



WHITE PAPER

Digital Client Certificates Securing Your Mission Critical Applications

CONTENTS

EXECUTIVE SUMMARY	1
SECURING MISSION-CRITICAL APPLICATIONS	1
Opportunities and Risks	1
Secure Network Access	3
Secure Messaging	4
Paperless Transactions	6
Barriers of the Past	7
INTRODUCING TRUE CREDENTIALS®	8
Overview and Approach	8
<i>Outsourced PKI Infrastructure</i>	8
Initialization and Setup	9
Identity Verification	9
<i>Employees or Known, Trusted Clients and Business Partners</i>	10
<i>New Unknown Clients and Business Partners</i>	10
<i>Consumers</i>	11
Certificate Delivery and Lifecycle	11
GEOTRUST EXPERTISE AND PRODUCT PERFORMANCE	12
Tested and Proven Products	12
Airtight Physical and Network Security	13
Scalability and Availability	13
CONCLUSION	15

EXECUTIVE SUMMARY

The opportunities inherent in securing applications for remote access, messaging and paperless transactions are within reach. Costs are low. Deployment is fast. And the technology can be employed in every enterprise, from finance, insurance and Internet commerce companies to education and government organizations.

Most people's first thought when considering the application of security to existing applications is about reducing risk or costs. But because digital credentials enable completely new capabilities not possible otherwise, they also offer new revenue possibility. Certainly there are significant opportunities as well to reduce costs especially in the secure access category. Replacing dedicated leased lines or time synchronization tokens provides a ripe opportunity to reduce costs by at least an order of magnitude. It is also intuitive that applying secure credentials to existing applications can reduce risks especially if they are replacing a simple password scheme. But the risks of open communications using email are huge when the content includes business critical or intellectual property.

True Credentials® from GeoTrust removes the barriers, addresses the risks and allows the enterprise to seize the opportunities inherent in moving quickly to secure mission critical applications for employees, business partners, and other trusted internal and external 'clients', in a fast and easy way.

SECURING MISSION CRITICAL APPLICATIONS

The Internet represents opportunity for enterprises to extend their reach, integrate their community of employees, business partners and customers, and to reduce costs by using inexpensive public networks. But the Internet represents risk for enterprises because it is open, anonymous and insecure. Seizing the Internet opportunity while securely addressing its risks has been the challenge and promise of security infrastructures for a decade. The barriers of the past have finally been addressed, however, making it possible now to turn the most mission-critical networked applications into safe and secure new business opportunities.

Opportunities and Risks

The Internet is an enabler for new, better, and cheaper ways to do business. It provides unparalleled reach with millions of registered domains and users worldwide. But it's the source of great risk too. The Internet (and the Web) are based on standards and a history that keeps it open and the information on it typically open, readable and shareable.

Standards, openness, and reach have been the engines of the unprecedented expansion of the Internet since 1995. Business, however, cannot thrive in an open, non-confidential, and anonymous environment. Business cannot change this fundamental fact and the Internet is not going to change its fundamental premises either. Such a stalemate can only be broken by providing a way to credential users, a way for them to present these client credentials electronically to the networked applications they use, and cryptography to encrypt all electronic transmissions so no one unauthorized can read or understand the transmission.

The computing model has changed dramatically for enterprises over the past 10 years. Figure 1 shows a side-by-side comparison of the network model used before enterprises expanded their infrastructure out to the net and after they networked. The transformation has been dramatic. The new model allows direct and immediate feedback from, and services for, the customer. It makes it possible to have all remote field sales people directly interacting with the customer relationship management (CRM) system. It makes it possible to have vendors directly connected into the supply chain purchasing process.

