Check ID in SAP

Clear Accountability  True Compliance  Fraud Prevention

Attribute-Based Access Control (ABAC) for SAP – including biometrics

© 2020 realtime North America Inc. All Rights Reserved.
Introducing bioLock from realtime:

- realtime was founded in 1986
- Special Expertise SAP Consulting
- bioLock developed in 2001
- First certified in 2002
- SAP Gold Partner
- Installed in all Continents
- Global Partnership with Fujitsu
- Used by International Companies and Governments

Attribute-Based Access Control (ABAC) in SAP

Siemens ID Mouse with bioLock in 2002

© 2020 realtime North America Inc. All Rights Reserved.
Without Biometric ID Check You DO NOT KNOW the Actual User

Without checking ID, you never know who is the actual User

Who is...
... behind the keyboard?

© 2020 realtime North America Inc. All Rights Reserved.
Understand Your Risk

Data Doesn’t Leak Itself
Accept Your Risk

People
Leak Data!
But “I Trust All My Employees”

True: Most of your employees will never do anything to hurt your company

In most cases it is just ONE BAD PERSON that will cause the most severe damages

Fraud Prevention is deployed to protect against the ONE PERSON - not the 1000’s of good once

Fraud is REAL:

The Controller of the small City of Dixon in Illinois STOLE $53.7 Million (Link to article)

Also read – THE “TRUSTED” Employee: https://www.acfe.com/article.aspx?id=4294980868


© 2020 realtime North America Inc. All Rights Reserved.
Help to keep your Honest Employees Honest

Just because you trust your employees it doesn’t mean they should be exempt from monitoring
Do You Remember this Man?

He was the
ONE BAD PERSON
that caused damages
Edward Snowden: the whistleblower behind the NSA surveillance revelations

The 29-year-old source behind the biggest intelligence leak in the NSA’s history explains his motives, his uncertain future and why he never intended on hiding in the shadows.
What Caused the Leak – Password Security

Snowden persuaded ~25 fellow workers at the NSA regional operations center in Hawaii to give him their logins and passwords by telling them they were needed for him to do his job as a computer systems administrator.

THE NSA DETERMINED...

inadequate security measures at the NSA played a significant role in the worst breach of classified data in the super-secret eavesdropping agency’s 61-year history.
The “Overlooked” and “Ignored” Security Challenges in SAP

- People share passwords
- Hackers hack SAP User credentials
- Co-workers look over your shoulder
- Secretaries have executive passwords
- Users write passwords on sticky notes
- Administrators have access to everything
- Anybody can take over unlocked computers
- Consultants always have extended authorizations
- Ghost workers (former employees who left months ago)
- Secret accounts are created and stay undiscovered in the system
- With 1000s or SAP permission ROLES all Users are “over-permitted”
- Snowden stole over 20 passwords to share confidential information
- Home Office use is here to stay – enforcing security rules is difficult

People with bad intentions can easily “take over” other SAP User accounts and access your most sensitive SAP data

© 2020 realtime North America Inc. All Rights Reserved.
The Solution: Additional Security Checkpoints

Your SAP Systems stores and manages your organization's most vital information. When it comes to securing that information, there is always room for improvements!

Do you close the swing bar in your hotel room to keep all the employees out, who normally would have access?

What if you could set unlimited additional “Security Locks” to narrow down SAP Security?
ID Check and Re-Authentication Options

- **Fingerprint**
- **Fujitsu Palm Vein**
- **The Nymi Band**
- **CAC / Smart-Card**

**Windows 10 / HELLO**

- BioLock is compatible with a variety of biometric and other re-authentication methods inside SAP...
- Cost Effective rollout to 1000's of SAP users with Windows Hello

**Nationality**

**IP - Address**

© 2020 realtime North America Inc. All Rights Reserved.
Complimenting your existing IAM and Compliance Strategy

The Control Center establishes granular control check points, natively integrated in SAP’s ABAP code, that can not be bypassed or hacked.

* TSA (Transportation Security Administration) has authority over the security of the traveling public in the United States.
The Concept - Compared to Airport Security

Step 1 – Check ID of the Traveler

Officer checks ID and compares travelers face with the picture on the government issued document

Step 2 – Check “Allowed” or “Denied”

Officer scans ID to see if traveler is on a terrorist watch list or other no-fly lists – or on TSA PreCheck*

ONLY if the travelers ID is confirmed and traveler is NOT on the “deny list” or specifically on the “allow list”, quick access to the sensitive area will be granted.

