demo/Data folder. You can see all files ending in x.dat. At the end of a demo day, you might want to delete some of the templates but make sure you exclude your own – otherwise you need to re-enroll.

Logon to SAP
SAP Log On Screen (users see this after connecting to a specific system from their computer):



Client 333

User

Password

Language EN

Information

System RTF - SAP ERP 6.0

ECC 6.0 - ABAP+JAVA-Server

Basis 7.00 / J2EE-Engine 7.00 SPS21 (seit 05/2012)

Kernel: 7.00

Unicode

J2EE-Zugang:

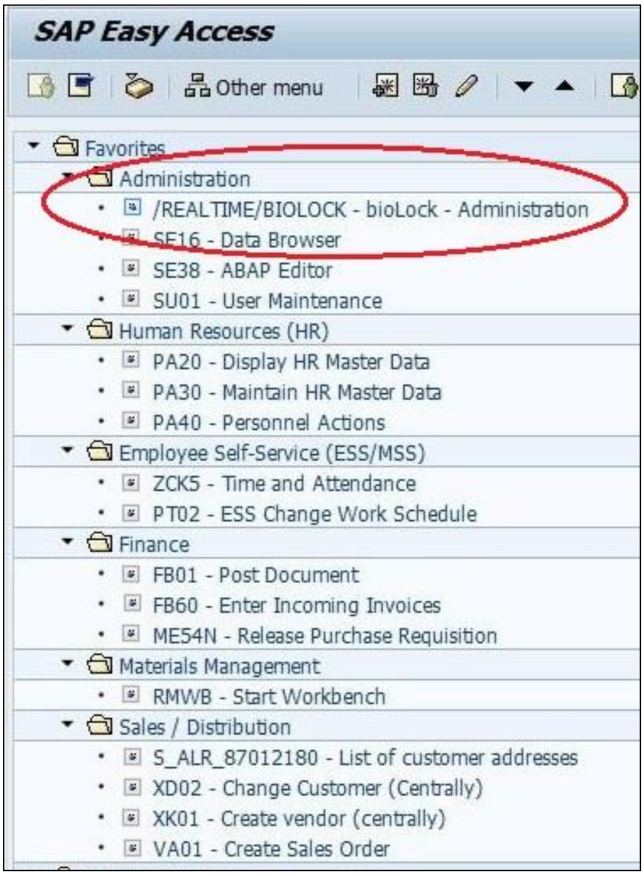
http://rtnts13.realtimegroup.de:51000

SLD (System Landscape Directory) - Server

Demonstration – Getting started with Enrollment

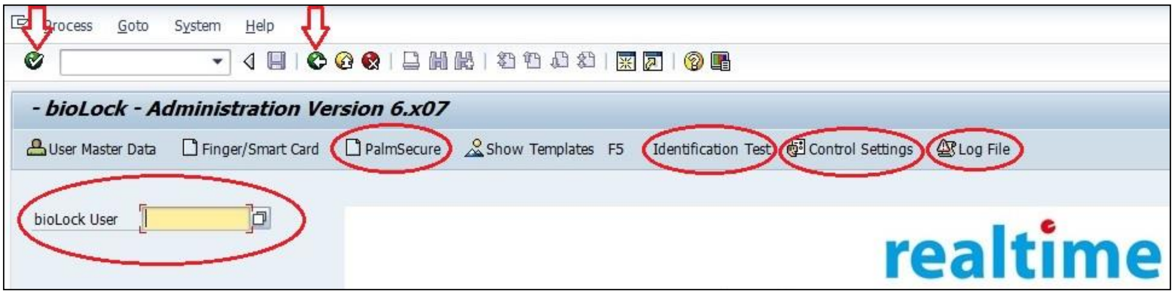
Once you are logged in you see the SAP Menu on the left. We have highlighted our 16 different demo scenarios in the Easy Access Menu. Everything is SAP authentic and users should not see that this is not an on-line SAP system (other than that you don't have to enter any detailed data).