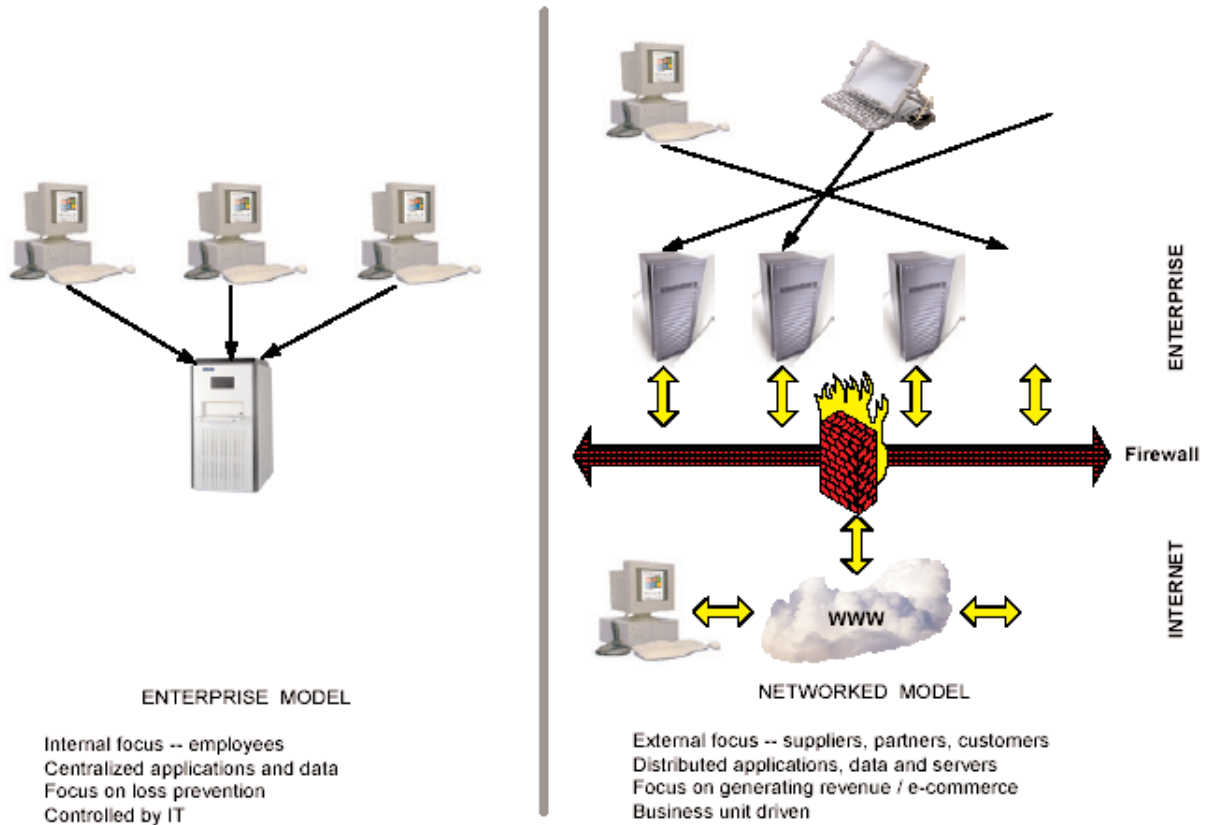


Figure 1

Promises have been made about technology to address the risks and enable doing business electronically for many years. This security technology is called public key infrastructure (PKI).

Technology by itself never solves critical business problems. Neither can technology by itself provide rich new business opportunities. Technology that requires large enterprise-wide investment in infrastructure, special staffing and training - and must be applied towards all applications running in the enterprise to pay back its investment - rarely succeeds. There are two simple questions to ask:

- What critical things am I being prevented from doing because I do not have a secure way to do them?
- If I was first to do X in a secure way, would I gain significant new customers and new revenue?

Applications focus is the key. What are the applications that need to be addressed within the enterprise that will attack the biggest security risks and provide the largest possible opportunity? Three application areas jump out as providing the largest opportunity for generating new revenue and taking advantage of the structural changes occurring in the networked enterprise:

1. Secure network access
2. Secure messaging / S/MIME
3. Paperless transactions

Secure Network Access

Secure network access (see Figure 2) allows someone outside the network perimeter and firewall inside to access internal applications. This has been done to date using time synchronized tokens, VPNs, or user-name / password through the browser. The leading provider of time-synchronized tokens has shipped over 500 million of them to date and yet many enterprises are looking to replace them because of high cost and low usability. Many VPNs require special client software but are very secure if they are authenticated with a digital certificate and not just a password. Password schemes are low security because people write down their passwords, they use the same password in multiple settings, they can easily be observed typing in their password, passwords can easily be guessed and because people relay their password on to others.

