

financial

i

business solutions in transaction banking



THE FINANCIAL-i GUIDE TO

Information Security

sponsored by

lead sponsor

IdenTrust

ACTALIS

citi

KOBIL *secure your identity*

SafeNet
an Information Assurance Company

25
YEARS
1988-2013

THALES

THE FINANCIAL-i GUIDE TO Information Security

Introduction	2	INFORMATION SECURITY IN PRACTICE
Information Security overview – Know your enemy	4	Data privacy in the enterprise – Implementing robust data protection.....
<i>Karen J Wendel, CEO of IdenTrust</i>		16 <i>Trisha Paine, industry marketing manager, financial services, SafeNet, Inc</i>
AUTHENTICATION & iIDENTITY MANAGEMENT		Expediting and securing PIN issuance – Safeguarding PINs against threats.....
Two-factor authentication – All present and accounted for.....	7	20 <i>Derek Tumalak, vice president, product management, SafeNet, Inc</i>
<i>Steve Brunswick, strategy manager, Thales Information Systems Security</i>		Mobile & Secure Online Banking – Security on the move.....
E-identification as a bank service – Solving the identity crisis.....	9	22 <i>Ismet Koyun is founder and CEO of KOBIL Systems</i>
<i>Joe Norburn, managing director, EMEA and Asia Pacific, IdenTrust</i>		Information security – outsourcing – In expert hands.....
Double Signing – Reading the signs	11	24 <i>Ambrogio Zirattu is CEO, Actalis</i>
<i>John Bullard, vice president, Global Ambassador, IdenTrust</i>		Directories.....
E-vaulting – Taking secure records management to the next level	13	26
<i>Hilary Ward, director, Global Information Products, Citi</i>		

FINANCIAL i

Publisher: Ian Rycott; **Sales director:** Mohamed Isman;

Advertising sales: Marc Carolissen, John Baird;

Production: Alicia Metzger; **Editor:** Anita Hawser

Financial-i, 40 Bowling Green Lane, London EC1R 0NE

Tel: +44 (0)20 7415 7169. www.financial-i.com.

Design: RSB Design; Printed by: The Friary Press, www.friary.co.uk

©financial-i 2008. All information and forecasts contained in this publication have been checked to the best of the author's and publisher's ability, but they do not accept any liability or responsibility for any errors, omissions or loss arising from decisions based on them. All rights reserved. No part of this publication may be reproduced without the prior permission of the publisher.

Introduction

Following on from our inaugural *Information Security Guide* published in September 2007, *financial-i* revisits the topic of information security which has taken on a heightened sense of urgency in light of events towards the end of 2007, and continuing into 2008. A string of high profile blunders by government departments, internet retailers and financial service providers resulted in sensitive customer information being lost or misplaced, increasing the risk that the information could be used for fraudulent purposes.

According to UK-based risk management consultants, Detica, the UK economy loses approximately GBP 14 billion a year due to financial crime. "The data explosion and the internet have enabled criminals to steal identities and commit serious crime with increasing sophistication. Globalisation and the explosion in social and corporate networking also mean businesses are far more vulnerable to seemingly remote disruptive events," stated Fred Chedham, head of Detica's Business Resilience Services.

Recent high profile events involving banks have also highlighted that the biggest threat is not just from external perpetrators. For too long information security has been thought of in terms of fencing off the corporate perimeter from external threats. But now with an increasing number of customer data and security breaches being the result of employee carelessness or internal fraud, traditional measures implemented to deal purely with external threats have been found wanting.

The internal threat presents an even bigger challenge for the financial services and information securities industries as it is not just a case of throwing technology at the

problem, and hoping for the best.

Paradoxically, says David Porter, head of security and risk, Detica, increasing security measures in operational silos can increase operational risk rather than reduce it, as people tend to become more complacent and less vigilant. Securing applications and databases from internal threats also needs to tread a fine line between locking down applications and providing enough flexibility to allow employees to go about their job without seeing security as an unnecessary intrusion.

With the proliferation of web-based trading portals and other applications for delivering financial services over IP networks, securing, encrypting and authenticating data and users of that data has become an integral part of doing business in an increasingly interconnected world. Financial service providers need to ensure that customer and transaction data is adequately secured and encrypted whilst it is stored and when it is transit. Furthermore, as the customers of banks become more comfortable about e-enabling their business processes and move more of their business online, whether it is mobile banking, electronic payments or digital document delivery, the need to ensure counterparties are who they say they are has never been greater.

The increasing popularity of mobile banking and accessing information on mobile devices also poses new challenges for the information security industry in terms of ensuring that the same levels of information security are applied to remote and mobile channels as it is to other parts of the enterprise. In this guide, we aim to outline some of the latest thinking around information security across the enterprise and multiple delivery channels.

Overview

Know your enemy



Karen J Wendel*

Information security is not just about information or security anymore. Like the Jericho Missile in this year's blockbuster movie "Iron Man", which can destroy entire mountain ranges, the array of weapons deployed against the global information ecosystem are vast, frightening, and unlike anything we have seen before. Information security breaches today include items such as trademark infringements, intellectual property asset frauds, consumer protection violations, trade secret, domain name fraud and disclosure violations, along with the usual identity theft crimes. The damages associated with the breaches are both qualitative and quantitative, ranging from significant reputational damage to direct corporate and individual financial losses.

A case in point was the announcement on 5 August 2008 by Michael Chertoff, US Secretary of Homeland Security, of the largest-ever hacking and identity-theft case. The 11 individuals named in the case allegedly captured the credit and debit card numbers of 40 million consumers, selling the numbers to buyers around the world who then used the numbers to either make purchases or ATM withdrawals. The information was captured through a technique called 'wardriving', which involves literally driving around searching for wireless networks. Once located, software was uploaded onto the networks to capture and log the data, which was then downloaded from a remote location by the individuals involved. According to the indictment, the scheme was highly lucrative, netting USD 11 million for one of the perpetrators.

The increasing digitisation of everything

continues to create ever larger pools of information that can be hacked, stolen, damaged or inadvertently lost in the mail, with resulting information security and identity theft issues that damage millions of consumers and corporates. Entities like the nonprofit Identity Theft Resource Center (ITRC) (www.idtheftcenter.org) tracks data breaches in the United States on a weekly basis. Their 12 August 2008 report shows 431 breaches in 2008, with 22 million records exposed. It documents the growth in the "malicious intent" categories, highlighting the increasing awareness of the monetary value of personal identifying information. Another such entity, the Open Security Foundation (OSF) Data Loss Database (www.datalossdb.org) tracks data breaches around the world, capturing not only the type of breach and the numbers of records exposed, but also information on the breach timeline and a map of the location where the breach occurred. Their report shows 205 breaches through 11 August 2008, with 28 million records exposed.

Reports like these provide concrete evidence that the entire information ecosystem is vulnerable and under attack. Many members of the global banking community have long taken the position that information breaches, and particularly identity theft breaches, were in large part driven by paper-based exposures, such as "dumpster diving" (sifting through rubbish collections). However, the 2008 ITRC report shows that 81% of all identity theft breaches are electronic. In large part, this is because in today's world, information is in constant movement, from place to place not only within an organisation but across

multiple organisations and geographies. As a result, information must be protected both while it is at rest and in movement.

WORKING TOGETHER

Regulatory entities around the world have responded to these challenges. Unfortunately, the common recognition of the challenges has not led to a common view on how to address them. The result is a dizzying array of regulatory and guidance regimes around not only information security, but also around notification requirements, electronic signature acceptance and encryption specification. One of the interesting side effects of the mounting regulatory pressure has been the increased reporting of information security breaches across the board by both banking and other entities. The resulting transparency has itself created outrage on the part of consumer and industry groups, leading to additional regulatory requirements. Anti-money laundering and anti-terrorist activities have also led to increased regulatory oversight and intervention, with rules that require higher levels of detail at not only access level (system login), but also the authentication (individual identity proofing at the Know Your Customer) level.

