OpenTrust White Paper
Secured Identity, the Next Disruptive Technology in IT Security.

Sherley Brothier, OpenTrust Chief Technical Officer
Paris, February 2009,

Please address comments to contact@opentrust.com

TABLE OF CONTENTS

I- Introduction

OpenTrust, founded in 2001, is a European leader in Identity and Access Management. Our customers include some of the most demanding European Fortune 500 and government bodies often involved in very sensitive areas (national security, nuclear energy, financial transactions, airlines etc.) as well as enterprises whose aim is simply to better protect their assets.

At OpenTrust, we believe that security will go through major transformation in the coming years. The present security paradigm is to create a "safe" and trustable environment with a "fortress" protecting corporate assets and over time posting additional guards at all entry points.

Security is now entering a new phase. Information Technology, over the past 40 years, has always progressed through major phases generated by disruptive technologies. The mainframe was followed by mini-computers, followed by the client server architectures, followed by the Internet. At OpenTrust we believe that Secured Identity is the next disruptive technology in IT security.

Secured Identity enables each network device and each user to be identified with certainty and trusted. The whole security paradigm is changing. Security is no longer based on the level of protection implemented but on the level of trust in the devices/users. Once identified as trusted, devices/users can then safely communicate with each other.

II- Combining Security and Flexibility: A Core Challenge for CIO's

CIOs today face complex challenges: Information Systems need to be adaptable to meet changing business requirements. Private networks are migrating to the Internet and electronic transactions must be securely implemented in order to boost productivity and mitigate risk. As always, IT budgets are requiring more to be done with less.

Challenges our customers are sharing with us include:

- How can we open the information system to mobile users, third parties and internet applications without compromising security?

- How do we ensure that our information system is flexible and can support Business Transformation (restructuring, acquisitions, new solutions) whilst continuing to meet constantly evolving security requirements?

- How can we secure and track access to critical applications when login/passwords do not provide an adequate level of security?

- How can we better protect ourselves from internal fraud?

- How can we ensure that our information is protected even in the event of a data leak?

- How do we attract and retain young talents if, due to safety and security issues, we cannot provide employees with a working environment that embraces the "new" technologies (Web 2.0, Skype, Wi-Fi etc.) that they use in their homes everyday?

- How can we implement electronic transactions to improve productivity?

These above challenges are familiar to most corporate IT security officers. Yet the real question is: How can we do all of the above without launching a costly & risky "mega security" project?

The answer is not to tackle each of these challenges individually but to implement an I.T. infrastructure which will address them all globally.

III – Peripheral Security: Only a First Step

The first step in securing I.T. systems is to use traditional defensive solutions (Firewall, filter/authentication proxy, anti-SPAM, anti-virus, IDS (Intrusion Detection System), etc.), purpose-built to detect and remedy vulnerabilities.

To overcome certain limitations and to facilitate password-based identity lifecycle management in the information system, many enterprises have chosen to deploy identity management projects based on a corporate directory, or on eSSO (Enterprise Single Sign-On) or Web SSO (Web Single Sign-On) tools.

Unfortunately, defensive security solutions are usually designed to provide protection for internal users within a private network, and thus do not cater for the growing need to access the corporate information system from the outside, via the internet.

Peripheral security was indeed appropriate when access to the Information System was limited to internal employees in a single location.

With mobile computing on the rise, enterprises must now enable employees to access data from multiple types of electronic devices (workstation, laptop, PDA, kiosk, cybercafé etc.), from any location (in the office, from another branch, from a location external to the enterprise), and from different networks (LAN, LS, xDSL, 3G, Wi-Fi, Internet etc.).

For instance a user might access an application from his laptop in his office using the corporate Wan, from his home PC using DSL access, from a restaurant using his blackberry or from the airport lounge using a public Wi-Fi access. This one user must therefore be able to access an application using *three different devices* and *four different networks*.

What's more, today's information systems are no longer restricted solely to internal employees. Partners and suppliers require access to some applications and consumers, via web portals, need to access customer care and/or e-commerce applications.