Our technology allows you to specifically “allow” (invite) users to access protected areas in your SAP System!

*TSA PreCheck lets specifically prequalified “allowed”(invited) travelers enjoy expedited security screening
Biometric ID Check for SAP Users, Employees and Customers

LOGON Protection
All named SAP Users
- Prevent Password Sharing
- Fast User Switching
- Step Up Control

Function Protection
SAP Power Users
- Transactions
- HR Infotypes
- Tables
- Buttons
- Values

Employee Verification
All Employees (none SAP Users)
- Employee Self Service
- Time & Attendance
- Medical Checkups
- Equipment Checkout
- SAP Digital Signature

Customer Verification
Anybody
- Social Security Beneficiaries
- Bank Customers
- University Students
- Retail Customers
- Medical Patients
- Other...

ACCOUNT CONTROL
FRAUD PREVENTION
ACCOUNTABILITY
EVERYTHING (See left)

© 2020 realtime North America Inc. All Rights Reserved.
Biometric SAP Logon Protection: Prevent SAP User ID “Stealing”

**Today - using traditional solutions:**
Fraudulent users have many options to take over any SAP USER ID and Password

- Shoulder Surfing
- Written Down
- Hackers use Password Sniffer
- CAC in reader
- Backspace in Logon

Ms. Jones is attempting to logon as Mr. Smith using his password

Biometric re-authentication prevents USER ID sharing or stealing

ONLY SMITH Can logon as SMITH!

**Tomorrow – using biometrics:**

Biometric ID check identifies Ms. Jones and does NOT allow access to Mr. Smith SAP Profile

The biometric ID Check ensures that only Smith can logon as Smith and Jones can only logon as Jones

© 2020 realtime North America Inc. All Rights Reserved.
Secure and Convenient Single Sign On Logon to SAP

Single Sign On (SSO) set up via SNC on Company Network

Today, any user with physical access to Mr. Smith PC can logon as SAP User Smith via Single Sign on

Check ID to re-confirm that the user on Smith PC is actually Mr. Smith

ONLY User SMITH can logon to his SAP User Profile “Smith” using convenient and fast SSO
Transaction Protection for HIGH RISK - HIGH CONSEQUENCE Areas

We have identified 100s of Sensitive Transactions that our customers have implemented as they were identified as HIGH RISK / HIGH Consequence areas.

While this list will help you with planning, you can protect any standard and custom SAP Transaction.

While these have been key areas which are subject to fraud in SAP, you might have completely different “pain points” in your companies SAP installation:

- Log-on is important, but is JUST THE BEGINNING!
- System Admin/DDIC:
  - Data access
  - (SE16, SU01...)
  - Transport Mgr.
- Mat. Mgmt./Logistics:
  - Inventory movement
  - Manufacturing / BOM
- SAP users in all industry verticals experience serious security challenges.

© 2020 realtime North America Inc. All Rights Reserved.
Function Protection Examples: Infotypes, Tables, Values, Buttons

ANY Standard or Custom SAP Transaction

- **Favorites**
  - Finance
    - FCC1 - Payment Cards: Settlement
    - FB60 - Enter Incoming Invoices
    - ZS_ALR_87012284 - View Balance Sheet
    - FB01 - Vendor Invoice / GL Account OVER $10K
    - F-53 - Post Outgoing Payments OVER $10K
    - ME29N - Release purchase order
    - Z_ME52N - change a purchase order
    - Z_ME54N - Release Purchase Order Receipt

- **HR Examples**
  - PA20 - Display HR Master Data
  - PA30 - Maintain HR Master Data

- **System Maintenance**
  - STMS - Transport Management System
  - SU01 - User Maintenance Initial Screen
  - SE16N - General Table Display
  - SE38 - ABAP Editor

- **Sales & Distribution**
  - Z_VA01 - Create a Sales Order
  - Z_VS03 - Display Scale (calculate shipping)

Any HR Infotype

- **Infotypes**
  - 0006 - Address
  - 0008 - Basic Pay
  - 0009 - Bank Details

Selected Tables

- **Data Browser: Initial Screen**
  - table name
  - LFA1
  - KNA1

Execution / Enter Button

- **Save/Print/Export Data “Button”**

High Value Transactions

- **Enter Payment Posting: Add G/L account**
  - G/L Account: 191102
  - GR/IR: Goods and services not invoiced
  - Company Code: 0001 SAP A.G.
  - Item 1: Debit entry / 40
  - Amount: 12345.67

- **Data Browser: Classified NSA Documents**
  - File Name: Snowdonia_Classified_NSA_Data

- **Confidential**

ANYTHING IN ABAP!