SAP Easy Access Bookmark Menu with bioLock Administration and 16 demo scenarios:



- Favorites
  - Administration
    - /REALTIME/BIOLOCK - bioLock - Administration
    - SE16 - Data Browser
    - SE38 - ABAP Editor
    - SU01 - User Maintenance
  - Human Resources (HR)
    - PA20 - Display HR Master Data
    - PA30 - Maintain HR Master Data
    - PA40 - Personnel Actions
  - Employee Self-Service (ESS/MSS)
    - ZCK5 - Time and Attendance
    - PT02 - ESS Change Work Schedule
  - Finance
    - FB01 - Post Document
    - FB60 - Enter Incoming Invoices
    - ME54N - Release Purchase Requisition
  - Materials Management
    - RMWB - Start Workbench
  - Sales / Distribution
    - S_ALR_87012180 - List of customer addresses
    - XD02 - Change Customer (Centrally)
    - XK01 - Create vendor (centrally)
    - VA01 - Create Sales Order

Please click on "bioLock Administration" at the top of the menu. You will see our main bioLock Control and Monitoring Center administration screen. Type your preferred demo user name in the white user field (We recommend first name or first initial / last name). Now click "PalmSecure". A pop up will ask you to enroll your palm:



If this is your first time we recommend using the plastic hand guide for PalmSecure (if available). Lift and lower your hand as instructed by the pop up window and please spread your fingers (High Five). Once the enrollment is successful, you will see a confirmation.

Now you need to go back to the SAP Log On Screen. There are only 2 buttons that you need to remember for the demo - both of them are green (highlighted in the screen shot above).
There is the green checkmark in the left upper corner that is the "confirm" button and has the same function as ENTER. Then there is the Green Back Button which will take you one screen back.

Simply click the Green Back Button twice and you should be back at the SAP Logon Screen.

Now Log On using your previously enrolled user name (First Name etc.)

You will see that the PalmSecure verification window will pop up for the SAP Logon. This is the first thing we want to tell customers that we protect the logon to prevent password sharing! Now it is important to point out that all other access control systems stop here while our bioLock control and monitoring center is just getting started.

NOTE that no colleague or customer has to logon as "admin" anymore as you can now use YOUR own user to log on to the system and enroll colleagues and customers.

Once you are back in the SAP main menu it is important for you to know that main menu's in SAP are called transactions. All item lines on the left of the screen are a selection of 16 well known transactions that we have combined in a book mark menu – just like any SAP user would do it on their home screen. We have also sorted our Transactions into different categories for your convenience. In HR (PA20 / PA30 / PA40) there are 100s of submenus that HR users use every day called "HR info-types" (see detailed instructions for details).

To make it easy the last Transaction in every category simply protects the access to the transaction to show the re-authentication. You can show some protection of very sensitive transactions that only authorized users should have access to.

Also go to back to the bioLock Administration Transaction (first one on the list) to highlight the two following features in every presentation.

Control Center Settings:
Click on Settings to show the table that defines the protections we have set up in the SAP System. Explain that the customer can set an unlimited number of biometric checkpoints in a live SAP system and control them with PalmSecure. Point out that protections can be specifically permitted to biometric templates of selected users only. As per example we can guarantee that only the two senior financial people with their biometric templates can execute outgoing wire transfers over $10,000.

Control Center Log File:
The Log File button shows a detailed log file about all checkpoint activity in the system. You can see who got accepted or was not authorized. You can even see how an unidentified user from a foreign IP address tried to access a highly critical transaction in the system. As no biometric template was identified, the attempt was rejected. Unfortunately we couldn't identify the "intruder". Note that this is a static log file sample. It does NOT show actual activities from your demo in this version of the software. But it shows some possible options that a customer could be interested in seeing. Point out that EMAIL NOTIFICATIONS could be sent to multiple e-mail addresses for every function so supervisors know what is going on instantly.

Try a few of the transactions first before moving on to more advanced functionalities that include table protections, info-types, masking social security numbers, preventing access to credit card information, outgoing wire transfers over $10,000, saving customer lists to a USB stick and time and attendance inside SAP.

