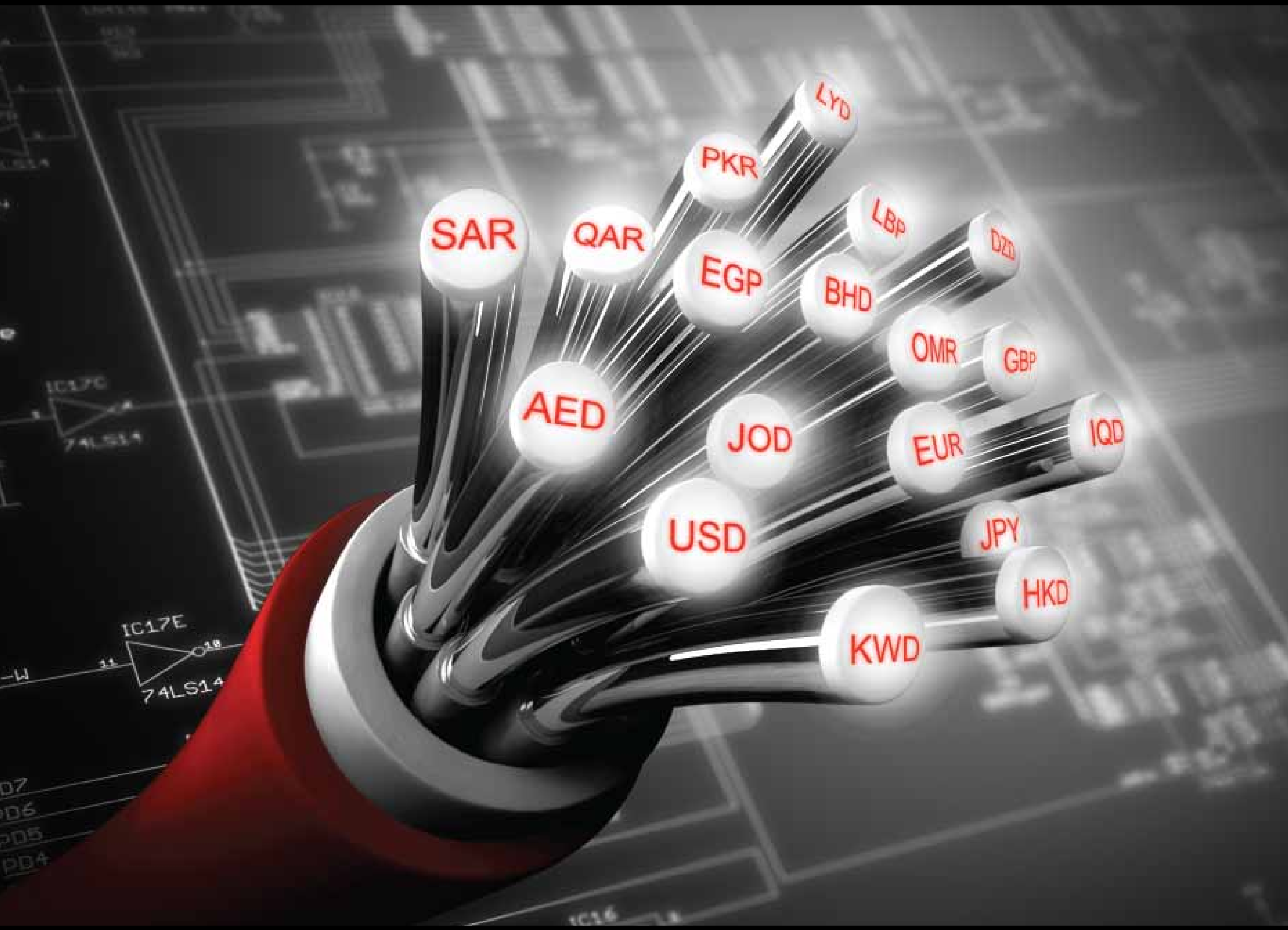
HSBC's Guide to Cash, Supply Chain and Treasury Management in the Middle East 2009



SABB ساب

HSBC

Treasury Considerations

A Security Profiling Model for Cash Management

Amit Lohani, Consultant, Banking and Capital Markets, Infosys Technologies, and Rajat Tyagi, Principal, Banking and Capital Markets, Infosys Consulting, India

- Over the years, companies have moved from manual to electronic processing and have started using the Internet for exchanging data with their banks, customers and suppliers.
- With the growing sophistication of identity theft, a more careful approach is required to structure access profiles that authenticate and allow entitled users access to their data.
- A clear and detailed understanding of treasury operations such as reconciliation, forecasting and positioning will help service providers to create meaningful security profiles.
- A security profiling model can be a foundation for a bank to build a strong cash management service for companies as well as a robust product feature to attract more customers.