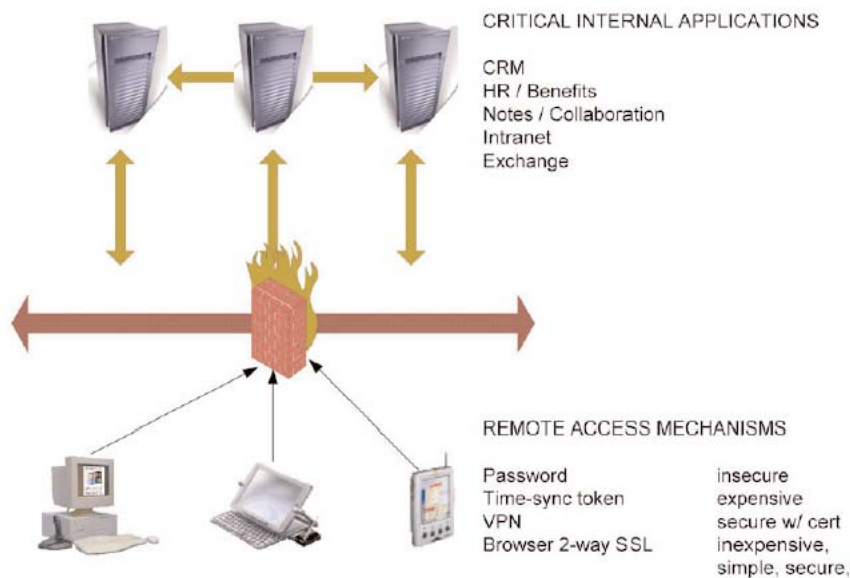


Figure 2

The driving motivation to provide secure access to mission-critical enterprise applications is to increase the efficiency of the workforce and to create a virtual enterprise that brings suppliers and partners in for trusted transactions. CRM applications are a great example. Benefits programs for employees are another. Just opening these up without adequate security is a recipe for disaster as the company's crown jewels are open to the unwashed Internet.

Secure access for all remote employees without special hardware and software but done securely over the cheap public Internet will eventually be a standard part of every enterprise.

The workforce has become more mobile, while the enterprise has become more and more sophisticated in how it uses its internal network for applications that drive the bottom line. Opening up the network to remote access means remote employees become as effective as local employees accessing rich information put on the internal network. Connecting the dots says that too much is lost if the remote employees cannot participate in the critical internal applications. On the other hand, opening up these applications to the wrong individuals would spell disaster. Previous approaches have been expensive, insecure or non-existent.

The time-synchronized token secure access approach requires a special token (usually put on someone's key chain) that generates a random number the user must supply along with a PIN at login time. But at \$45-55, tokens can be replaced by digital certificates at less than one quarter the cost. VPN is a powerful technology that creates a secure IP "tunnel" from client to host that secures every application it can access. But, VPN is weakened substantially when the login requires only a password. Replacing that password with a digital certificate makes VPNs a much tighter secure access mechanism.

An inexpensive, secure mechanism that uses standard clients and servers we all already have is two-way SSL secure access. Just installing a client certificate in standard browsers activates two-way SSL. One-way SSL is the common secure communication mechanism we are all familiar with when browsing and shopping on the Web - a server-installed digital certificate activates the lock symbol in our browser. Two-way SSL requires that the browser client also authenticate itself to the server. This replaces user-name password schemes. The user is authenticated (logged in) to the certificate on their machine and then that electronic credential is passed from client to server machine becoming this user's electronic identity. Unlike passwords, certificates are not moved from one user's machine to another. They cannot be relayed over the phone to someone else. They are not forgotten and they cannot be guessed.

Like one-way SSL sessions, all data transmitted is encrypted and cannot be decrypted even by an eavesdropper with a supercomputer.

Secure Messaging

Secure messaging (think email for now but later, instant messaging, voice over IP and so on) is about making sure only the intended recipients of your message can read it (see Figure 3). The more that email is used, the more important it becomes for company confidential information. This is especially true for email going outside the enterprise. Email moves across the public network from server to server in plain text. Servers along the way can and do save all messages they touch and have the right to do so. In most email systems, a sender has no control over who gets a forwarded email message and no audit trail showing this has happened (we have all been burned by this even when we say "please do not forward"). Email is routinely getting companies into trouble (think about Microsoft's embarrassing messages that keep showing up in the press because an employee forwards it outside). Securing email has not been done extensively because of the difficulty in authenticating senders and receivers and in getting them their certificates. But once certificates are correctly installed, all standard email clients support signing and encrypting.