SAP’s Internal Programming Language

CHECK ID for ANY Function or any “Click in SAP”!

© 2020 realtime North America Inc. All Rights Reserved.
Masking or “Hiding” Fields

Let the Biometric ID Check decided who can see sensitive parts or fields of any screen

This could be a Functional Location or Functional Equipment in a PM Notification
Prevent Unauthorized Export of Sensitive Data

Exporting a confidential list with 5 mouse clicks...

NOTHING STOPPED Snowden from clicking the save / “Generate Button”
Biometric Technology to Stop another “Snowden Data Breach”

A biometric “checkpoint” configured in the Generate / Save Button would have prevented the Snowden Data Breach and other breaches.
Test Drive the Data Breach Scenarios in our Simulator:

Start the Simulation in a Web browser:

- Click Continue
- Start Simulation
- Prevent Export of Tables Via USB Flash Drive
- Mask or Hide Fields
- Etc...

https://www.realtimenorthamerica.com/biolocksimulation/20/

© 2020 realtime North America Inc. All Rights Reserved.
Extensive Function Protection Administration Settings

Extensive Customization Overview

Configuration of Function Protection

User Master Data with Remote Enrollment

Invite Selected Users

© 2020 realtime North America Inc. All Rights Reserved.
Configure a Transaction Protection in 3 Simple Steps (1Minute)

**Step 1:**
Pick any SAP Transaction that needs a restricted access. Select your preferred restriction criteria. Palm Vein or Fingerprint is highly recommended. Enable global protection and assign a free (random) defined Function number.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description of System Function</th>
<th>Inspect.F.</th>
<th>Glob.Check</th>
<th>Invitation only</th>
</tr>
</thead>
<tbody>
<tr>
<td>470</td>
<td>F110 Automatic Payment Transactions: Status</td>
<td>Nymi Band - NFC reader</td>
<td>✔</td>
<td>Invite Defined</td>
</tr>
</tbody>
</table>

Protect multiple Transactions in each step which allows protection to dozens of transactions within minutes!

**Step 2:**
Enter the transaction code into the table and assign it to the previously defined Function Number associated with the protection criteria.

<table>
<thead>
<tr>
<th>Transaction code</th>
<th>Transaction Text</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>F110</td>
<td>Parameters for Automatic Payment</td>
<td>470</td>
</tr>
<tr>
<td>FB60</td>
<td>Enter Invoicing</td>
<td>120</td>
</tr>
<tr>
<td>FB25</td>
<td>Print Check for Payment Document</td>
<td>122</td>
</tr>
<tr>
<td>FK02</td>
<td>Change Vendor (Accounting)</td>
<td>445</td>
</tr>
<tr>
<td>LT01</td>
<td>Create Transfer Order</td>
<td>662</td>
</tr>
</tbody>
</table>

**Step 3:**
Enforce “least privileged access” by specifically inviting “allowed”, biometric privileged, users to access Function 470.

GURANTEED: ONLY SMITH can access F110 NOW!

<table>
<thead>
<tr>
<th>Invited bioLock users for global check</th>
<th>Description of System Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>430 MILLER</td>
<td>ME52N - Change Purchase Requisition</td>
</tr>
<tr>
<td>432 MILLER</td>
<td>ME54N - Release Purchase Requisition</td>
</tr>
<tr>
<td>440 SMITH</td>
<td>M801 - Post Good Receipt for PO</td>
</tr>
<tr>
<td>470 SMITH</td>
<td>F110 Automatic Payment Transactions: Status</td>
</tr>
<tr>
<td>51 SMITH</td>
<td>Release Blocked Invoice</td>
</tr>
</tbody>
</table>

© 2020 realtime North America Inc. All Rights Reserved.
Protect Functions Like Outgoing Payments on a Nano Level

While some customers prefer to protect just the access to the F110 transaction, others configure the ID CHECK for the execution of the PAYMENT RUN on the function level for ultimate protection and accountability.

An ABAP Programmer will add a “checkpoint” via ABAP Code and link it to the function number 471 which is configured in the software.

The log file shows Thomas Smith executed the Payment Run at 17:29 on October 16th for clear accountability.