Demonstration – Detailed Scenarios
NOTE that for simplicity the last transaction in every category is always a transaction protection only. If you are in a hurry always choose the last transaction as it is simple and straight forward!

Administration
bioLock Administration (Unprotected / allows enrollment / log file view and shows protection table)
PalmSecure / Identification Test / Settings / Logfile

This is the transaction to the bioLock control and monitoring center. Please note that the original transaction contains a massive amount of protection functionalities. We have only enabled a very few main functions for this demo. The most important one is to enroll your palm vein template. You will use this transaction to enroll customers during the show. Simply type their name in the white field and click the "PalmSecure" button to enroll their credentials. Note that you can use this with YOUR user name. You do NOT need to log on as Admin. Now you can also run "Identification Test". Click the button and ask any enrolled user to put their hand over the device. It is important to show users that any authorized or unauthorized user can be uniquely identified. The "Settings" available in the full system are very extensive, but here we have narrowed it down to one important table that you should explain. Here we define the SAP security checkpoints and what we can do with them. Last you see the "Logfile" icon that shows an extensive (simulated) log-file of who got rejected and who got accepted executing which function. Note that this is a screen shot of a real log-file that shows many possible scenarios.
Point out that supervisors could instantly be notified via email notification of unauthorized users' attempted accesses.

SE16 – Data Browser (shows the possibility to protect SELECTED tables only like customer lists)
This is a critical function for SAP users as it gives them access to many tables. We want to show that table "KNA1" (customer list) can only be accessed with biometric credentials while the table "LFA1" (suppliers) does not require biometric verification. Simply select "LFA1" from the drop down and click "ENTER" or the green check mark in the left upper corner. The supplier list will be visible without biometric verification. No go back using the green back button and select "KNA1". Confirm and you see how this specific table is protected with biometrics. Explain how customers can pick and choose which tables they want to protect.

SE38 - ABAP Editor (Transaction protection only / Restricts Access to Source Code of SAP)
This is a critical transaction that allows anybody to access programming source code. This is a typical transaction that any customer would want to protect to ensure privileged biometric access to this sensitive transaction.

SU01 – User Maintenance (Transaction protection only / Prevents copying of users or password resets)
This transaction allows passwords reset and to copy users. Anybody could create secret users that could be used to prevent accountability or to use it after leaving a company and losing original credentials. Here you can also reset passwords to existing users to get access to their credentials.

Human Resources (HR)
PA20 – Display HR Master Data (show Info-types such as 0008 / 0009 and 0006 which is open)
In HR we have 100s of sub-menus called Info-types. HR employees quickly type those Info-types in a field to get access to the desired submenu. In HR many of these menus are critical. In the dropdown box start with the first Info-type, "0006 / Addresses" and "Enter" The address window will become visible without biometric verification as this function is not considered critical by the customer. Now go back using the green back button and select "0008 / Basic Pay". Confirm with "Enter" or the green checkmark.
NOTE: In HR users like to display information. You can also select the "Eyeglasses" icon under the "Green checkmark" to display. It is very sensitive in an organization that employees not know each other's' salaries. Therefore this function is protected with PalmSecure so only authorized users can see that Mr. Miller has an annual salary of $250,000. Go back and select "0009" to show that the bank details are also protected with biometrics. Point out that all Info-types can be individually protected. This allows the customer to further restrict access for authorized users which is one of the major challenges to be addressed this year.

PA30 – Maintain HR Master Data (show how SSN and birthday is masked)
In PA30 you can modify existing HR data. We use this example to show how a standard screen is displayed, but the Social Security Number and the Birthday fields are masked in the original screen. Anybody with the right SAP credentials can see the screen – but NOT the masked data. When an enrolled user provides the biometric template the Social Security Number and Birthday will be un-masked and visible. After selecting the PA 30 transaction from the main menu, you see the "Maintain HR Master Data" Screen. The Info-type Personal Data is pre-selected. NOTE: As this is NOT a pre-selected field, you cannot press "Enter". You need to click the "green checkmark" or the eyeglass icon to continue. Now you have two interesting options:

Put your enrolled hand over PalmSecure and you will see the personal data INCLUDING the birthday and social security information in the left bottom corner.
Now go back to the previous screen, select the "green checkmark" and put your left hand on the device (assuming you did NOT enroll a template with your left hand). You will see the same personal data screen, but the social security number and the birthday are masked or hidden.
Note: You can do this kind of field "masking" with any fields in live SAP screens such as credit card numbers, health information or functional locations in PM notifications.