Internal as well as external communications is vital in any business or organization. Email is by far the most prevalent form of communication in these situations. Email has been and continues to be the "killer application" of the Internet. Its ubiquity has made it a mandatory part of everyone's lives. All modern email clients support signing and encrypting messages to keep communication private and confidential. Both parties of the communication must agree to use digital certificates. With a certificate installed, email clients and servers continue to work unaltered but all the intermediate servers, ISPs and networks can store messages without ever being able to read them (the host enterprise however, can establish a key recovery scheme that allows them to decrypt any message sent by an employee if required). The key

is getting certificates to all senders and recipients of emails and for that to happen, all employees and all trusted clients and business partners must be authenticated and provided a digital certificate that they download and install. Figure 4 shows the email certificate and the dialog in Microsoft Outlook when a signed and encrypted email is being sent.

The cost of secure messaging implemented in this fashion is just a few dollars per sender (certificate) per year.

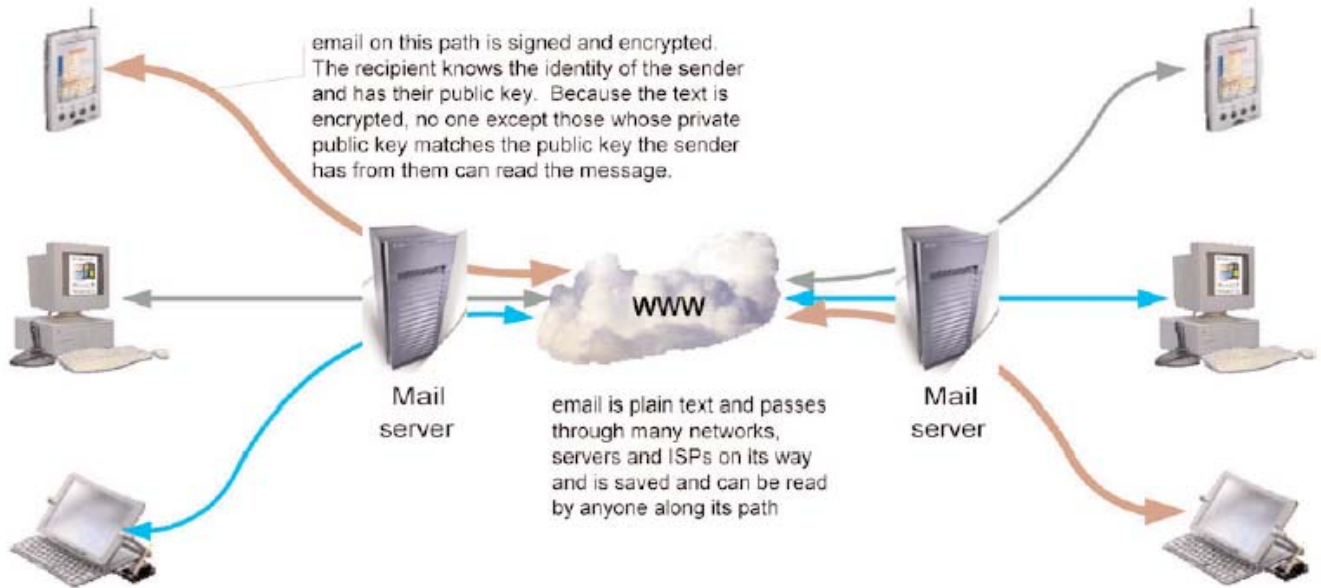


Figure 3

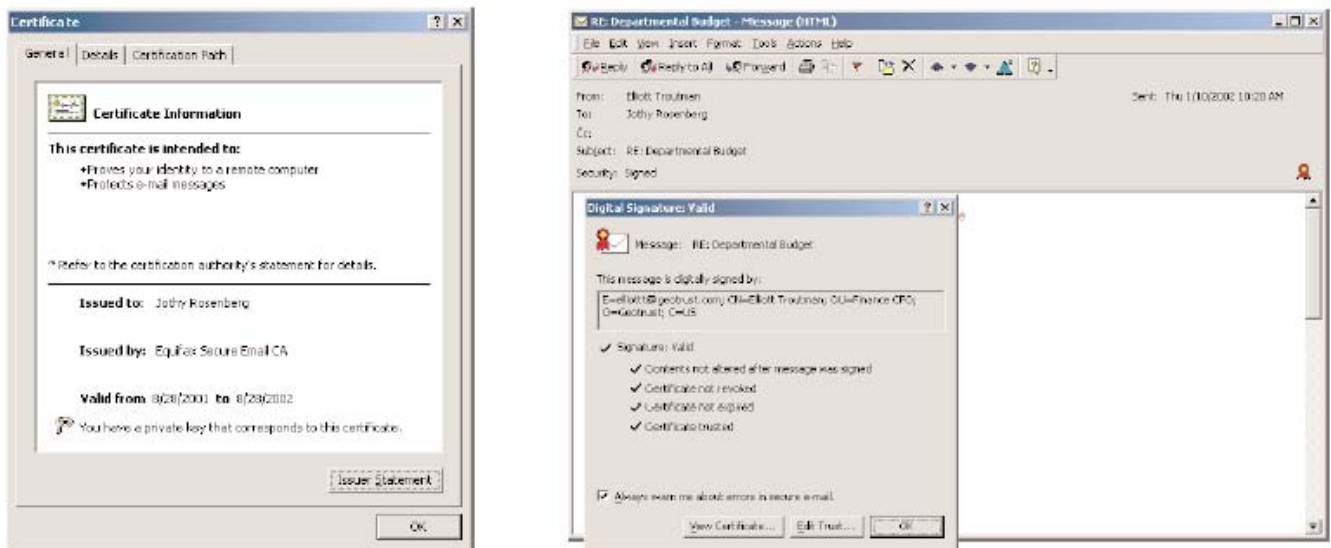


Figure 4

Paperless Transactions

In a sense we can say that there has been a steady trend for 30 years towards the "paperless office" (see Figure 5). On-line forms, email, Lotus Notes, and the Web itself are testaments to our progress. Only last year was it made legal to sign a legally binding document electronically with the US eSign legislation (similar exists in Europe). Now that it is legal, the floodgate has opened as loans, insurance, contracts, mortgages and more can be done completely on-line. For loan and insurance applications, it is typical to see end-to-end process time shorten from 60 to 15 days.

Paperless transactions have been the holy grail of maximizing efficiency. What is needed to achieve this elusive goal is a way to prove the identity of the signer, that the signer intended to sign and that the signed document was never altered in the slightest way. Identity is proved by asking the consumer a series of questions ("shared secrets") from a confidential credit file.

That can only be done by a federally sanctioned credit bureau such as Equifax or Experian. This identity must then be made electronic by tying a digital certificate to that individual. The encryption keys associated with the digital certificate are used to perform the cryptography behind the digital signature. The original document and the digital signature are transferred intact across the network to the enterprise who saves them. Document integrity can be proved via the digital signature. Non-repudiation is provided by the association of the signature to the keys in the certificate to the authentication process back to the individual whose intent can now be proved.