IT systems are open to many user groups. IT systems rely heavily on the internet. IT systems can therefore no longer rely uniquely on peripheral security.

In many cases, CIO's can't guarantee positive answers to four fundamental questions which, if an information system is to be considered trustworthy, must be answered positively:

- Am I 100% sure of the identity of the individual or the machine with whom I am communicating?

- Am I 100% sure that my data/transaction has not been tampered with?

- Am I 100% sure that if lost or stolen, the data is completely protected?

- Am I 100% sure that I can rapidly adapt my information system to evolving business requirements without creating new security weaknesses?

When asked in private many CIOs answer "No" to some of these four questions and even sometimes "no" to all of them.

IV- Secured Identity: the New Foundation for Trust

CIOs are requiring IT systems that are more secure, less complex to manage and that give users the freedom to use laptops and external devices to optimize productivity. The dilemma is that heightened security usually is accompanied by increased inflexibility in the I.T. system resulting in constraints for users that can hinder productivity.
In order to combine these objectives, which currently appear contradictory, a new disruptive approach is needed.

The foundation for Electronic Trust is that each device and each user has a secured identity i.e. *an identity which can never be forged*. Based on this identity, the I.T. systems can identify each user/device with certainty, determine if a user/device is trustworthy or not and as a result to which resources it may access.

Electronic Trust is a powerful and beautiful concept. The beauty of it is that it is based on an incremental approach. Electronic Trust allows companies to leverage investment already made in their IAM: This is why we refer to "Electronic Trust AIM 2.0."

Indeed most companies have started IAM projects. Some have simply implemented LDAPs. Others have implemented provisioning and SSO. The most sophisticated ones are deploying roles and rights management. Electronic Trust can begin as soon as a company has deployed an LDAP.

V - The Benefits of Electronic Trust

Electronic Trust can be deployed in three areas. Each area can be deployed separately in a "step-by-step" or "need-by-need" approach. However in the long term, relying on a common infrastructure to support all three areas results in significant savings and reduces the complexity of the I.T. infrastructure.

Trusted Network and Infrastructure:

Each network device (servers, routers, workstations, VoIP telephones, smartphones etc.) must be given a trusted identity for authentication. Key benefits are:

- Access to the network is only granted to devices which carry an identity approved by a set policy. These devices are therefore considered safe for the network. All other devices will be isolated and their access limited to public data & applications.

- Within the network each device will only have access to a defined set of resources. For instance, one PC may be set to access the servers and applications from a given department (R&D for instance) while, another PC, which does not carry the proper identity (for instance a visitor, or an employee from another department), will only be authorized to access certain resources such as the Internet or a printer.

- "Trusted domains" also called "security bubbles" can be easily created within each network.

Trusted Identities for Users:

Identity Aware Networks provide identification for devices, but a reasonable doubt about who is actually using the device can remain. Login/passwords can be forced or stolen without the user even being aware of it.

A stolen SSO login/password will give a thief access to a large number of applications. SSOs are indeed more user friendly but they call for higher levels of security.

Only strong authentication based on smart cards and OTPs (One-Time Passwords) provides identification right through to the user himself.

A user who possesses a smart card and/or a one-time password, has been identified in person. He signs a chart agreeing to keep his pin code confidential and to make an immediate declaration if his card is lost or stolen. The key benefits are:

- All devices are equipped with double security; the certificate on the card and the pin code. In order to connect to a network, a user needs access to the PC, to the Smart card and to the pin code. Even if two of these three elements were stolen security would not be compromised.

- The user is identified with certainty and can therefore be held fully accountable for his actions.

- The content of a desktop or laptop can be encrypted to protect the data even in the event of theft.

- A single card can be used for multiple purposes (PC access, access to premises, micropayments for cafeteria or coffee machine…). In addition, most users are more comfortable with one pin code than with multiple passwords that must be changed regularly.