While the overall situation is not a particularly joyful one, there are pockets of good news. The banking industry has made progress in addressing the issue of information security, including providing better notification for the victims of information security breaches. However, 10% of the reported information security breaches still come from banks, up from 7% in 2007. Banks will be forced, by either market or regulatory conditions to improve. Yet simply improving the banking industry will not solve the problem. As banks upgrade their protective barriers, criminals will move to easier targets and will instead attack the banks' customers, which will either directly or indirectly create revenue and security issues for the banks. So what should the banking industry do? There is no

silver bullet. However, there are three things that could shift the direction of the battle.

First: take the lead

The banking industry has shown that it can work together to create common solutions to common problems, with SWIFT as a leading success story. It is time for the banking industry to take a stance on information security and to do it quickly, crafting a guideline that can be used as a path to a safer environment.

Second: get serious about identity, not just security

Controlling access to banking systems and information is good, but not sufficient. Banks and their customers need to know exactly who is using their systems and information, and they need to know it in real time. It is time for banks to acknowledge what governments have known for years – public key infrastructure (PKI) is the best tool available for managing not only security, but identity. The challenge for the vendor community is to simplify the implementation.

Third: protect the ecosystem

Banks must also think beyond their perimeters. It is not sufficient for them to simply hide behind their own firewalls. They must work proactively with their customers and the vendor community to find solutions that flow seamlessly between all parties. Banks must establish information and identity best practices that their customers can use, and they should be aggressive in driving compliance.

Banks have long been uniquely positioned as trusted guarantors of identity and custodians of information. By working cooperatively with their customers and the broader security community in the three areas outlined above, banks have the opportunity to expand that role and to leverage it into new and profitable business partnerships.

**Karen J Wendel is CEO of IdenTrust
www.IdenTrust.com*



Authentication & identity management

TWO-FACTOR AUTHENTICATION

All present and accounted for

Steve Brunswick*

The UK government is not stemming the number of fraudsters operating online, according to the House of Lords Science and Technology Committee's follow-up inquiry to its *Report on Personal Internet Security*. Concerned by the lack of progress that has been made, the committee's recommendation was to fast-track the introduction of a co-ordinated e-crime law enforcement unit, which highlights the growing challenge facing the government, businesses, banks and individuals when it comes to keeping the internet safe.

Since 2000, the total value of online shopping transactions has increased by 871% according to APACS, proving that the committee's concerns are not unfounded. Valued at GBP 34 billion in 2007, UK internet retailing is experiencing exponential growth. With the current systems in place often only asking for card details, the online world is proving the perfect opportunity for fraudsters to commit card-not-present fraud (CNP).

THE SCALE OF THE PROBLEM

Much progress has been made in recent years to stamp out card-present fraud. The UK's migration to EMV chips and the resultant fall in face-to-face and ATM fraud reassured the public that banks were investing in solutions to reduce risk. However, the success of EMV is now being threatened by growing consumer awareness of the risks associated with online fraud. The below figures from APACS reveal the fraud challenge of CNP transactions, which resulted in approximately GBP 291 million worth of losses in 2007. Consumer propensity to spend increasing amounts of money online coupled with a lack of strong

authentication means that financial institutions can be sure CNP fraud will continue to be a blot on the horizon unless there is a new approach.

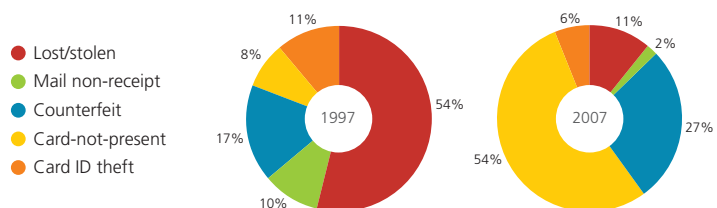
Many UK banks have already addressed one area of weakness – online banking. The introduction of smart card or CAP readers to provide two-factor authentication is a significant step. By making customers strongly authenticate themselves using an unconnected smart card reader and their bank card for online banking, the banks have the identity confirmation required before transfers are initiated.

Figures published by APACS demonstrate that online banking fraud losses were reduced by 33% cent between 2006 and 2007. The roll-out of two-factor authentication in the UK is steadily improving online banking security and showing a return on investment. A recent announcement by Barclays stated customers using two-factor authentication for online banking experience no fraud whatsoever.

For those banks which have not migrated to the CAP infrastructure, there are other solutions available to address online banking



Card fraud losses split by type (as percentage of total losses)



APACS, *Fraud the Facts 2008*, www.apacs.org.uk/resources_publications/documents/FraudtheFacts2008.pdf

fraud. A mobile phone can be used for strong authentication by a bank in numerous ways. SMS password confirmation is one method that serves as dual-channel identity authentication, making the transaction stronger, but not as secure as Chip and PIN. Another method is via an application on a customer's handset. The handset acts as a PIN-activated challenge-response device, providing a code to strongly authenticate the online transaction. However, online banking is only a small element of online financial activity and banks are yet to make any announcements regarding the extension of such security measures to the wider online environment for all types of transactions.

WHAT IS BEING DONE?

It is the card schemes that are currently leading the CNP fraud challenge. Verified by Visa and MasterCard SecureCode are initiatives that encourage customers to register in order to protect transactions with an additional password. The systems allow financial institutions to confirm a cardholder's identity to the online retailer. However, of the 83 million credit and debit cards currently in circulation in the UK, only 20 million are registered with either scheme.

THE TIPPING POINT

With the publicised success of strong authentication for online banking, security advisors in banks are in a strong position to advocate the business benefits of extending its success to cover the whole online payments space. Moreover, banks could soon be facing more stringent regulations in this area that will contribute to the need to address the issue sooner rather than later.

A data breach notification law, as demanded by the House of Lords Science and Technology Committee, would provide both an incentive to avoid data loss and an early warning for affected customers. The introduction of this could create further transparency and enable banks to competitively differentiate if they employ a strong security approach.

THE LOYALTY CHALLENGE

In the past many banks were able to absorb fraud losses created by fraudulent online transactions. Not only is this figure steadily rising, but addressing the fraud that is committed in card-not-present transactions is not only about direct bottom line impact. There is a growing challenge that is more important: customer retention.

According to a recent survey by enterprise communications company, Thunderbird, almost two-thirds (63%) of consumers are actively considering "switching" banks in the next 12 months. This statistic reveals the knife-edge that banks are competing on to keep customers happy. In fact, only a very small number of consumers surveyed felt a sense of "loyalty" to their banks (17%).

Financial institutions are all too aware of the decreasing opportunity to differentiate their services. However, with security breaches constantly highlighted by the national press, banks are presented with an opportunity to allay consumer's online fears and benefit their brand image at the same time. Stronger security will enable a bank to show customers that they are reacting to the threat, and improving customer retention as a result.

THE FUTURE OF ONLINE SECURITY

The overwhelming increase in card-not-present fraud attacks is moving up financial institutions' list of priorities. Combining the financial losses of this type of fraud with the growing consumer impact of security breaches, banks must start taking preventative measures now. The investment in two-factor authentication for online banking is showing promise and should be regarded as a solid platform from which to progress to a wider online security strategy to combat CNP fraud. For those banks which have not made the investment in CAP, mobile authentication is an attractive option. With few opportunities to differentiate services, it is time for banks to take the security opportunity to the next level and implement two-factor authentication for e-commerce.