Cash management services offered by banks form a core part of a company's treasury operations. Since cash management involves the transfer of money and related information, security is of vital importance. Over the years, companies have moved from manual to electronic processing, automated various systems and have started using the Internet for exchanging data with their banks, customers and suppliers. At the same time, newer encryption and security technologies have become almost impossible to break. But cash management systems still lack technologies that can allow users access to data on a structured need-to-know basis.

With the growing sophistication of identity theft by fraudsters, along with "phishing" and spyware, a more careful approach is required to structure access profiles that authenticate and allow entitled users access to their data. This article looks at key security challenges and how creating a security profiling model can enhance a bank's cash management services.

Why Security Profiling is Important

Security profiles control access to organisations and employee or applicant records within a business group. System administrators use these profiles when defining users' responsibilities. Various international banking and technology regulators have provided guidelines for security profiling.

For instance, a guideline for e-banking from the Bank of International Settlements states that "banks should establish appropriate authorisation privileges and authentication measures, logical and physical access controls, adequate infrastructure security to maintain appropriate boundaries and restrictions on both internal and external user activities, data integrity of transactions, records and information, and the existence of clear audit trails for all e-banking transactions".

Similarly, Payment Cards Industry Data Security Standards lays down the following three guidelines for strong access control measures:

- Restrict access to user data by business need-to-know basis;
- Assign a unique ID to each person with computer access to data; and
- Restrict physical access to user data.

Despite these guidelines and various security measures in cash management businesses, banks are still losing millions of dollars through unauthorised access and fraud in cash management services. Regions like the Middle East are more susceptible as rapid growth in corporate business has outpaced the regulatory and security guidelines and controls in place for banking.

Security Challenges

The security challenges in cash management are not new to banks and financial institutions. Over the years, banks faced multiple security risks and various providers proposed solutions to mitigate such risks. When a new challenge was encountered, different solutions came from vendors to overcome the particular problem.

In the last few years, centralisation of a company's treasury has been successful in standardising operating procedures and in achieving significant cost benefits for many companies. In addition, regulatory requirements such as the Sarbanes-Oxley Act 2002 (which sets standards relating to the regulation of financial practice and corporate governance) have promoted interest in centralised operations. But, with centralisation, the need to have different levels of access to information for different users becomes even more important.

Similarly, user authentication has to evolve from a simple binary operation to a more linear one. Instead of authentication being a simple binary result of the user being authenticated or not, cash management systems need to get additional authentication information before a user can access more secure data. Also, if the user tries to authorise a transaction of a higher amount or a higher volume of data, the application should support a complex authorisation matrix (like ones based on a company's internal signing authorities). These require the setting up of a more complex profiling framework.

Auditors and security officers also expect a centralised view for the security policy of all of cash management services and systems. The management of security policies has ceased to be the responsibility of information technology (IT) professionals and instead comes under the domain of business administrators – requiring profiling policies to be presented in a business-user context.

This means that profiling logic previously embedded within each application must now be taken out of that code and put into some sort of logical container for administration and audit purposes.

A Cash Management Security Model

Banks have developed comprehensive physical security systems to protect their physical assets. Similarly, they have electronic security systems to protect their IT assets. A cash management security model should not only look at securing information from unauthorised access but also ensure that legitimate users have access when needed. For instance, at a high level information could be structured for access in three groups:

- Customer data that is available to all – customers, external parties and bank users (data such as customer account and settlement instructions to enable its customers and suppliers to access a customer's account);
- Customer data that is available to specific customers and bank users (such as customers' transaction details); and
- Data that is *not* available to the customer but is available to bank users (such as customer compliance and money-laundering alerts and risk-profiling).