Trusted Electronic Transactions:

Would you start a transaction if you did not know who you were dealing with? The answer is obviously no, and without trust and accountability no transaction can take place. This is why Trusted Digital Identities are a prerequisite for implementing digital transactions.

Once the Identity infrastructure is in place, the other elements of a trusted transaction infrastructure such as providing proof of the integrity of data exchanged or having access to electronic proof in case of claims can be implemented.

Electronic transactions open doors to a wealth of productivity for companies who are still dealing with administrative processes using paper. Why do two companies who use similar ERP systems still send out invoices and forms in paper format? This seems incredible but is still reality in many cases.

Placing Identity Management at the heart of the IT infrastructure brings security, flexibility and productivity together to new standards. In order to better understand how each of the described benefits can be reached, we need to take a more detailed look at each area of electronic trust.

VI – Trusted Networks and Devices: Intelligent Access Networks

We live in an increasingly connected world where the internet is the preferred method for connecting offices and branches within an enterprise: MPLS VPN offered by service providers currently provides high levels of security while supporting high added value functions such as WAN service quality (including multi-service providers).

The same applies to mobility requirements with roaming connections on the increase due to internet and high speed mobile phones or 3G+ devices: the internet is also the preferred method for remote information system access.

Until now, security has been addressed from two angles. Firstly, the network is protected peripherally using filtering rules (IP address, MAC address, TCP/UDP ports, NAT, etc.) and secondly using software and applications (IAM, SSO, LDAP, Directories). The worlds of the network and of the application have been, until now, managed totally independently. Identity Management 2.0 bridges this gap.

Over the last 3 years, OpenTrust has developed a global approach to security where peripheral security is complemented by "Trusted Ecosystems", where each device has its own identity. Each component (router, network, machines & devices, servers) knows if it can trust the calling component and/or the component that it must in turn call to perform a task (and so on).

This concept of digital identities (and consequently strong authentication) placed at the root of each system is gaining popularity among networking equipment vendors. For example, CISCO is now referring to « CISCO Trusted Security2 » or the « TrustSec » model to recognize data associated with a user's role and then, based on this role, regulate what is authorized and what is not.

In most cases, the 802.1x protocol and X509 certificates are the principal components implemented for machine authentication. For instance, the decision to connect one machine to a VLAN rather than another is based on strong authentication, machine status and whether the calling machine meets certain security requirements (« antivirus » or « anti spyware » up to date for example etc.) along with the physical location of the machine. The same applies to VOIP telephones where X509 certificates are used in the IP workstations to authenticate and encrypt communications.

The traditional physically segregated network (with little room for evolution and costly to maintain) is replaced by a logical network based on the different roles and privileges of trusted machines. Placing identities at the core of the network brings a number of breakthroughs.

- Each device becomes a Policy Enforcement Point. Even if a malicious packet manages to penetrate the network, this packet is quarantined when it reaches a router or a switch as the router or switch recognizes that the packet in question has been sent from a device that does not comply with the policy defined by the company.

- Users who are not authorized to access an application are prohibited from communicating with the server that hosts this given application. This drastically reduces the risk of denial-of-service and other attacks.

- Large enterprises are able to integrate several networks into one without compromising selective accesses. This can lead to significant savings.

- Also, in the case of an acquisition or spin off, Identity Management enables rights to connect to certain parts of the network to be easily granted or revoked, a flexibility that I.T. managers had only dreamt about in the past.

VII - Trusted Users: Credential and Smart Card Management

Over the past few years, more and more enterprises have been choosing to deploy IAM solutions produced by market leaders such as IBM/Tivoli, Sun etc.) using LDAP or ActiveDirectory, provisioning (Identity Management) solutions, meta-directories or eSSO/WebSSO functions to manage users and/or employees.

Until now, identity and access management has been perceived as the management of the lifecycle of identities held in different repositories of the corporate information system. This approach requires authentication via login/password and goes hand-in-hand with the associated security risks (identity theft) and complexity for the user (remembering many passwords).

The question « *Am I 100% sure of the identity of the person with whom I am communicating* » can only be positively answered if existing identity management solutions are integrated with a state-of-the-art solution in strong authentication and digital identity support: **the smart card**.

