



This photo was taken by Adventier consultant Luke Finsaas during his adventure along the Gulf of Nicoya.

ESTABLISH INDISPUTABLE ACCOUNTABILITY

FRAUD PREVENTION, DATA PROTECTION

PROBLEM

News of financial fraud is in the headlines daily. Unfortunately, the majority of it is committed by insiders. Occupational fraud accounts for an average loss of 7% of revenue (approximately \$994 billion in total) for U.S. organizations (ACFE 2008). So how do you prevent fraud from costing your company?

REDEFINE THE SECURITY APPROACH

The first step to ensure your company is protected against fraud is to secure your sensitive data. With our partner, realtime, we offer the most effective fraud prevention tool: *bioLock*. With *bioLock*, SAP customers can control access to critical functions, sensitive data and transactions to prevent fraud through the advanced technology of biometrics.

PROCESS

The *bioLock* tool sits on top of your existing SAP Security and adds an additional layer of protection. It protects SAP access, transactions, fields and infotypes at the data level, uniquely identifies the users independently from the SAP user profiles, and accepts and rejects requests based on biometrics and logs activities.

Users conduct and confirm critical activities by swiping or touching their finger to a device that uses new biometric technology, which measures electrostatic capacity, subskin texture, and blood stream to biologically confirm the user's identity. *bioLock* records the actual user and type of transaction made by or functions denied to the actual user in SAP's and realtime's log files.

FACT DATA

- 64% of all passwords are written down Rainbow 2003
- 33% of corporate users share their passwords with others Global 2003
- 70% of people approached at a security tradeshow gave up their password for a candy bar BBC 2004
- 44% of network abuse is done by employees CSI 2008
- 52% of insider threats were found to be predominantly accidental by organizations surveyed IDC 2009
- Smart cards and tokens can be lost, stolen, copied, borrowed or passed on to another person. There is no proof that the actual user was the authorized user.

FRAUD PREVENTION, DATA PROTECTION (CONT.)

REAL LIFE SCENARIOS

Scenario 1 realtime 2009

A director used one of his employee's user profiles and passwords to commit fraud in the SAP financial system. When the fraud was discovered, the employee spent half a year in jail for a crime that she did not commit. Eventually, the director was arrested for stealing her password and committing the fraud.

Scenario 2 IDGNS 2008

Inadequate IT security allowed a trader at French bank, Societe Generale, to make a series of unauthorized transactions that ultimately cost the bank \$7.2 billion.

Scenario 3 CNET 2006

In May 2006, personal records from about 26.5 million veterans were stolen from the Department of Veterans Affairs (VA). The Veterans Groups sued the VA, seeking up to \$26.5 billion in damages.

Scenario 4 FOX 2006

An administrative assistant at Coke stole formula trade secrets from the company and attempted to sell them to Pepsi for \$1.5 million. Pepsi contacted Coke immediately, and FBI authorities arrested the former Coke employee.

BENEFITS

- Adds layer of security to your SAP system
- Protects companies from risk of million dollar losses
- Implemented and running in a few days
- Requires minimal training, configuration or maintenance
- Protects SAP access, transactions, fields and infotypes at data level
- Uniquely identifies users independently from SAP user profiles
- Accepts and rejects requests based on biometrics and logs activities
- Compatible with leading biometric devices and biometric laptops
- Has immediate ROI in first year and very low TCO
- Is the only certified biometric technology available for SAP

BioLock also provides a Level-V Security Protection, which is the first SAP certified biometric protection.

Level I: SAP Logon

Level II: Transactions

Level III: Fields and Infotypes

Level IV: Field Values

Level V: Dual Confirmation (2 signatures on a check)

TECHNICAL CHALLENGE	BIOLOCK
Outdated access control methods do not adequately protect information. Extensive password sharing allows fraudulent actions without accountability.	<i>bioLock</i> expands justification for biometrics from simple password replacement to Fraud Mitigation.
No solution for fast user switching (multiple people using 1 computer)	Fast User Switching Mechanism
No technology in place to protect critical functions or actual data	Critical transactions require additional re-authentication with biometric credentials
SAP only identifies SAP user profile, not actual user	Logon to selected SAP User Profiles requires biometric authentication
No way to prove in log file who actually used SAP profile	Log file proves actual user executed critical function or task
No way to prevent users from transferring excessive funds or creating unauthorized PO's	Dual confirmation group can require two individuals to authenticate (true SoD)
Gaps in security roles tend to "over permit" users to execute too many critical functions	<i>bioLock</i> increases security, accountability, and productivity and is easy to use!