**Steve Brunswick is
strategy manager,
Thales Information
Systems Security
[www.thalesgroup.com/
InfoSysSecurity](http://www.thalesgroup.com/InfoSysSecurity)*

THALES

E-IDENTIFICATION AS A BANK SERVICE

Solving the identity crisis

Joe Norburn*

Banks have a long and rich history of providing introductions and proofs of identity. Bankers' acceptances date back to the 12th century when they emerged as one of the early forms of the instruments used to finance trade, and letters of credit were thought to have been used by traders like Marco Polo as they explored the edges of Western civilisation. Given the central role that banks have always played in civilised (and some uncivilised) countries, it makes eminent sense that they would also be the institutions that would "vouch" for their customers.

So what does that mean in a digital age, where customers no longer travel with neat leather portfolios containing elegant letters from their bankers and instead interact primarily in an electronic form? Who should be the guarantors of the identities of the entities and individuals transacting in the electronic ether? And how can those guarantors translate those actions into business models that deliver profitable and sustainable revenue streams? More importantly, how do those guarantors work together in a cooperative fashion, avoiding the creation of millions of complex bilateral interactions or guarantees?

Everyone has seen the famous New Yorker cartoon by Peter Steiner of the dog in front of a computer and the tag line "on the internet, nobody knows you're a dog". Clearly, some form of identity needs to exist in that environment, and the ideal would be to have a single interoperable one. The idea of a single interoperable global identity is at once obvious and exciting – nobody wants to wander around with a necklace of

different devices, passwords or challenge questions to remember.

Yet while the concept may be an attractive one, the actual question of how to deliver it is challenging. Multiple solutions have been suggested over the years, ranging from expensive solutions such as the US Federal Bridge that cost billions of dollars to build, to lightweight solutions proposed by entities like the Liberty Alliance and the flawed Microsoft Passport initiative. Individual communities, such as the research entities of the major pharmaceutical companies, have created common shared identity standards, but with limited scope and no ability to function outside the community. Countries have created country-specific solutions, all with their own idiosyncrasies and rules, none of which allow interaction with the rules of other countries. Banks have created different solutions for each of their businesses and often each of their geographies, putting the banks' customers in the cumbersome position of managing multiple different devices and identity solutions for dealing with just one bank.

GOING GLOBAL

The end result is a world of solutions, each existing as a separate island floating in a sea of activities. Individuals or corporates that want to deal across multiple islands must travel from island to island, accommodating the customs of each one. A group of banks came together in the late 1990s to explore how to create a common identity standard. They explored alternative solutions for establishing such an identity, ranging from government-based initiatives to third-party providers such as credit scoring entities. In



the end, they concluded that the most logical solution was for the banking industry to step up to the plate. The logic behind the decision included a number of key points:

■ **Existing Relationships**

Banks have relationships, of some sort, with the vast majority of participants in the global electronic economy, whether corporations, governments or individuals. These relationships are based on a foundation of trust built over centuries of banking/customer interactions, of which identity is just one element.

■ **Regulatory Compliance**

Banks, unlike governments or other potential third-party providers, are regulated on a relatively consistent global level, particularly as it relates to items such as identity. Not only do banks need to follow a particular set of guidelines to identify their customers, but those guidelines are also enforced by external entities.

■ **Transaction Processing**

The concept of a global, interoperable identity requires at its very core a deep and thorough understanding of large-scale transactional systems. The traditional core competencies of banks in the cash management and payment space are readily translatable into the creation of common identity platforms.

■ **Geographic Footprint**

Banks are one of the most omnipresent entities on the planet (after McDonald's and 7-Eleven). The ability to address the needs of all players in the ecosystem is a key differentiator.

The banks also felt that the most logical reason for the banking industry to create a global, interoperable identity was that, as an aggregate, banks must perform some form of identity vetting and should address how electronic transactions of all kinds will provide identity non-repudiation. The time and effort spent managing the complexity of that identity environment could be dramatically reduced if the community as a

whole created a common solution to a common set of problems.

The mechanism for creating such a solution, however, needed to be one that would keep the identity space firmly in the banks' control. Banks are increasingly under threat, not only on the information security front, but also in terms of players who seek to disintermediate the banks from their core constituencies. Banks must find ways to strengthen the ties that exist between them and their customers, not outsource them, and there is no single element more valuable – and potentially more dangerous if misused – than the identity of either a corporate or an individual. The concept of a global, interoperable identity with the banks themselves as the issuers meets that goal.

EARLY SUCCESS STORIES

A number of early adopter banks recognised the power of such a solution, including players like Citi, Royal Bank of Scotland and Standard Chartered who deployed identity services as an offering to their customer base. The success of such deployments has been driven by the definition of clear use cases for the identities, with solutions that targeted particular corporate pain points such as signatory management or local regulatory compliance. These deployments represent the first stage of the evolution of e-identification as a bank service. The second stage will occur when more banks are willing to acknowledge the benefits of an interoperable identity as opposed to a world of 'siloes' solutions.

Last but not least, a common interoperable global identity standard is a key element in the fight to enhance information security. By using identity, with the associated encryption and strong authentication elements, as the means for controlling information, banks and their customers will be better positioned to avoid and/or eliminate damaging information breaches. Such a scenario delivers wins for everyone and the banking community should take up the challenge to make it happen, sooner rather than later.

**Joe Norburn is
managing director,
EMEA and Asia
Pacific, IdenTrust
www.IdenTrust.com*

DOUBLE SIGNING

Reading the signs



John Bullard*

As has been the practice in the paper-based world for centuries, individual officers within corporations have used handwritten signatures to authorise and initiate messages associated with payment instructions, in exactly the same way as they have used their handwritten signatures for the authorisation of all other forms of organisational activity. However there is now a growing demand among the corporate community, from large multi-nationals through to small and medium enterprises (SMEs), to grasp the opportunities afforded by technology to migrate this practice from paper to an electronic format – hence the growth of what is referred to as individual or user-level signing, and/or double signing capabilities.

This demand is driven not only by the obvious business process benefits, which can be delivered by electronic as opposed to paper-based systems, but also by regulation/legislation passed by governments, which impacts corporations not only in their local/domestic markets, but also in their international activities. Sarbanes Oxley from the USA, the EU's 8th Company

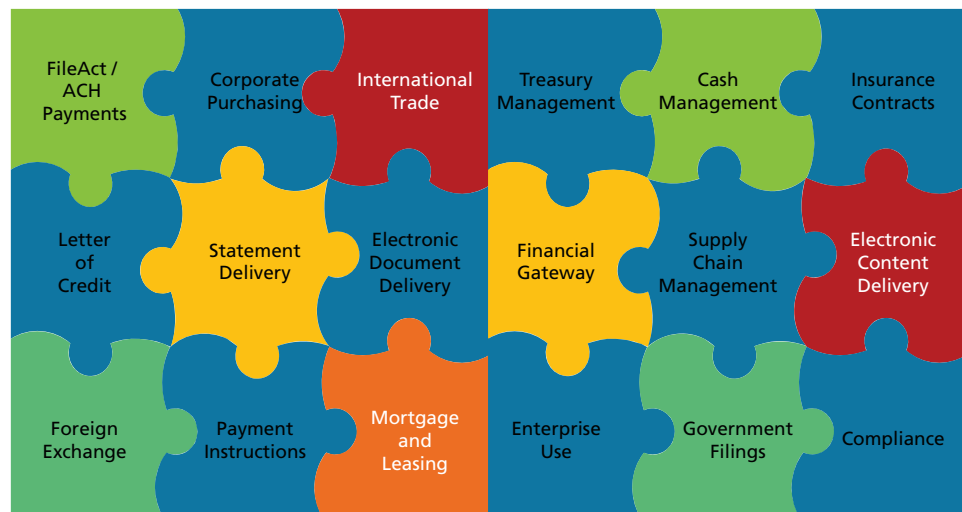
Law Directive, and Japan's J-SOX are well known examples. Historically, both banks and their corporate customers have relied upon "entity level" (organisational) digital signatures as the methodology for achieving privacy, authentication, message integrity and non-repudiation for payment instructions executed over SWIFT.