Re-Enforce Segregation of Duties with Biometrics

Many times the same employee has the capability to execute conflicting business processes.

Employee 1 creates a Purchase Order

Employee 2 approves Purchase Order

Employee 3 issues a $250,000 Payment

Use biometrics to guarantee a true Segregation of Conflicting Duties.


© 2020 realtime North America Inc. All Rights Reserved.
Reduce Corruption and Collusion with Dual Controls

2 or more users need to confirm sensitive or high-value transactions to prevent corruption and collusion.

After a first authorized user has requested the function, a 2nd authorized user must re-confirm the request on the same PC. Both users will be uniquely identified and logged in the log file for accountability.
Often Convenience is Chosen over Security

For 20 Years the Nuclear Launch Code at US Minuteman Silos Was 00000000

The codes, known as Permissive Action Links (PALs), were supposed to prevent the use of nuclear weapons without the authorization of the president of the United States.

All PAL codes were reset to 00000000 to ensure that the missiles were ready for use regardless of whether the president was available to give authorization.


© 2020 realtime North America Inc. All Rights Reserved.
Increase Security and Convenience to Sensitive Approvals

With the increasing pressure from International Compliance Regulations like GDPR, SOX, etc. many employees are required to execute SAP Digital Signature on an increasing basis, resulting in a massive productivity loss and inconvenience for employees.

Reduce the Digital Signature Processing Time from 10 to 15 Seconds to Just 1 Second

Click on the biometric icon and provide a biometric credential instead of typing the information. Alternatively, trigger the process automatically if a biometric device is recognized.
What Happens when a Protected Function is Triggered?

Step 1
User requests SAP Function

User requests SAP function. e.g. Log-on, Customer Service activity, etc. Check SAP server for credentials.

Step 2
User Provides Requested Credential

bioLock prompts a user for a re-authentication

Sample biometric template is extracted, encrypted, and compared with reference template in bioLock/SAP

Step 3 User’s request is accepted or denied

Activity Allowed

Activity Denied

© 2020 realtime North America Inc. All Rights Reserved.
There is NO Training Required for the Users

Note that there is no change for the user! The SAP transaction is entered as always.

Without Biometrics
Everybody with authorized or unauthorized “access” can issue a payment via F110

With Biometrics
Only specifically invited (biometric privileged) users – like Smith – can issue a payment via F110

NO USER TRAINING REQUIRED – just show your hand or put your finger on the fingerprint reader...

If a transaction or any SAP function that is restricted by bioLock is detected, biometric re-authentication will be required.

ALL OTHER users that are not specifically invited with biometric credentials will ALWAYS be rejected: Colleague Jones, Consultants, SAP Support, Admins, DDIC, Secretaries, Coworkers, Snowden, Interns, Ghost Workers, Hackers, Spouse etc.
The Clear Difference Offered by Granular ID Check

Without Biometrics
Many Unauthorized and Unknown Users can theoretically access ANY sensitive SAP Function

With Biometrics
Only SMITH who is specifically invited via the bioLock “Allow List” can access the SAP Function

Using Biometrics is an additional SAP Policy Enforcer for Attribute-Based Access Control (ABAC)

© 2020 realtime North America Inc. All Rights Reserved.
Clear Accountability in Log File for Auditors / Security Teams

<table>
<thead>
<tr>
<th>Date</th>
<th>User Name</th>
<th>bioLK User</th>
<th>First name</th>
<th>Last name</th>
<th>N Text</th>
<th>Func</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.10.2019</td>
<td>SMITH</td>
<td>SMITH</td>
<td>Thomas</td>
<td>Smith</td>
<td>was accepted</td>
<td>471</td>
<td>Execute Payment Run - F110 Automated</td>
</tr>
<tr>
<td>16.10.2019</td>
<td>SMITH</td>
<td>JOHNR</td>
<td>John</td>
<td>Renner</td>
<td>not authorized*</td>
<td>471</td>
<td>Execute Payment Run - F110 Automated</td>
</tr>
<tr>
<td>16.10.2019</td>
<td>JONES</td>
<td>JONES</td>
<td>Amanda</td>
<td>Jones</td>
<td>not authorized</td>
<td>471</td>
<td>Execute Payment Run - F110 Automated</td>
</tr>
<tr>
<td>16.10.2019</td>
<td>MATHIAS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.10.2019</td>
<td>DDIC</td>
<td>BONGANI</td>
<td>Bongani</td>
<td>Magwebu</td>
<td>was rejected</td>
<td>470</td>
<td>F110 Automatic Payment Transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>not authorized*</td>
<td>471</td>
<td>Execute Payment Run - F110 Automated</td>
</tr>
</tbody>
</table>