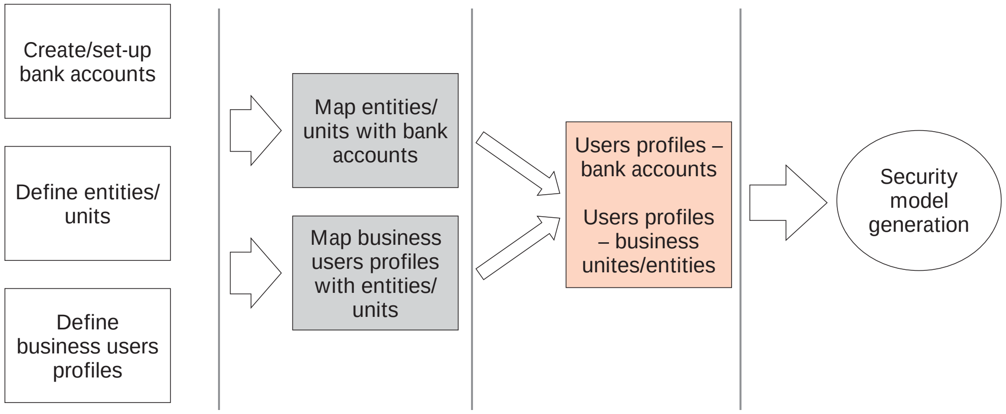
Once banks start thinking about their high-level needs, a framework defining the users and entities can be formed. These entities can be business units, functions or any user-defined group.

The simple way is to define various lines of business units, creating bank accounts for those units and, finally, providing users access to those accounts. Hence the mapping is between users and accounts.

The other way can be defining user profiles and providing access to functions, i.e. the set of actions or operations that can be performed by a user in any line of business. This method can map users directly with functions. For a complex situation, the mapping can be a user to multiple functions of different units. This all depends on how the bank or company wants to set the user profiles based on its requirements.

The situation becomes more complex when a single bank account is accessed by multiple entities, and banks want to have one set of actions for one user while a different set of actions for another one.

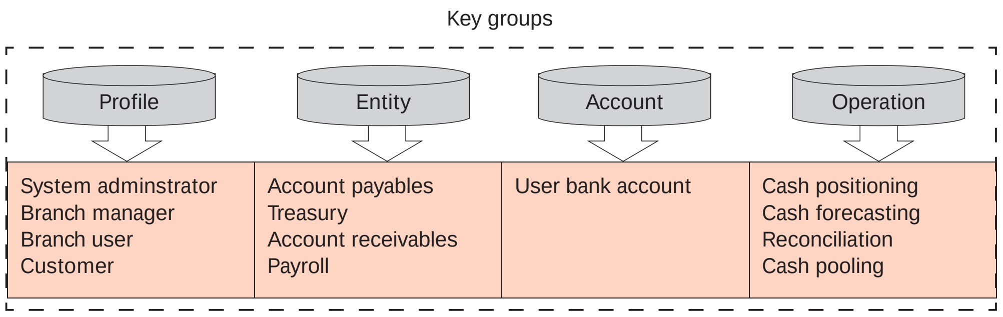
FIGURE 1: Security Model Set-up Process


Create/set-up bank accounts
Define entities/ units
Define business users profiles
Map entities/ units with bank accounts
Map business users profiles with entities/ units
Users profiles – bank accounts
Users profiles – business unites/entities
Security model generation

Source: Infosys

A robust solution can be formed by defining the profiles and mapping them to various business units or entities, and, at the same time, mapping the customer accounts with business units or entities. The access can be provided only if the user profile is defined in both mappings. This will be a two-way security feature and will not allow unauthorised users to access the secured data.