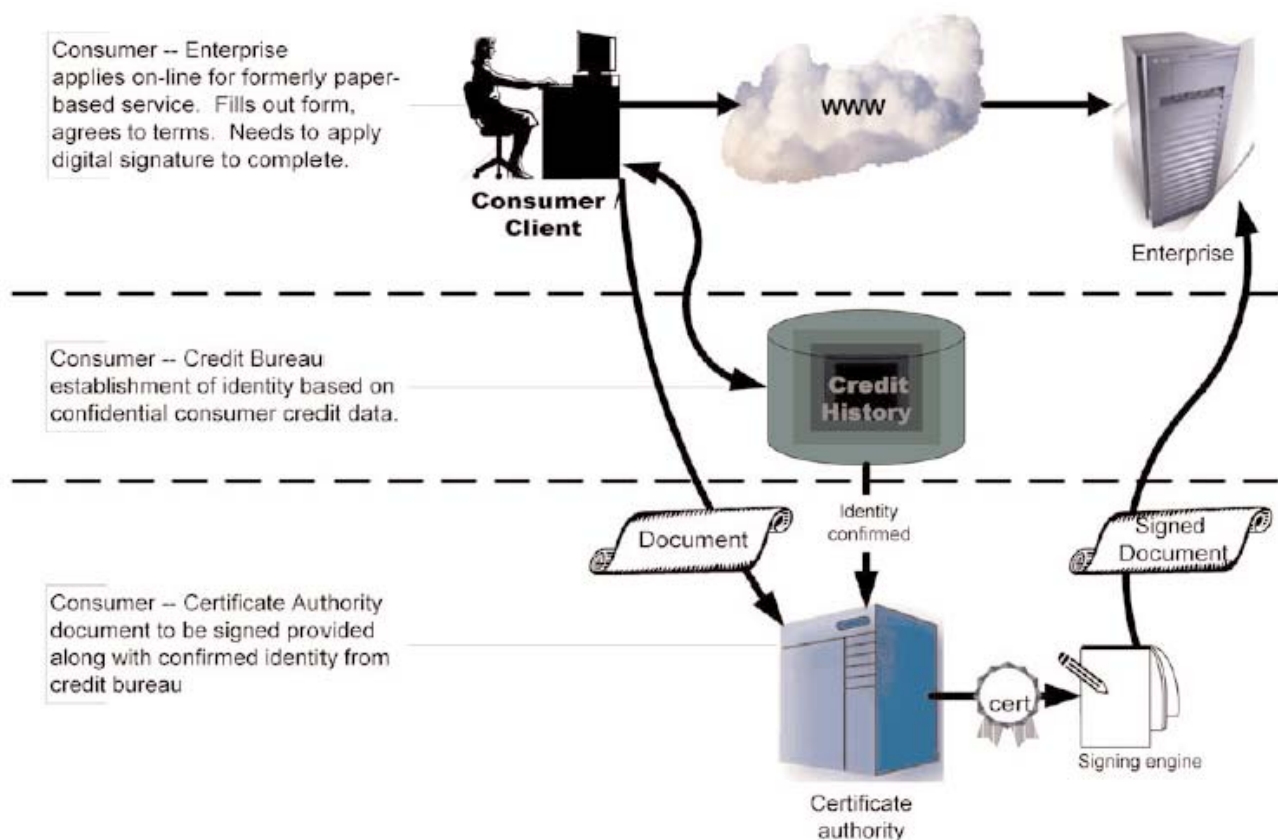


Figure 5

Barriers of the Past

An overarching barrier to achieving the benefits of securing network applications has been the time and expense required to bring in large complex PKI systems, to hire specialized talent and to convert the entire enterprise and every application in it to use identity and security infrastructure all at once.

PKI is highly complicated and costly to administer, especially across an enterprise. Costs associated with deploying PKI include:

- Registration Authority (RA), Certificate Authority (CA), key management and recovery software;
- Acquisition, support and maintenance of associated hardware (many times in redundant secure facilities);
- PKI program manager/administrator (at times a 24/7 operation);
- Help Desk and support to end-users and external clients.

Studies show that the cost to deploy (self-managed) a 1,000-user PKI system include \$350k start-up (minimum) and \$200k per year to maintain. Upgrades to PKI software/systems are difficult and costly to manage. And a seasoned PKI program manager can cost upwards of \$125-150k (salary) per year. Managed certificate services cut these costs significantly by softening the burden on internal resources, placing the operational burden on the outsourcer, eliminating technology (PKI) obsolescence because the system is built and maintained centrally ala the Centrex central office phone model.

There are additional barriers to building out secure messaging across the enterprise that are firmly addressed by a managed security service. One is the need to install complex systems that maintain large directories of individuals and their credentials. Provisioning new credentials, revoking credentials of departed employees and partners, and renewing credentials on a pre-determined time period are high-overhead tasks. As with any security deployment, maintaining the security of these systems and the data they contain is paramount but difficult and expensive.

The big win for any enterprise dealing with consumers doing high-value transactions is the paperless transaction. Doing reliable, on-line authentication of random consumers is not straight-forward. Likewise, neither is building out the necessary systems to issue public and private keys to consumers. The second-generation PKI systems are coming on line.

INTRODUCING TRUE CREDENTIALS®: A FULLY-MANAGED SECURITY SERVICE

True Credentials is the first second-generation enterprise security service. A second-generation security (PKI) service is one that is fully managed (i.e. outsourced) including authentication of recipients, requires no complex software at the enterprise, enables quick and easy deployment of applications, and involves very low initial investment making it possible to apply security to one application at a time in priority (ROI) order. True Credentials is deployed in production and is delivering real value to many major enterprises in all three application areas we have been discussing.

Overview and Approach

A centralized, managed security infrastructure provides the most power, most flexibility and most cost-effective options to enterprises. The system looks to the enterprise like two Web services: a management interface that provides a secure administration portal and a clean, simple operational Web interface for delivering certificates to users. The most critical aspect of a certificate-based security solution is who and how registration authority (RA) functions are performed. A fully managed security service can provide the most flexibility allowing the enterprise itself to authenticate its employees, the service provider to authenticate unknown business partners and a licensed credit bureau to authenticate consumers. Centralized infrastructure is most easily built to be substantial, robust and secure. The goal is to provision digital certificates in an efficient factory-like operation. A great deal of flexibility can also be offered in what optional application components are tied into each instance of the service. For example, one enterprise may choose to have confidential PINs delivered telephonically.