Today, most cards and tokens are designed to hold secrets required for authentication (X509 certificate, OTP seed, eSSO secrets, etc.) and can also be equipped with magstripes, RFID, MIFARE, HID etc.

Authorization, based on a single corporate badge and on strong authentication, is then integrated into a trust infrastructure. Not only does a smart card provide secure support for a user's digital identity, it also provides a means of lifecycle management for both physical (premises, canteen payments etc.) and logical (user credentials) access.

This solution, that OpenTrust calls, « Trusted Identity » provides an extremely high level of digital identity security (both physical and logical) with:

- End-to-end identity and credential management

- Full integration with leading Identity Management solutions

- A single point for managing digital identities, delivering increased productivity and efficiencies

- Cost benefits by combining physical and logical access and reducing operating and Help Desk costs

- A simplified approach for users to manage their identities (elimination of multiple passwords)

VIII - Trusted Transactions: Electronically Secured Transactions

Although paperless transactions are now a reality in today's business processes, there is still a long way to go: when placing an order with a supplier, a project manager makes a purchase request in the ERP system (or asks his assistant to do so); the request is then approved and the PO generated. Why then print the PO out on paper to send by fax or regular mail to the supplier who, more often than not, will enter the information into his *own* ERP system in order to process the order!! Setting up an ERP system within an enterprise costs vast sums of money: it seems illogical to continue to send out purchase orders on paper.

If we wish to send this type of information electronically, we must be 100% certain that we can guarantee the integrity of the transaction between applications.

OpenTrust's solution of « Trusted Transactions » provides a reliable, simple and secured means of proving that each transaction can be trusted by both sending and receiving parties. Based on digital identity, digital signatures and proof management, a "trusted transaction" is fully traceable, non-repudiable and executed in accordance with rules and regulations.

Since companies will be bound by electronic transactions to the same extent as a paper contract, the people involved in the transaction need to be identified beyond any possible doubt. In addition, different users may have different roles in a transaction (processing the transaction, approving the transaction etc.). Identity management will ensure that each user involved in a transaction is confined to his own role as defined by the company (for instance, a person processing a transaction cannot be the one approving it). This can be extremely useful when companies need to prove for regulatory purposes that a given procedure is always respected.

Once the identity management infrastructure is implemented, the next step is to secure document integrity and time-stamping services. Indeed, we can only rely on a document if we are fully confident that it has not been tampered with by a third party and if reliable proof of when it was sent is available.

The final step is the possibility to archive, retrieve and restore the documents even years later in event of a dispute over the transaction. OpenTrust partners with third parties for archiving transactions.

Electronic transactions are a combination of technology, of regulatory/legal elements and of business processes. They still often require tailored solutions. However, the benefits of electronic transactions are so important that one can question why so few companies have not yet decided to implement them. Until now, one of main inhibiting factors has clearly been the complexity of electronic identities. The new generation of Identity Management Solutions has, however, removed this inhibiting factor, providing companies with a wide range of simple yet secure ways to improve productivity.

IX - Conclusion

OpenTrust places trusted digital identities at the root of each information system component, be this the network and each active network component (router, hub etc.), the workstation or device (PC, Laptop, Smart phone, etc.), the user (or to be more precise the digital identity that will be used by the systems and applications), or the systems and the applications themselves that require authentication, traceability and privacy.

Identity management is a disruptive technology. It is a disruptive technology because it changes the paradigm for security. Security is based on Trust, not on peripheral protection. It is a disruptive because it allows IT managers to manage their infrastructure with greater flexibility. It is disruptive because it reconciles mobility and security. It is disruptive because it opens up new opportunities for improved business processes and increased productivity. It is disruptive as this trust-based approach to security will dramatically help leverage existing applications and facilitate the creation of new services.

OpenTrust solutions have already been deployed to millions of devices & users worldwide within Fortune 1000 & Governments; ask for our Customer Business Cases at com@opentrust.com