FIGURE 2: Key Groups in Security Profiling

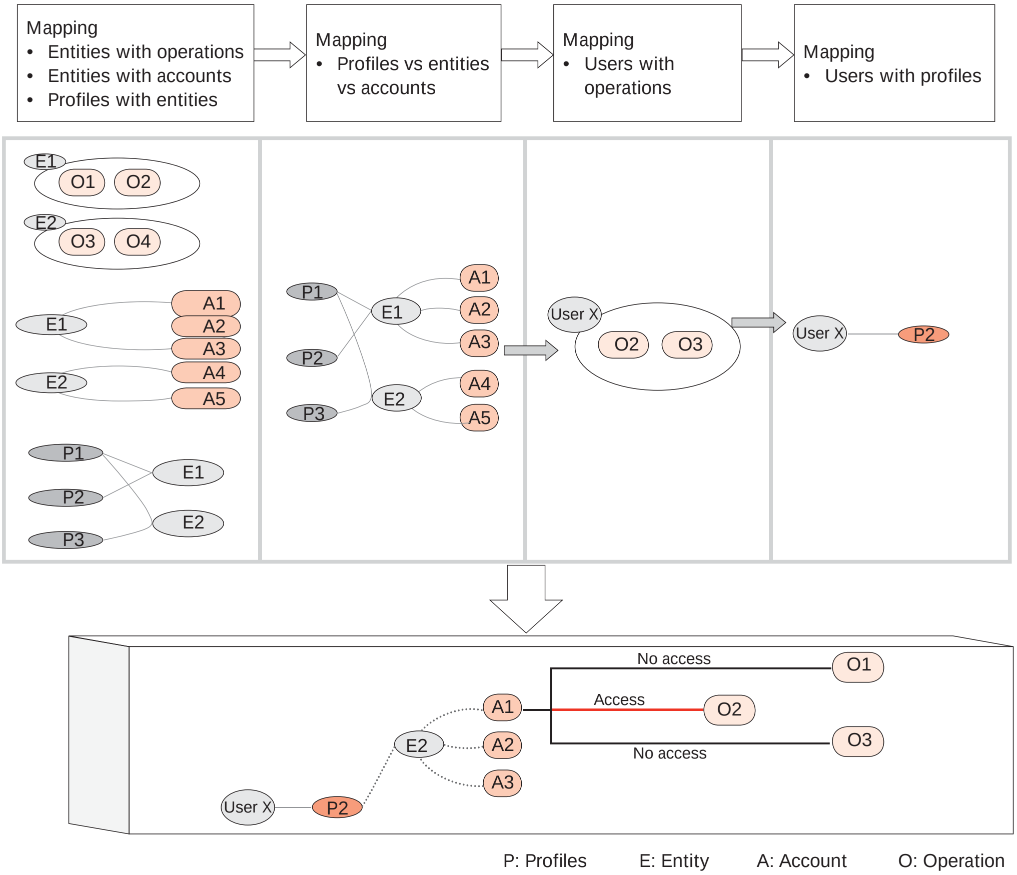


Profile	Entity	Account	Operation
System adminstrator Branch manager Branch user Customer	Account payables Treasury Account receivables Payroll	User bank account	Cash positioning Cash forecasting Reconciliation Cash pooling

Source: Infosys

To access account details, a user must have access to the entity or business function pertaining to that account. Once this is defined, access rules can be created by mapping the bank accounts with the user profiles. The accounts within a cash management system can be used for various operations, such as payables, receivables and payroll. The security model can be used to specify which account of the entity can be used for these operations. This can help companies to put controls in place and improve security.

FIGURE 3: Security Profiling Set-Up Process



Source: Infosys

Conclusion

A clear and detailed understanding of treasury operations such as reconciliation, forecasting and positioning will help service providers to create meaningful security profiles. Banks need a framework that provides flexibility and a comprehensive approach to accessing secure cash management services. Such a framework is possible through a matrix of profiles, entities, accounts and operations. The security profiling model suggested can be a foundation on which to build a strong cash management service for companies, especially for large global corporates in the Middle East. Most of the bank clearing systems in the region are currently operated manually. Though local banks in Middle East countries have yet to achieve a robust cash management system, the lack of automated systems and the high volume of transactions are forcing banks to automate their settlement systems. Security profiling considerations will provide key inputs to achieve this goal.

References:
"Risk Management Principles for Electronic Banking", Bank of International Settlements, July 2003.
Payments Card Industry Data Security Standards, www.pcisecuritystandards.org/security_standards/pci_dss.shtml.
"Service-Oriented Security: An Application-Centric Look at Identity Management", Oracle white paper, April 2008.
Oracle Human Resource Management Systems glossary, see download.oracle.com/docs/cd/A60725_05/html/comnls/us/per/gls.htm.

Integrated Receivables Solutions

fast forward your receivables

Euromoney Cash Management Customer Poll
Best Domestic Cash Manager in United Arab Emirates, Saudi Arabia, Qatar, Bahrain, Jordan, Kuwait and Lebanon (2008)
Best Cash Management Bank in the Middle East (2005-2007)