PA40 - (Transaction protection only / Restricts Access to Personal Actions)
This transaction is used for the hiring process. Unwanted access could allow creating fake employees and paying them. Therefore the entire transaction is protected.

Employee Self-Service (ESS/MSS)
ZCK5 – Time and Attendance (show employee gets identified and recorded for work)

This is the ultimate time and attendance application that allows customers to track time and attendance with biometrics inside SAP. While in normal scenarios the biometric template is matched to SAP User ID's to restrict access, in this scenario we have matched the biometric template with an employee ID in HR. If the worker comes to work in the morning a welcome screen at the gate will require the worker to provide biometric credentials. The system will uniquely identify the worker and register him or her for starting work at this time. The activities are logged directly in the CAT2 tables in SAP. Buddy punching is prevented.

To get started select the transaction and you see a screen welcoming you to work. Any arriving employee will click on the "Identify / Identificar" button and put their hand on the PalmSecure. The system identifies the actual employee based on their palm vein template and logs the employee as arrived at work. Press "Enter" and the next employee in line is ready to do the same. This is great to do with a group of customers that you have previously enrolled. Click the green back button to go back to the main menu.

PT02 – ESS Change Work Schedule (Transaction protection only / Worker changes shift on kiosk)
In ESS (Employee Self Service) we see more and more kiosk application where users access their employee data to view pay stubs, request vacation, file expenses or change shifts. This is a liability for the organization as theoretically anybody could view and modify another employee's data. Only biometric technology can reconfirm that the actual user is the owner of the information in question, and has not stolen/guessed/borrowed the password of the other employee. Therefore the entire transaction is protected and you can see how a co-worker is prevented from changing your shift on your behalf. Of course functions inside ESS should require re-authentication also, for example if a user wanted to change their bank information.

Finance
FB01 – Post Document (Outgoing payment over $10,000 requires biometric approval)

In International law a payment over $10,000 has to be reported. In this scenario we have protected an outgoing payment with biometric credentials, but only if it exceeds $10,000. It allows us to simply narrow down a selected subgroup of privileged finance team members that can issue higher amount payments. This could also be combined with a dual approval group. As per example a payment over $100,000 would require one person to request the payment with biometric credentials and a 2nd biometric user would have to reconfirm the activity.

Click on the FB01 transaction. The next screen will show an entry form to select all kind of parameters for your financial transaction. We have filled out the form – simply click the green checkmark to continue. Now you have two options. In the white field "Amount" you have the choice between $8,000 and $16,000. Select $8,000 first and press enter. The next screen shows that the payment is posted. NO biometric verification was necessary. Click the green back button and do the same with $16,000. As this amount is over our pre-defined value of $10,000 the biometric verification will be necessary. Click the green back button to go back to the main menu.

FB60 – Enter Incoming Invoices (Transaction protection only / Restricts Access to Invoices)
One of the first steps a fraudulent employee would do is to create a fake vendor using the transaction XK01 (see below). Once the fake vendor is created the user would create a purchase order, release the purchase requisition (below) and finally enter the invoice for payment. Therefore we have protected the entire transaction with PalmSecure to prevent creating fake invoices.

ME54N – Release Purchase Requisition (Transaction protection only / Restricts purchases)
This is a good example of a transaction that would allow an unauthorized user to execute an unauthorized requisition. In this example the user is releasing an unauthorized purchase requisition for 12 Fujitsu devices. We have protected the entire transaction so only authorized users can confirm the purchase of those devices. It establishes clear accountability for releases.

