



# bioLock



## Biometric Fraud Mitigation for SAP®

### PRODUCTS & SERVICES

### bioLock expands the scope and justification for biometrics from simple password replacement to Fraud Mitigation...

- Protect SAP Access, Transactions, Fields or Infotypes to the Data Level
- Uniquely identify actual users independent from the SAP User Profile
- Accept or reject request based on biometrics and log any activity
- Compatible with leading biometric devices / biometric laptops

### bioLock will address many of your Security Challenges:

bioLock is the first SAP certified biometric identity management system that has a 3-level security protection: Level I - SAP Logon, Level II - Transactions, Level III – Field and Data. bioLock will uniquely identify the “actual user” independent from the SAP User Profile and log all critical activities. Sarbanes-Oxley Section 404 requires that companies develop strong internal controls to detect and mitigate fraud. With insecure, outdated passwords, fraud detection and obviously no fraud mitigation can be accomplished. Learn more at: [www.fraudmitigation.com](http://www.fraudmitigation.com). bioLock offers Internal Control and Audit departments not only the ability to prevent unauthorized access on all levels, but also to prove who did what and when within the mySAP ERP System.



Imagine your company’s research data or critical production data can be protected with biometrics and be ensured that only authorized trusted users can access or even change data. In addition, a detailed log file will clearly show which person accessed any transaction or which person was denied trying to execute a protected function. This comes in especially handy, when multiple authorized users are using one computer. See our Warehouse Case Study for more details on “Fast User Switching”. No more sleepless nights about those administrators – or anybody using the administrator’s passwords - being able to access anything within the company.

In HR, certain information like social security numbers, salaries or health insurance details are always being compromised and lead to bad publicity and lawsuits. In Finance, it is important to verify who did access the company balance sheet or who made a million dollar wire transfer to a Swiss bank account. With 20 ways to get a password for any SAP User profile, traditional access controls do not keep up with the new challenges of data trafficking. Using biometrics will not only uniquely identify a user but could require two different individuals to authorize critical tasks making it the “ultimate” and only “true” electronic signature!

### SAP about bioLock:

*“Data security and access controls will be on top of everybody’s list for the year 2006,” said James Alfano, Director for IT Security, SAP. “Together with realtime’s bioLock, SAP can offer one of the most advanced solutions in the market”.*

*(Quote from realtime’s NetWeaver Certification Press Release Jan. 06)*

- Restrict and protect access better
- Clearly identify the actual user
- Log all activities for audits (SOX)
- Fraud Mitigation
- Fast User Switching
- Accountability

It is often the work of an employee within the enterprise that causes the most damage (Richard Mogul Gartner)

Average damage last year:

First Single Incident:  
\$159,000

Every Forth Incident:  
\$ 1 Million +

9 Reported Incidents:  
\$ 1 Billion +

(Source: 2006 Study ACFE)



bioLock is SAP-certified and NetWeaver certified SAP presented bioLock at multiple SAPHIRE's. The solution is displayed in the Global Solution Center realtime is a member of SAP's Industry Value Network



[www.bioLock.us](http://www.bioLock.us) 1-877-bioLock

Innovative - Inexpensive  
Convenient - Safe



Kenneth D. "Pete" Gunn, Director,  
Safety & Security, Homeland Security  
Coordinator, Florida Space Authority

## PRODUCTS & SERVICES

### bioLock redefines the Security Approach with Innovative Technology:

bioLock sits on top of the existing SAP Security adding an additional Layer of Security. With bioLock you can basically protect every "mouse click" in the SAP System independent from the SAP User Profile. Now you don't have to worry about protecting the access to all your 1000's of corporate wide SAP Users. You define which transactions, functions or tasks (like financial, HR, production, research, purchasing) are critical within your organization and you define how many people should have access to those critical tasks that we would protect with biometrics. Depending on the nature of the organization, companies end up protecting a few 100 to a few 1000 users with biometrics – not the entire company - since all other internal or external intruders would not be able to access biometric protected tasks anyway.

If the corporate balance sheet is protected with biometrics and only the CFO has access to it based on his biometric template, no other individual would be able to access the balance sheet, even if they get a hold of the administrator password and log in as SAP ALL (SAP\*).

It is possible to assign certain biometric templates to other SAP Users. For example the biometric template of the executive secretary Mary could be assign to the CEO's SAP User, Joe. Now she can still work with the SAP User "Joe", but if critical financial data would be changed under Joe's SAP user profile, Mary would still be uniquely identified and it could be proven that it was Mary, who did the changes. This functionality comes in especially handy, when multiple users use one computer and it is not convenient for every person to log out and back into the SAP system (Fast User Switching). You want to ensure that only authorized administrators will be able to log in as SAP All – all others will be rejected.

Our dual confirmation group allows us to protect highly sensitive tasks with two or more people (two signatures on a check). Now two individuals could be required to execute a wire transfer. The finance person has to request the wire transfer with biometrics and the supervisor will confirm. The log file clearly shows who requested and who confirmed the task. Everything can be confirmed via biometrics or Smart Cards or with a combination of both, offering the ultimate dual authentication down to the execution level. bioLock is compatible with smart card standards of the U.S. Government and most existing hardware.

All activities that are protected with bioLock, will be recorded in the SAP Log file (for 3<sup>rd</sup> party analysis tools) and realtime's own log file with all relevant data. realtime's log file can be sorted by users or activities and stored in different formats or emailed to the auditors. There are no more excuses: "It was not me!" bioLock eliminates outdated passwords, enhances security and convenience while enabling clear monitoring and auditing. bioLock also reduces unnecessary password administration cost and saves the user costly time.

The bioLock software is installed and configured in hours. Protection of transactions, and the registration of bioLock users take minutes. Actual use is intuitive and requires no training. The software is installed within SAP in its own reserved name space and does not change your SAP configuration. It runs on SAP 4.6, 4.7 and higher. Leasing is available.

The bioLock technology is installed at Universities, Financial Institutions, Oil Companies, Utility Companies, Manufacturing Facilities and Government Organizations around the world. SAP TV mentioned bioLock in a movie about Sarbanes-Oxley and made a dedicated bioLock movie about our award winning installation at Brevard County Government. These movies can be viewed at URL: [www.bioLock.us](http://www.bioLock.us) (select Movies in the Info Center to the left)

*"When I first saw this innovative technology, I thought: This is something we absolutely need here in the State of Florida to improve our Homeland Security. I personally introduced realtime to Brevard County Government, and I hope that the successful installation at Brevard will inspire more government and private organizations across the nation to protect their vulnerable IT systems with innovative biometric technology."*

82% of all passwords  
are written down  
(Source: SAP Info)

40% say they share  
passwords frequently!  
(Source: Rainbow)

24% Internal Security  
breaches using somebody  
else's accounts or permissions  
(Source: InfoWorld)

70% of unauthorized  
access to IT systems is  
done by employees  
(Source: Gartner)

95% result in significant  
financial losses  
(Source: Gartner)

Call us to schedule an educational  
online presentation for your team!



realtime North America Inc.  
World Trade Center  
Tel: +1-813-283-0070  
Fax: +1-813-283-0071  
Info@biolock.us