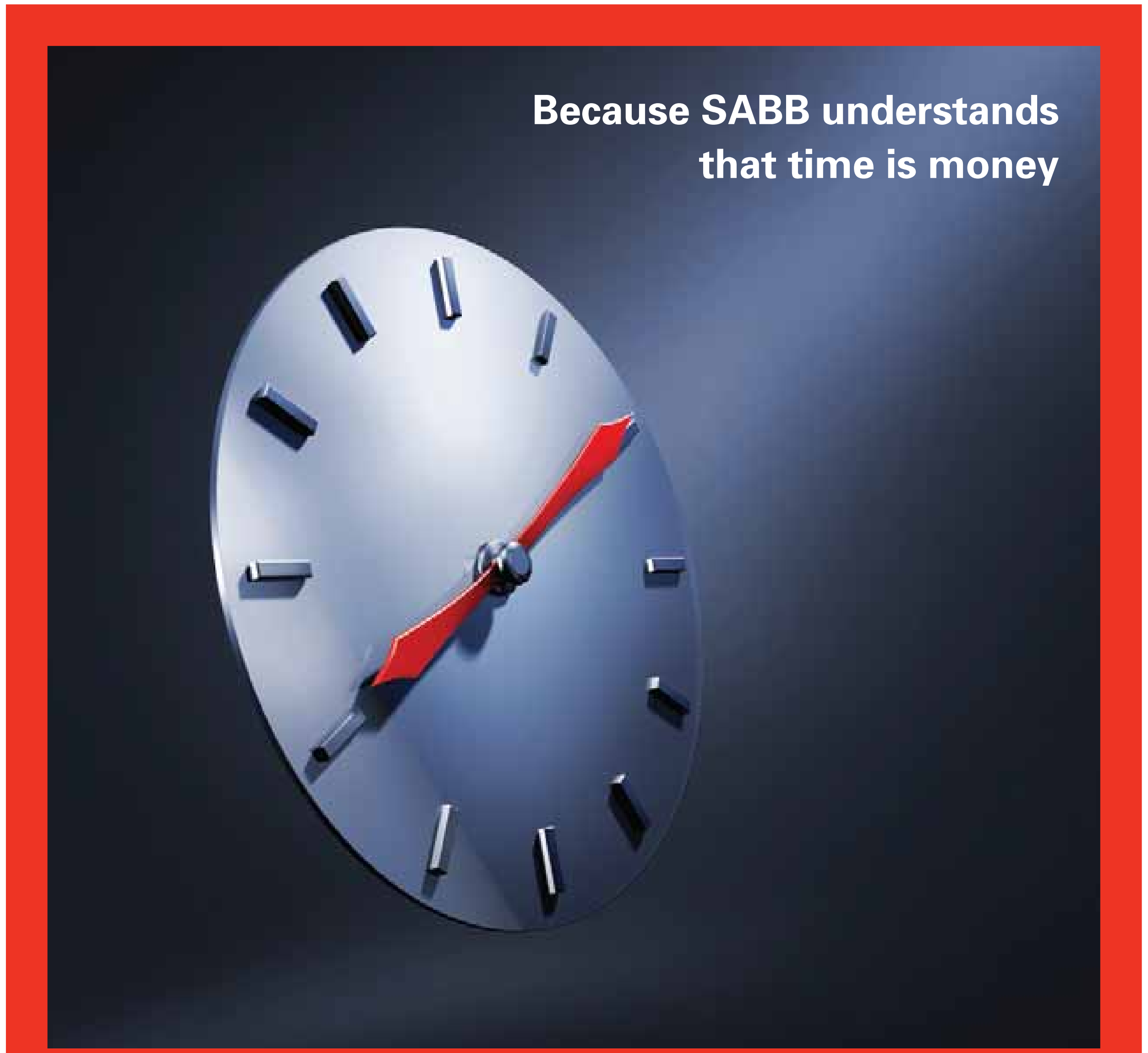
Euromoney Awards for Excellence
Best Cash Management Bank in the Middle East (2005-2007)

Global Finance
- Best Overall Bank for Cash Management in the Middle East (2007-2009)
- Best Bank for Payments and Collections in the Middle East (2007-2009)
- Best CLS-Linked Bank Offering in the Middle East (2008-2009)

For successful integrated receivables and payment solutions through innovative technology and convenient access, contact the HSBC Cash Management team today by visiting www.hsbcnet.com

HSBC
The world's local bank

Issued by HSBC Bank Middle East Limited, PO Box 66, Dubai, UAE. Regulated by the Jersey Financial Services Commission. CRN 090201



In global business, hours and minutes have replaced weeks and days. That is why SABB is geared to turning around your trade-related transactions as quickly and as smoothly as possible, enhancing supply chain efficiencies. Contact SABB Trade and Supply Chain today to see how our solutions can help you.

Global Finance Magazine
Best trade finance bank in Saudi Arabia (2009)

email tradeservices@sabb.com
click www.tradeservices.sabb.com

SABB ساب
Local vision, international expertise

Issued by the Saudi British Bank, a Saudi Joint Stock Company, C.R. 1010025779. PO Box 9084, Riyadh 11413, Saudi Arabia.

CMP - TCM 09013