However, having the knowledge that an instruction comes from an entity, and not knowing exactly from whom within the entity, is no longer a sustainable option. Sharpened corporate governance and the law both require much greater transparency. Another driver for the adoption of user-level signing can be found inside the evolving structure of corporate treasuries. As the volume of payment instructions continues to grow year on year, an average Fortune 500 corporation will execute between 100,000 and 500,000 payment instructions per

A scheme-based approach to managing the operational risk challenges of eSignature/eidentity interoperability and liability in a world of electronic networks



Each application can be used independently or as part of a broader interconnected supply chain offering – all supported by the same underlying trusted electronic identity credential



month, anything from 1million to 6 million per annum. Concurrently as more corporations move away from a geographical or product delineated treasury management structure toward a centralised model – a “payment factory”, so too does the number of payment instructions which move internally within the organisation also increase. Therefore there is a resultant need to undertake validations both internally as well as externally in order to ensure complete data integrity.

How can this demand be addressed? The key surely lies in having a framework under which trusted digital identity credentials can be issued at the individual level in a fully interoperable environment, where those credentials can support multiple applications across multiple geographies and sectors within the overall supply chain. Given their strong KYC practices, banks are ideally placed to perform this issuance function to authorised officers within each corporate customer. At the same time, treasury management application vendors can build their product so that it is compliant and can be enabled by the credentials. This gives those vendors an assurance that they are future-proofed and are building products to a standard “voltage”; it gives corporate treasury full freedom to choose from a range of vendors who are compliant with a

“voltage” which is recognised and useable worldwide.

How does this fit together? The steps are as follows:

- Take an unsigned payment file and apply an individual's high assurance signature to it.
- Validate the individual signature (using online validation) to ensure that it has not been revoked or expired.
- Insert this signed payment file into a SWIFT FileAct envelope and forward it to the receiving banks and payee.
- Decrypt the payment instruction so that it can be routed correctly.

Through this process, the double signing capability can be used with multiple messaging networks, including SWIFT. Whilst providing corporates with the ability to closely control their payment flows, it also provides the bank with full details of the specific content and authorisers of large payment instruction files.

**John Bullard is vice president, Global Ambassador, IdenTrust
www.IdenTrust.com*

E - VAULTING

Taking secure records management to the next level

Hilary Ward*

To meet the demands of a rapidly growing global economy, businesses are increasingly looking to leverage paperless workflows to reduce processing time, internal lag-time and the expense of paper communications – all without compromising visibility or governance. The migration of business-critical processes from paper to electronic has become essential in achieving efficiencies that are key to remaining competitive in today's global marketplace. Equally important in this migration process is the ability to store, manage and archive electronic assets of high sensitivity in a legally compliant fashion.

The growing legal applicability of digital signatures coupled with the ubiquity of paperless workflow environments via digital credentialing and signature technology has created the need to securely store electronic documents or data. These digitally signed documents must be maintained in a manner, which preserves the legal integrity of the document over its life span, even after the authorised employee has left their role at the firm or the firm is no longer in business.

The credibility of digitally signed transactions hinges on an organisation's ability to store and archive data in a manner that is compliant with regulatory and federal requirements throughout the entire transaction processing workflow. An eVault facilitates the archiving and lifecycle management of electronic data and digitally signed documents in a manner that complies with emerging standards and regulations for the treatment of electronic documents. E-Vault facilities should be compliant with

National Archives and Records Administration (NARA), Electronic Signatures in Global and National Commerce Act (ESIGN), and Uniform Electronic Transactions Act (UETA) regulations. For financial services, this also includes SEC 17a – 4 electronic storage regulations as well. As such, much like in the paper world today, information stored through e-Vaulting may be used to provide legal enforceability in disputes or litigation procedures.

Compliance refers to the role of the records management custodian from capture or creation, retention and preservation of the integrity of the information through to proper disposal of the data or document at the end of its lifecycle. Electronic documents consist of the electronic original record and "metadata" or key pieces of information about the electronic record. The term record applies to various forms of electronic information that can be stored in the eVault, for example, Word documents, PDFs, XML, SWIFT messages and batches. An eVault extends the document lifecycle – starting with document creation to its subsequent storage, modification and retrieval – and provides the following benefits:

- Once received by the e-Vault, transaction information and digitally signed documents are stored in a manner which preserves the format, as well as the visual display of "what the user saw" when they signed the original document. This allows authorised users to access and reproduce the signed originals of documents.
- Each transaction creates a cryptographically linked audit trail that uses identity as an enabler to facilitate



secure, paperless workflows and legally binding processes. So, upon completion of a transaction, a transaction receipt that is digitally signed by an authorised employee is stored and made available in the e-Vault.

- In practical terms, the use of e-Vaulting can deliver dramatic improvements to process efficiency. For example, storage and archival capabilities combined with robust search capabilities will reduce both storage costs and time consuming searches through many databases. Clients have the ability to define the record lifecycle beyond the standard legal requirements.

At the very heart of a secure e-Vault transaction is the high-assurance digital identity, which is a physical representation of the user's online identity. This unique identifier is issued on a smart card or USB token. E-Vault services deliver enhanced security through real-time validation of the authorised user's digital identities, as well as physical and electronic controls to prevent unauthorised access to records. E-Vaulting offers greater visibility into the actions of authorised end-users and their role as defined by internal processes. In providing identity assurance, non-repudiation and document integrity, e-Vaulting mitigates the risk associated with sensitive business processes when transacting with business partners.

One of the unique value propositions of e-Vaulting is the ability to conduct lifecycle management of the electronic records, documents or data stored within the e-Vault. Transactions can be stored and maintained for pre-determined periods of time based on audit requirements. The digital signature, as well as the date and time at which the signature was processed is captured and stored for audit purposes. Prior to retrieving or inspecting a document, the digital signature associated with the content must first be validated. E-Vaults also allow users to search records associated with specific digitally signed transactions or by the authorised signer.

Because banks already act as trusted third parties facilitating business-to-business transactions, it is a natural extension of this role to act as an electronic records custodian. Banks have long held a special responsibility in identity certification as regulated institutions, trusted financial intermediaries and administrators of policies such as "know your customer." Entrusting the identity assurance of business partners to a bank is a natural evolution of this relationship. In this way, banks are able to play a vital role in helping to create the "chain of trust" that is critical in the digital world. Banks are utilising their expertise in managed identity services to help customers leverage digital technology and secure storage platforms to effectively carry out business transactions electronically in a comprehensive and legally enforceable manner.

With the widespread "electronification" of business transactions, communications and documentation, the need for secure records management has never been greater. As firms transition from paper-based processes and physical safekeeping to electronic ones, they will need to be able to deal with both physical as well as electronic documents, which include electronic signatures, electronic records, handwritten signature on electronic records (for example a wet-ink signature on a CSP document) or certified images (converted paper documents to electronic), ensuring that these are considered reliable and that digital signatures have legal applicability under government regulations. There will be hybrid models across multiple industries until full electronic processes are adopted. Consideration will need to be made in terms of internal policies related to records management including risk and compliance, legal, and retraining people to adopt new processes. Yet, the benefits of e-vaulting makes highly dynamic, secure records management possible, allowing companies to achieve greater efficiencies, as well as profoundly increase visibility, control and security over business processes.

**Hilary Ward, director,
Global Information
Products, Citi
[www.transaction
services.citigroup.com](http://www.transaction
services.citigroup.com)*



Information security in practice

Implementing robust data protection



Trisha Paine*

Enterprises worldwide are spending approximately USD 20 billion annually on IT security, yet very costly breaches continue to occur. This is due, in large part, to a focus on network security rather than data privacy. Data privacy is the process of securing critical data as it is being stored, transmitted, and used within the enterprise. The need to augment network and perimeter security mechanisms with data privacy technologies has never been more vital. Given that most estimates cite that more than 50% of security breaches are perpetrated internally, perimeter security mechanisms, such as intrusion detection systems (IDS) and firewalls are ill equipped to address the many threats to sensitive data.