Materials Management

RMWB – Start Workbench (Transaction protection only / Restricts Access intellectual property)

Certain organizations own product recipes or Bills of Materials which are extremely valuable trade secrets. Loss of such Intellectual property could be extremely costly if that information were exposed to unauthorized parties. Protecting access to such information with biometrics will ensure that only authorized "eyes" will see this confidential information. Therefore the entire transaction is protected.

Sales / Distribution

S_ALR_87012180 List of customer addresses (Export of Customer list to text file protected)

There are many ways in SAP to access customer, supplier, or other lists. A few mouse clicks allow the user to export this list as a text file, save to a USB drive, or DropBox or other cloud storage and take it right to the competition. We suggest placing a biometric checkpoint into the "Save" button so that no matter what list you access in which area, as soon as the save button is executed, biometric credentials will be required to save the list. The bioLock Control and Monitoring center can specifically define which biometric template will allow executing this button. Click on the transaction and you see a customer list as well as an open menu tree (normally you have to click on "list/save/local file" but we have predefined this to make it easier). Click on "Local File" at the bottom of the menu tree. You see a screen where you could normally enter a destination location/filename (we have pre-defined that for you). Simply click Generate or Replace. Now you need to re-confirm with your biometric credentials that you are authorized to save the list to a USB Disk. Generally, this authority should always be protected with PalmSecure and narrowed down to just a few senior people in the company. Click the red X from the Windows message and the green back button to get back to the main menu. Always show what happens if you put a non-enrolled hand on the device.

XD02 – Change Customer (centrally) (View of Credit Card Information protected)

Very recently we have seen many news items about credit card fraud. Most of those are hacked and downloaded lists (we prevented these above) but we also see a lot of incidents where employees simply look at customer's credit card information to write them down. In this example we have protected the credit card button and specifically require the biometric credential of specifically invited users to view the card numbers. Click on the "XD02" transaction to get to the next screen. We have preselected "*Customer 31 / John Eberlein*". Click on the "Payment Cards" button in the center of the screen. A biometric verification is necessary to view the screen with the credit card information.

XK01 – Create vendor (Transaction protection only / Prevents creating fake vendors for fraud)

This is the number one transaction to commit fraud. The first step is to create a fake vendor in the system so the fake vendor can receive funds against a fake invoice approved by a fraudulent employee. While the entire transaction is protected we also recommend re-authentication at the final step for indisputable accountability.

VA01 – Create Sales Order (Transaction protection only / Clear accountability in sales process)

This is another sample from one of our customers who uses bioLock in a retail scenario, where hundreds of cashiers switch between hundreds of cash registers. All cashiers have biometric templates enrolled which allow them to create sales orders on all cash registers. They will be uniquely identified for accountability and their actual credentials will be matched to the sales receipt for auditing purposes. It also prevents customers from creating a sales order while the sales representative is helping another customer. It prevents the common issue of using generic passwords to access a shared cash register, which prevents accountability.

On the next page is a brief summary of the 16 transactions that are described in detail above. You can print this page as a quick reference guide that can easily be brought to a show or demo.

valantic bioLock for use with SAP ERP – powered by Fujitsu PalmSecure Simulation Demo: Functional Overview

Navigation tip: Remember to use the green check mark in the left upper corner to confirm a task and the green back arrow to go back!
On any menu item, click the button to the left of the description, not the description text. Advanced scenarios are highlighted (bold) below:

Administration

- bioLock Administration (Unprotected: allows the enrollment of customers & identification test, log file view and shows protection table) Note – once a test user is enrolled, log out and lock back in as that user!
- **SE16** – Data Browser (shows the possibility to protect SELECTED tables only, like customer lists)
  Select the unprotected LFA1 (supplier list) – then show the protected KNA1 (customer list). Explain individual table protection.
- SE38 - ABAP Editor (Transaction protection only) - Restricts Access to Source Code of SAP
- SU01 – User Maintenance (Transaction protection only) - Prevents copying of users or password resets.