1. Smith is the only person accepted to execute a Payment Run
2. John Renner is not authorized - even he is logged in as SAP User Smith*
3. Amanda Jones not authorized – even she has full SAP access to F110
4. Hacker accesses Finance Director Mathias SAP User – is still rejected
5. External Consultant Bongani (Logged in as DDIC/Admin) – Still NOT authorized*

* Note: Windows Hello does not support 1:N Identification and can not identify “not authorized” users in the log file.
User Cases: Employee and Customer Identification in SAP

Employee Identification at Transnet, South Africa

Customer Identification at the National Social Security Administration (NSSA) in Zimbabwe

Biometrics prevents social security fraud for 100s of Thousands of Social Security Beneficiaries in Zimbabwe:

- Enrolled beneficiaries with bioLock directly inside the SAP System
- Card and biometrics is required to receive benefits
- Only uniquely identified Beneficiaries can receive benefits
- Double Dipping is prevented
- Payouts were reduced significantly

Download Case Study

Card + Biometrics to uniquely identify 100s of Thousands of Customers

Manufacturing success story nominated for Fujitsu best product award:

Transnet using kiosks with build in Palm Vein Scanners connecting the shop floor employees to SAP for Plant Maintenance: https://youtu.be/quE3rs-nlrl

© 2020 realtime North America Inc. All Rights Reserved.
Some bioLock Customers – Click to Download Case Studies

Energy Company, Bahrain
Banking in London, UK
School District, Florida
Retail in Germany
Transportation in Africa
Workflow Protection
HR Requests
Perimeter Access
Vendor Payment
Public Sector
Connecticut, US
Namibia
Mexico City
Johannesburg
Zimbabwe

Download all PDF Documents as ZIP

© 2020 realtime North America Inc. All Rights Reserved.
How the “Snowden Data Breach” Could Have been Prevented

- Check ID in SAP for employees, vendors or customers
- Set unlimited Security Checkpoints in SAP
- Protect any Standard or Custom Transaction
- Secure any Function, Value, Buttons, and more
- Only allow access after a confirmed ID check
- Use Fingerprint, Palm Vein, Nymi Band, and Smart Cards
- Windows10/Hello enables bioLock without extra hardware
- Specifically “Allow” users and narrow down SAP Security
- Create Clear Accountability and Controls with Log Files
- Control the weakest link in security – the Human Being
- Establish True Compliance by re-enforcing SoD’s
- Prevent another Snowden Data Breach

bioLock is the Policy Enforcer for Attribute-Based Access Control (ABAC) in SAP including biometrics

© 2020 realtime North America Inc. All Rights Reserved.
Learn More about bioLock and Granular Controls in SAP

View Videos in our realtime YouTube Channel

Two easy ways to share a technology overview with other Team Members:

View Videos in our dedicated Fujitsu Palm Vein YouTube Channel

Manufacturing Kiosk

See Customer Presentations, Live Demos, Technical Presentations and more (YouTube)

Test Drive bioLock via Online Simulation

Easy 5 Scenario Overview for a quick Test Drive: www.biolocksimulation.com
Advanced 20 Scenario Detailed Test Drive: www.biolocksimulation.com/20

This Professional Fujitsu Video shows how Transnet Africa uses Palm Vein Kiosks and bioLock to connect their unconnected workers with SAP (YouTube)

Educational Online “Teaser” Overview

www.CheckIDinSAP.com

© 2020 realtime North America Inc. All Rights Reserved.
Contact us for an Informal Online Presentation and Demo

Contact us for more information, an on-line presentation / demo, or a pilot installation.

Thomas Neudenberger
+1-813-283-0070
www.bioLock.us
Thomas@biolock.us
www.linkedin.com/in/neudenberger

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited. SAP and its logos are trademarks or registered trademarks of SAP AG in Germany and in other countries. PalmSecure is a trademark of Fujitsu Limited. bioLock is a trademark of realtime. All other trademarks mentioned herein are the property of their respective owners. We would also like to thank the ACFE (The Association of Certified Fraud Examiners) for proving the detailed fraud reports and statistics.

© 2020 realtime North America Inc. All Rights Reserved.