The price paid by organisations when breaches become public has skyrocketed. One estimate states that compromised firms lose 2.1% of their market value within two days of a publicised breach, which translates into an average loss of USD 1.65 billion in market capitalisation per incident. This is on top of very real, but harder to quantify, losses that stem from damaged brands and diminished consumer trust. Many firms do whatever they can to keep these breaches from going public. In fact, recent estimates state that only 30% of all security breaches are reported at all. With the rising incidence of threats to sensitive data, and increasing policies and mandates to protect that data, organisations must address data privacy in a

comprehensive fashion. Those that wait for a legislative mandate, or, worse, a security breach, before they do so, may be putting an entire business at risk.

DATA PRIVACY THREATS

There are multiple points of vulnerability within the corporate IT infrastructure, including networks, laptops, application and database servers, and storage systems. Malicious network administrators, mis-configuration, stolen authentication credentials, improperly defined authorisation policies, or malicious software installation can compromise servers. Storage threats include compromise of management interfaces and storage subsystems, theft of hardware such as servers, desktops, laptops, and hard drives, and theft of backup tapes.

CLASSIFYING SENSITIVE DATA

Data classification is an important element of achieving data privacy. One of the first steps is to adequately classify data, by taking the following actions:

- **Identification and classification of sensitive data.** This is a critical first step that will help determine the time it will take to implement a data privacy solution and the impact to the enterprise.
- **Determine where identified sensitive data is located.** For each type of data, organisations must determine which

applications, databases, storage subsystems, and backup media manipulate and store the information.

Once the location of the data has been identified, firms need to determine specific details of each location, such as application/database version, storage size, and OS version.

■ **Determine data access models.**

Identify which applications, users, and processes access the data, and the mode of access. For example, if an application accesses a database, administrators need to understand if the connection is made via driver (e.g. ODBC or JDBC), direct access, or some other mode. The goal is to identify different points of integration for a data privacy solution that provides the highest level of security with the most ease of integration.

DEFINE SECURITY POLICY AROUND IDENTIFIED DATA

Once the data identification and classification process is complete, you are ready to develop a security policy.

■ **Acceptable Threat Level.** While most organisations want maximum security for their sensitive data, it is important to realise that deploying a data privacy solution can range from simple to complex, depending on such factors as data to be encrypted and access methods. Those firms considering a data privacy solution must determine an acceptable level of threat, keeping in mind that the sooner in the data processing life cycle the data is encrypted, the more secure the overall environment.

■ **Authentication and Authorisation Policies.** Develop an authentication and authorisation policy that leverages best practices and historical information to help determine which users, processes, and applications have access to sensitive information. This will help to not only ensure a more secure solution, but will also create a user- or application-based

policy for the access of critical information.

■ **Compliance Measures.** There are many legislative and vertical compliance initiatives that require companies to consider encrypting sensitive data. Architects should identify the legislative measures that apply to their specific organisation, review the laws/language with the assistance of a legal team, and, once an acceptable threat model is agreed upon among business and legal entities, translate those legislative requirements into technical requirements.

LEVERAGE EXISTING TECHNOLOGY STANDARDS

A comprehensive data privacy solution will deploy several technologies across the security framework. It is important to leverage existing technology standards that will help ensure security, performance, scalability, interoperability, and supportability of the overall solution. By leveraging existing technology where appropriate, enterprises can more quickly and effectively deploy a complete data privacy solution. This should include the following:

- **Leverage Secure Transport Standards** – Existing standards, such as SSL and IPsec, are widely used for securing data transport over IP networks and are easily leveraged for deploying a data privacy solution.
- **Authentication, Authorisation, and Auditing Technologies** – Understand, and possibly leverage all of the AAA services within an organisation to augment a data privacy solution. This should include users and processes that have access to different resources, as well as an audit trail that provides detailed logs for each access.
- **Specialised Hardware** – Dedicated hardware platforms can perform cryptographic operations at a much faster rate than a software-based

solution running on standard hardware. Some hardware solutions even provide an additional level of security by never allowing private keys to leave the device and performing all cryptographic operations internally.

- **Cryptographic Algorithms** – Use of standard and proven cryptographic algorithms, such as AES and RSA, are critical to ensuring a high level of security and to manage risk associated with evolving to future data privacy solutions.
- **Software Interfaces** – Use of standard software interfaces is important for managing the risk of future enhancements to data privacy solutions.

DATA PRIVACY IMPLEMENTATION

Implementing a data privacy solution can be done at multiple points within the enterprise. Choosing the point of implementation not only dictates the work that needs to be done from an integration perspective, but also significantly affects the overall security model. Below are four options for deploying a data privacy solution and the pros and cons of each model.

- **Network-level encryption** guarantees the most secure deployment of a data privacy solution because it ensures that the data is secured at every point within the enterprise. Enterprises routinely interact with customers, partners, and other entities over the internet, and secure the transport of those communications with well-defined and mature technologies, such as SSL and IPsec. Yet once these secure communication points are terminated, typically at the network perimeter, secure transports are seldom used within the enterprise. Consequently, information that has been transmitted is in the clear and left unprotected. One solution is to selectively parse data after the secure communication is terminated and encrypt sensitive data elements at

the SSL/Web layer. Doing so allows enterprises to choose, at a very granular level (usernames, passwords, etc.), sensitive data and secure it throughout the enterprise.

- **Application-level encryption** allows enterprises to selectively encrypt granular data within application logic. This solution provides a strong security framework and, if designed correctly, will leverage standard application cryptographic APIs, such as JCE, MSCAPI, and other interfaces. This type of solution is well-suited for data elements (for example, credit cards, e-mail addresses, critical health records) that are processed, authorised, and manipulated at the application tier. If deployed correctly, application-level encryption protects data against database and storage attacks, and theft of storage media.
- **Database-level encryption** secures data as it is written to and read from a database. This type of deployment is typically done at the column level within a database table and, if coupled with database security and access controls, can prevent theft of critical data. Database-level encryption eliminates all application changes required in the application-level model, and also addresses a growing trend towards embedding business logic within a DBMS through the use of stored procedures and triggers. Careful consideration has to be given to the performance impact of implementing a database encryption solution. First, enterprises must adopt an approach to encrypting only sensitive fields. Second, this level of encryption must leverage hardware to increase the level of security and to offload the cryptographic process in order to minimise any performance impact.
- **Storage-level encryption** enables enterprises to encrypt data at the

storage subsystem, either at the file level (NAS/DAS) or at the block-level SAN.

This type of encryption is well-suited for encrypting files, directories, storage blocks and tape media. In today's large storage environments, storage-level encryption addresses a requirement to secure data without using LUN masking or zoning.

ESSENTIAL BUILDING BLOCKS

There are clear choices regarding the modes of implementation when considering a data privacy solution. All of these options vary in terms of security model, yet each provides a level of protection aligned with the potential requirements of an enterprise. While these modes may vary, there are also strong commonalities that represent the foundation of data privacy implementations.

Secure Key Management

It is essential that a data privacy solution include the ability to securely generate and manage keys. This can often be achieved by centralising and, where possible, automating key management tasks on a single platform, which leads to both operational efficiency and reduced cost.

Cryptographic Operations

Enterprises should fully understand the capabilities of cryptographic operations, including when to use certain algorithms to secure data, hashing functions and keyed hashes for data elements such as passwords, and digital signatures to ensure non-repudiation.

Authentication and Authorisation

Authentication allows the enterprise to restrict which users are allowed to access data in the clear. Coupled with an authorisation component, this can provide a strong layer of security with granular access controls.