Human Resources (HR)

- **PA20** – Display HR Master Data (show Info-types such as "0008 - Basic Pay" and "0009 - Bank Details")
  Select 0006 first which is unprotected, then show 0008 and 0009 which are protected. Highlight possibility to pick and choose.
- **PA30** – Maintain HR Master Data (show how SSN and birthday fields are masked for unauthorized users)
- Click green check mark and provide valid credentials to show birthday and SSN. Repeat with invalid credentials to mask data.
- PA40 - (Transaction protection only / Restricts Access to Personnel Actions)

Employee Self-Service (ESS/MSS)

- **ZCK5 –** Time and Attendance (show that an employee gets identified and recorded for work attendance in SAP)
  Click the "*Identify*" button to execute T & A functionality. Recognized user is logged as "*present*" in SAP CAT2 tables.
- PT02 – ESS Change Work Schedule (Transaction protection only) - Employee changes work shift on kiosk.

Finance

- **FB01** – Post Document (Outgoing payment over €10,000 requires biometric approval)
  Show that financial transactions over any predefined amount can be protected. In our scenario we have set a threshold value of €10,000 (customer can pick any amount). Select € 8,000 from the drop down and confirm. Amount is posted to the payment screen. Go back and select €16,000. Now the biometric verification is required because defined threshold was exceeded.
- FB60 – Enter Incoming Invoices (Transaction protection only) - Restricts access to Invoices
- ME54N – Release Purchase Requisition (Transaction protection only) - Restricts access to Releasing Purchases Requisitions)

Materials Management

- RMWB – Start Workbench (Transaction protection only) - Restricts access to Bills of Materials (BOM) , protects intellectual property)

Sales / Distribution

- **S_ALR_87012180** List of customer addresses (Export of Customer list to a USB drive or external file protected/prevented)
  Anybody that gets access to any lists in SAP can simply export them to USB by clicking on System/List/Save/Local File. For simplification we opened this menu structure for you. Click on "*local file*". The authentic window will request a file destination (which we have filled in). Click "*generate*" and explain that only specifically permitted biometric users can export/save this data.
- **XD02 – Change Customer** (centrally) (Access to Credit Card Information protected)
  Credit Card Fraud is exploding. The previous scenario prevented downloading a full credit card list. This scenario prevents unauthorized users from accessing one individual's credit card information. Click on the transaction XD02. To "fast-track" we have skipped the step to select a specific customer and go to the payment options). The payment screen opens immediately. Now click on "*payment cards*". Point out that only specifically permitted users with biometric credentials can see the credit card information.
- XK01 – Create vendor (Transaction protection only) - Prevents creating fake vendors for money laundering/fraud.
- VA01 – Create Sales Order (Transaction protection only) - Clear accountability in sales process. Useful for POS, Retail.

Review the latest trainings videos and manuals at http://www.palmsecurebiolock.com/
For questions please contact us at support@palmsecurebioLock.com

Conclusion

The valantic bioLock for use with SAP ERP – powered by Fujitsu PalmSecure simulation software is a powerful tool that allows a Fujitsu representative to quickly give a prospective customer a preview of how SAP security can be improved. Normally any demonstration involving SAP is no casual matter. This free software tool overcomes all the limitations of typical sales or demonstration situations, such as insufficient lead time, impromptu opportunities in front of a desired audience, lack of network connectivity in a trade show setting, or lack of access and/or privileges in a given SAP system. While the scenarios shown are fixed and of limited flexibility in the current version, the software is very effective in moving a prospect to the next phase in a sales cycle, namely organizing a detailed live SAP demo session. Even if you do not have a PalmSecure device present, the demo will still run although with reduced effectiveness. We encourage distribution of this software, in combination with a PalmSecure device, to all SAP customer-facing sales personnel, trade show representatives and partners, in order to maximize selling opportunities.

Appendix

About valantic:

Established in Europe over 30 years ago by former senior SAP® managers, valantic is a SAP® Software Gold Partner specializing in biometric security and identity management software systems. bioLock™ software is the only biometric software system integrated for use with SAP® and HANA. A wide variety of global corporations in many industry verticals, plus government entities are served by valantic software.

Contact
FUJITSU
E-Mail: palmsecure@ts.fujitsu.com
Website: www.fujitsu.com/palmsecure
2018-01-26