Logging, Auditing, and Management

When encrypting data, one has to consider the fact that data, keys, and logs will be accessed, encrypted, managed, and

generated on multiple devices and in multiple locations. When considering an enterprise-wide solution, it is essential to consider one with a centralised interface to view information as attacks occur, and that ensures compliance with logging and auditing requirements.

Backup and Recovery

A mechanism is needed that backs up all cryptographic keys and configuration information, and that can restore all of the information from a secure device after an unplanned outage. As the enterprise considers key rotation as part of a proper security strategy, they must also design a mechanism with which to associate cryptographic keys to periods of time during which the keys were used.

Hardware

Today's complex and performance-sensitive environments require the use of specialised cryptographic chipsets built around handling high volume cryptographic operations. Doing so will help keep application, database and storage systems at optimal performance levels.

CONCLUSION

A data privacy solution is a comprehensive way to protect enterprises from an increasing number of attacks that are focused on extracting critical data. It will not only help to protect sensitive information but also work to comply with state, federal, and vertical legislative measures that require the use of encryption for sensitive data at rest. When considering a data privacy solution it is imperative to know the fundamental elements that make up the solution, to leverage standards-based technologies, and to ensure that the proper planning and co-operation occurs within and across the enterprise. Doing so will ensure an effective solution that will meet both business and security requirements within an enterprise.

**Trisha Paine is industry marketing manager, financial services, SafeNet, Inc.
www.safenet-inc.com*



Safeguarding PINs against threats



Derek Tumulak*

Over time, methods of personal identification have evolved from simple name and face recognition to today's electronic-based techniques. Much of the impetus for this evolution has been the advancement of computer-based financial transactions, in particular Automated Teller Machines (ATMs), which provided consumers with access to their funds anywhere at any time. The Personal Identification Number (PIN) came into existence at the same time as the ATM as a means of authenticating the person executing the transaction. Today, the PIN is still most commonly used with ATM and credit cards.

Security is at the core of all PIN-based transactions. Two-factor authentication provides the basis for non-repudiation of financial transactions, which is an essential characteristic of card-based commerce. The person inserts or swipes the encoded card (something you have), and then enters the PIN (something you know). It is imperative that cardholders keep their PINs confidential and complex in order to maximise the security of their accounts. However, PIN privacy originates with the card issuer. The ability to securely deliver PINs to cardholders must be a priority of every card issuer and financial service provider. Sending PINs through traditional mail is costly, time consuming, and highly insecure. Instead, why not look to the same technology used to provide

customers with access to their financial accounts – the internet. In the proper environment, PINs could be securely issued and managed over the web, providing a wide range of benefits to both the cardholder and the card issuer.

TRADITIONAL PIN ISSUANCE – METHODS AND LIMITATIONS

Traditionally, cardholders request a card by mail, internet, or at their local branch office. In a few weeks, the card arrives, followed by a separate PIN mailer. Although a standard method of issuance, these tamper-evident, laser-printed PIN mailers are known to be vulnerable to attacks that reveal the PIN without tampering. Some card issuers prefer to issue cards and PINs in the local bank branch, where the cardholder will be asked to select a PIN through a dedicated terminal or at an ATM. Problems occur when fraudsters place overlays on ATM PIN pads to register cardholder key strokes, or covertly switch out dedicated terminals with dummy terminals to gather the sensitive PIN and cardholder data. Others perform PIN issuance through an interactive voice response system that allows a computer to detect voice and touch tones through a phone call. Unfortunately, these systems cannot be effectively secured.

A STUDY IN PIN MANAGEMENT

With 3.2 million customers, Egg Banking, plc, a Citigroup company, is the world's largest online bank. Several years ago, Egg

began a search for a secure and convenient method of delivering cards and PINs to its customers.

Egg wanted its customers to enjoy the best service possible by being able to use their cards immediately after they received them, rather than having to wait seven to 10 days for their PIN to arrive by mail. Egg also wanted to lower the risk of PIN mailers being intercepted, as well as decrease the costs associated with providing up to three million new PINs a year. Yet, allowing customers to retrieve their PINs via the internet seemed dangerous, even to some of Egg's own IT people.

One of the challenges was ensuring that the customer was the only person able to view their PIN. Preventing disclosure of the PIN across the entire transaction would be difficult since typical SSL sessions meant encrypted data had to be decrypted on the web server. The card issuer holding Egg's customer PIN data had doubts as to whether a technology actually existed to achieve this goal. The solution was found through the implementation of a web-based application security module, with an integrated hardware security module for secure key management.

Egg was able to deploy a secure end-to-end encrypted tunnel between the cardholder and the card issuer, providing cardholders with a safe and convenient way to retrieve their PIN over the Internet. Egg has realised major cost and time savings. For every million cardholders, Egg saves USD 5 million a year in postage and fulfilment costs. PIN requests are now fulfilled instantly, allowing the customer to immediately use their card. These savings will continue as new card customers come on line, or existing customers need new PINs or replacement cards.

SECURING PIN ISSUANCE PROCESS

Egg realised a competitive advantage by offering the enhanced customer experience of instantly issuing PINs over a secure,

easy-to-use web session. With this approach, the hardware and software components are integrated into the card issuer's existing IT architecture and web portal to facilitate the delivery of PINs across the internet, or other communication networks, to the customer. Using hardware-based cryptographic key management ensured that the keys and processes were stored and managed exclusively within FIPS-validated hardware.

“With customers retrieving their own PINs, they feel more in control”

Using the existing bank web site and user authentication system, this solution made use of standard web security protocols, without any customer requirement for applets or browser plug-ins. By leveraging existing authentication and processing systems, no changes need to be made to the core architecture and, therefore, no potential vulnerabilities can be introduced to these sensitive areas.

Considering that the point of issuance can often be the weakest link in today's heavily mandated EFT system, encryption has proven to be the most effective data security solution, ensuring that the storage and transfer of consumer card data is protected against manipulation and fraudulent card production.

With customers retrieving their own PINs, they feel more in control. They no longer worry as to when their PINs will arrive and no longer have to wait for days or weeks before they can use their card. Financial service providers can be assured that sensitive financial transactions execute in a trusted environment that is immune to physical, logical, and operational threats.

**Derek Tumalak is vice president, product management, SafeNet, Inc.
www.safenet-inc.com*



Security on the move



Ismet Koyun*

Security concerns are one of the biggest obstacles preventing bank customers from making online banking transactions. Secure online banking is one of the major challenges facing the increasing importance of e-commerce worldwide. Fraudsters are becoming more and more impudent in their attempts to spy on bank customers' passwords, using trojans, phishing, pharming and man-in-the-browser attacks. While user identification with the still used PIN/TAN-procedure represents a big risk, a smart card and certificate-based user authentication offers the highest security standard. This kind of user authentication has been standardised in Germany as HBCI/FINTS.

The necessity of a card reader, however, makes this procedure highly restrictive for users when carrying out their banking operations. According to a study conducted by Forrester Research, only 30% of all Europeans using the internet believe that important personal information such as data from credit card accounts is always secure in online transactions. The study showed that in future, banks will have to face up to their customers' fears that online banking holds unacceptably high security risks. Only in doing so will they be able to win more users for online banking and keep their existing customers.

SAFETY NET

Potential online banking users' fear of fraud is justified. Traditional user identification procedures with PINs and TANs have many weak points and offer criminals numerous points of attack. Since the first phishing attacks began in 2004, fraudsters' falsified emails are now looking more and more

authentic, thus making it difficult to distinguish false bank websites from real ones. Banks have introduced indicated transaction numbers (iTAN) – during an online bank transfer the computer tells the user which TAN from a list they have to use. This procedure protects against phishing, but not against trojans, with which criminals still can spy on passwords.

Despite the well-known risks, the majority of internet users in Germany (72% according to a current W3B-survey) are still using paper-based PINs/TANs for their online banking operations. Approximately 30% use the iTAN alternative. The most secure procedure for online banking – a smart card and certificate-based user authentication – is only used by approximately 6% of online banking customers.

For this procedure, the customers need a smart card reader, which has to be installed between keyboard and computer. With the help of the smart card, the user authorises himself to the bank's computer and is therefore safe from password theft through phishing, trojans and other attacks. "Especially with this future-oriented technology and a secure smart card reader, there is no longer any chance for phishing. All banks should implement a smart card function and in the long term make it available to all their customers for all transactions", says Olaf Jacobsen, security and online banking expert at the German Association of Volks-und Raiffeisenbanken in Berlin.

One of the biggest obstacles for customers today is the need to purchase a smart card

reader, which has to be connected to the computer and so restricts those who want to carry out banking operations on the road. With conventional smart card solutions, software has to be installed on the computer to be able to prepare transactions offline. Again, the user is bound to their home computer. To meet users' demands for carrying out transactions anywhere, any time, KOBIL Systems developed KOBIL mIDentity.

The solution consists of a smart card reader with an integrated SIM-card sized smart card and a flash memory, on which the Mozilla Firefox browser has been preloaded as a CD-ROM image. It is set up so that the internet address of the bank is configured in mIDentity and cannot be changed. Bank customers therefore can't be diverted to false websites. No driver or software has to be installed on the computer, as the browser automatically starts after mIDentity is plugged in.

TRAVELLING LIGHT

Bank customers are, therefore, completely flexible and mobile – and still absolutely secure. Another advantage is the significantly reduced quantity of bank support, as all settings are preconfigured and the user works in a 'read-only' area, where he cannot change anything by accident or deliberately. Customers can start their online banking transactions immediately.

The smart card the bank supplies to their customers has all the necessary keys and certificates for authentication already integrated, guaranteeing secure banking. The Mozilla Firefox browser on mIDentity also includes a list of trustable CAs, with which the certificate of the bank is checked. To be able to see account data, SSL authentication from both sides is needed. The bank website is verified with the certificate of the bank on mIDentity. The bank server then checks the identity of the bank customer.

If both authentication processes are successful, a secure communication, via SSL

encoding, between bank server and customer will be set up allowing the customer access to their account. At first, however, customers are limited to a 'read-only' authorisation for the account data. To

carry out transactions a digital signature is needed. After the bank customer has filled in the transaction data, they confirm this with a digital signature. To do so, a private user key has been saved on the mIDentity smart card. This private key signs the transaction and sends it to the bank. While the bank customer only has to fill in their PIN, the signature of the transaction is automatically carried out by the smart card. In this way, the customer and the bank can be sure that the transaction is only carried out by the authorised customer and that the content has not been manipulated.

Customers can prepare transactions offline without connecting to the internet. They only have to plug in their mIDentity to the USB port of any computer and then insert their data into the self-opening Mozilla Firefox browser. They can prepare several transactions and sign them offline. As soon as they are online, they can send the prepared transactions to the bank. With conventional procedures, users have to install special software on their computer to be able to do offline preparation of transactions. With the mobile KOBIL mIDentity solution, bank customers have the software on their smart card reader, which means they can easily make secure online bank transfers from any internet cafe, for example. With the integrated flash memory, users can encrypt their data and access it anywhere, any time. The card reader can be loaded with many applications making it suitable as a secure solution for many company applications as well.



**Ismet Koyun is founder and CEO of KOBIL Systems. www.kobil.com*

KOBIL® 
secure your identity

In expert hands



Ambrogio Zirattu*

The term “outsourcing” indicates a long-term, continuous relationship between a customer (financial institution) and a supplier (outsourcer), in which the customer entrusts performance of a particular process that is not core to its business to the supplier. Outsourcing also allows the customer to delegate to the supplier any problems relating to the process. In this way, banks can benefit from the service without having to manage it directly. Literature abounds on the choice between insourcing and outsourcing (make-or-buy), and the parameters that underpin either solution. Outsourcing certainly provides the best value when implementation of the process in question would require the creation of a specialised unit, often a new division or subsidiary, which has little or no relevance to the core business of the main company. A Certification Authority (CA) is an excellent example of this kind of activity.

Financial institutions can no longer afford to provide online services without the support of cryptography, secure authentication, confidentiality and non-repudiation of transactions. However, implementation and management of CA systems goes beyond most financial institutions’ in-house expertise as it requires a dedicated IT infrastructure, highly specialised and dedicated staff and service guarantee levels, as well as high levels of reliability, availability and integration. Outsourcing the activities of a CA is therefore a winning choice. In fact, CAs in the open market are highly

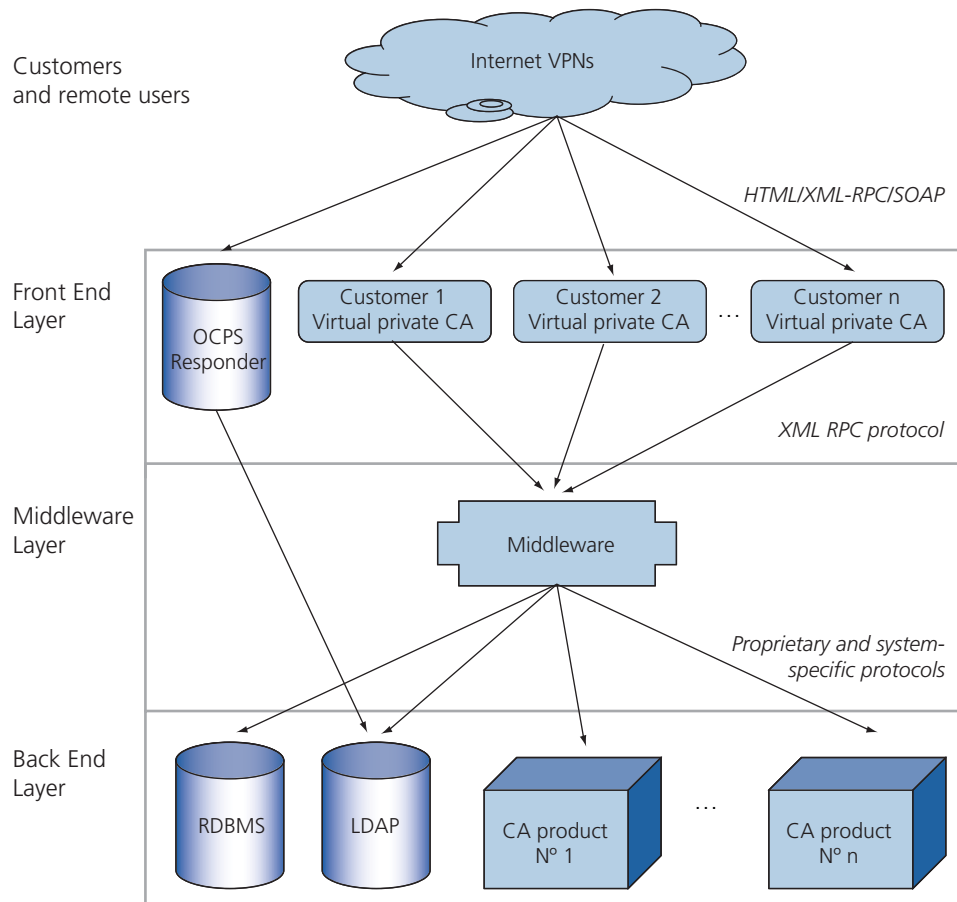
specialised companies that provide a wide range of dedicated products and services. And given the competitive nature of the market, they tend to select those personnel that are most capable of satisfying customers’ requests with the ability to adapt to the changing needs of the market.

However, there are specific characteristics that a CA ‘outsourcer’ must satisfy in order to ensure customers gain the maximum benefit from their outsourcing choice. It is not simply about transferring IT systems to the outsourcer. The outsourcer of CA services should have a technological infrastructure that is constructed in such a way that each customer receives a complete, highly personalised service delivered using a single, dedicated IT infrastructure, which makes real cost savings and optimisation of hardware and software resources possible.

To provide this level of service, the IT infrastructure must be designed and built from the outset with outsourcing in mind, and the CA services should be configured and personalised in such a way to appear totally dedicated to the needs of each customer, while working within the same technological infrastructure. This is what is referred to as a “Virtual Private CA”.

IT ARCHITECTURE OF A VIRTUAL PRIVATE CA

Actalis has addressed the market challenge of CA outsourcing services by designing and



creating a CA IT infrastructure comprising a multi-layered system, where different CA market products (Unicert, Microsoft, Cybertrust, Entrust, custom-made, open-source) are isolated in a dedicated layer, which is used and shared by each customer. The front-end where customers directly interact contains specific configurations that correspond to each customer's business processes. The second layer is the true heart of the infrastructure. It comprises an intermediate layer and middleware – this is responsible for translating and normalising each complex operations request into a series of single, consistent, smaller actions that is shared between all customers. There are two additional layers: one is dedicated to the management of the data persistence and consists of a relational database management system with the support of interface and management functions; the

other is dedicated to the management of cryptographic and key material.

In order to best adapt the CA service to customers' business processes, the front-end layer features a web services (SOAP and XML-RPC) interface. This way, each customer can remotely integrate and request specific services directly from their IT infrastructure so they can quickly modify the characteristics of their CA service in response to market requests. This is referred to as the "Service Portal". Using this Service Portal architecture, Actalis was able to offer four of the major Italian banks an outsourcing service for IdenTrust CAs in addition to a large number of financial institutions and many Italian public bodies.

*Ambrogio Zirattu is CEO, Actalis
www.actalis.it





Directories

IDENTRUST

IdenTrust is the global leader in trusted identity solutions, recognised by global financial institutions, governments, and commercial organisations in over 175 countries.

IdenTrust enables organisations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimise investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust.

The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (P.L.O.T.) to create a comprehensive environment for issuing trusted identities.

FOR MORE INFORMATION:

Karen Wendel, Chief Executive Officer

Tel: +1 415 486 2900

Email: karen.wendel@identrust.com

55 Hawthorne Street, Suite 400
San Francisco, CA 94105, USA

www.IdenTrust.com



IdenTrustTM

ACTALIS

ACTALIS is today one of the leading companies, in both the domestic and European security consultancy market, thanks to its proven ability in designing, developing and managing certification authority systems and services.

ACTALIS offers a wide range of security consultancy services, from check-up to a complete development of Information Security Management Systems, from training on PKI and Information Security, to the design of ad-hoc security solutions for risk mitigation and management, providing its customers with highly qualified professionals.

ACTALIS is a Qualified-certification-service-provider issuing qualified certificates, accredited by the Italian Body (CNIPA), operating with the leading Italian banks on PKI based security solutions in compliance with main international standards and best practices.

ACTALIS is playing a key role in the most important Italian PKI projects, such as: IdenTrust initiative, Italian Banking Association «Progetto Microcircuito» and Corporate Banking Interbancario. Founded in March 2001 by SIA and SSB, ACTALIS from May 2003, has also incorporated the e-security branches of SECETI and BNL Multiservizi (company of BNL Group).

ACTALIS S.p.A.

Via Torquato Taramelli, 26, 20124 Milan

Rome Office: P.le Dell'Agricoltura, 24, 00144 Rome

Tel: +39 02 68825.1; Fax: +39 02 68825223

Email: info@actalis.it

www.actalis.it



CITI GROUP

Citi is a leading provider of managed identity services that help customers utilise digital credentials and signature technologies in a comprehensive and legally enforceable manner.

As a trusted partner to the world's top corporations and governments in more than 100 countries, Citi is uniquely qualified to address identity challenges in establishing trust in B2B transactions by coupling our rigorous KYC processes with proven identity management technology to create value for our clients including:

- Greater visibility into the actions of authorised end users and their role as defined by internal processes;
- Control and governance over the access and activities of end users;
- Assurance of identity, non-repudiation and document integrity to mitigate risk associated with sensitive business processes when transacting with business partners.

For more information about Citi Managed Identity Services, visit us online at:

www.identitymanagement.transactionservices.citigroup.com



KOBIL SYSTEMS

KOBIL Systems stands for secure data and secure communication on every computer worldwide. Business or personal use – KOBIL offers security to everyone.

The technology market leader is setting new standards and is deemed to be a trendsetter with products such as the miDentity, the world's smallest bank and office on 16.94 square centimetre only.

KOBIL technology is used by numerous companies such as Deutsche Telekom, Swisscom, Arcor/Vodafone, T-Systems, DATEV, Commerzbank, Migros Bank, YapiKredi und Isbank as well as the German Parliament, and the German Federal Office for Information Security BSI. KOBIL Systems GmbH, founded by Ismet Koyun in 1986, is headquartered in Worms, Germany.

KOBIL Systems GmbH
Pfortenring 11, 67547 Worms, Germany

Kris Nowak
VP International Business Development
Tel: +49 (0)6241 3004-43
Mobile: +49 (0)172 651 5508
Fax: +49 (0)6241 3004-80
Email: kris.nowak@kobil.com

Salim Güler
VP Business Development
Tel: +49 (0)6241 3004-30
Mobile: +49 (0) 160 743 2735
Fax: +49 (0)6241 3004-80
Email: salim.gueler@kobil.com

www.kobil.com



SAFENET

SafeNet has provided encryption technologies for the world's most important top financial services institutions. Trusted to protect more than 80 percent of the world's fund transfers – \$1 trillion per day, SafeNet uses a portfolio of proven solutions to protect and secure the applications of payment processors, card issuers, acquirers, switches, merchants, leading banks, central banks, governments, and e-payment solutions providers.

SafeNet is a global leader in information security. Founded 25 years ago, the company provides complete security utilising its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. UBS, Bank of America, Adobe, Cisco, Microsoft, the US Departments of Defense and Homeland Security, the US Internal Revenue Service and scores of other customers entrust their security needs to SafeNet.

FOR MORE INFORMATION, VISIT:

www.safenet-inc.com

Contact: Charmaine Earley
Email: charmaine.earley@uk.safenet-inc.com
Tel: +44 (0)1276 608004

www.safenet-inc.com/financial

**THALES**

For more than 25 years, Thales has provided end-to-end security solutions for banks, financial institutions and stock exchanges worldwide. We secure value bearing transactions, data preparation for card and PIN issuing, and provide advanced user and message authentication solutions supported by secure identity management and token issuing. The Thales HSM 8000 secures 70% of the world's credit/debit transactions, and our P3 system is the most widely used EMV card data preparation solution in the world.

Our SafeSign strong authentication solution further extends Thales' financial security solutions. SafeSign is in use today securing personal and corporate on-line banking, one of the world's busiest stock exchanges, VocaLink's BACSTEL-IP direct/credit system and a host of other applications.

We are also experts in Global Security Risk Management, IT Security Risk Management, and Crisis and Business Continuity Risk Management and count many world-leading banks and financial institutions as our customers.

CONTACT DETAILS

Thales
Meadow View House, Long Crendon,
Aylesbury, Bucks HP18 9EQ, UK

Tel: +44 (0)1844 201 800
Fax: +44 (0)1844 208 550
Email: emea.sales@thales-esecurity.com

www.thalesgroup.com/InfoSysSecurity

Financial-i Ltd, 40 Bowling Green Lane, London EC1R 0NE, UK

tel: +44 (0)20 7415 7169 fax: +44 (0)20 7415 7172
e-mail: info@financial-i.com
www.financial-i.com