Another enterprise may require a secure time- and date-stamp notary function applied to each signed document. This is a walk before you run approach. Go for the biggest ROI first and move one application at a time.

Outsourced PKI infrastructure

With True Credentials, the big investment, specialized expertise, and expansion and centralized maintenance capability, are centralized at GeoTrust's state-of-the art facilities. It follows a simple, but secure model where all RA functions, all specialized expertise, all flexibility and maintenance are handled at the GeoTrust central facility.

Initialization and Setup

So what is really involved? It all starts with an assessment of the enterprise application most in need of security services. Careful study and planning of policies and procedures that will be needed, modifications to applications and education of the user community must proceed implementation. Typical implementations start with GeoTrust cutting a private Intermediate Certificate Authority (ICA) on behalf of the enterprise. This ICA is issued off the GeoTrust Root Certificate Authority providing the enterprise and their end users with the best of both worlds: wide spread ubiquity and private branding.

Browsers and email clients have many certificate authority root keys embedded in them when they are shipped so that individual (client) certificates signed by one of these CA roots will be automatically accepted with no unfriendly warning dialogs. The key cutting process is formal and audited and results in a live root key residing in special cryptographic hardware in a secure, radio-frequency-emission blocking facility. The managed services are configured for the proper type of authentication and for the other enterprise-specific options offered depending on whether it is for secure access, secure email or paperless transactions. The administrator designated by the enterprise is authenticated and provided a digital certificate. An HTML interface dedicated to the administrator of this enterprise is created. The user-facing Web site for delivery of digital certificates is created, optionally after co-branding with the enterprise's look and feel. Policies and procedures for key recovery (lost user certificate), revocation (fired employee) and renewal (one-year expiration) are put in place. True Credentials is now ready to be deployed.

Identity Verification

Operationally, the most critical aspect of any enterprise security service is to establish the identity of the constituents using the service. This needs to be covered in some detail to fully appreciate how these complexities are addressed by a managed service. After that, we will look at the actual certificate delivery process, and third, we will look at overall certificate lifecycle management.

Enterprise constituents break down into three groups: employees, known clients and business partners, new and unknown clients and business partners, and consumers.

Employees or Other Known, Trusted Clients and Business Partners

Identity verification per se is not the issue with known users - they are already identified, in the case of employees, by the HR department. But transferring this knowledge into practice and managing the employee credential information as employees come and go will end up being a nightmare if it is not made easy, streamlined and automated.

How to meet those requirements for employees and trusted business partners:

- The authenticated administrator presents their certificate to a special management interface creating a two-way authenticated and encrypted transmission channel and uploads changes to the list of authenticated employees as often as needed. The list includes a shared secret unique to each employee that the administrator has already communicated to each individual employee;
- The managed service processes the new list and posts emails to each new individual found therein;
- This email contains a hyperlink to the URL (the operational interface) where employees obtain their new certificate;
- Once at the operational interface, the employee provides their shared secret provided by the enterprise. If there is not a correct match, the employee is directed to their administrator to rectify;
- The certificate is created and is downloaded into the operating system certificate store using the standard built-in browser mechanisms;
- The final application requiring a certificate (browser, email, VPN client) acquires this new certificate from the standard OS certificate store.

New, unknown clients or business partners (e.g. on-line exchange, supply chain)

Identity verification is a very significant issue when the individual or business partner is unknown. Is the company real? Is the individual really an authorized representative?

These are critical facts to establish if this company is going to be brought into a trusted relationship with the hosting enterprise (as with a supply chain) or with other members of this enterprise's community (as with an on-line exchange). The managed service provider has established processes and expertise to perform business identity authentication. This is a core competency of a managed security services provider; its not core to the enterprise nor it is an easy expertise to establish.

- The names of new applicant companies are provided to the managed service provider directly from whatever enrollment process the enterprise uses or via a batch file;
- The authentication process requires the business to provide their legal business license, articles of incorporation, attestation that the individual representing the company online is authorized to do so;
- Upon successful completion of these steps, the new company and its representative are added to the repository;
- Just as with the employee process, email is then sent to the representative to receive their new certificate.

Consumers (e.g. paperless transactions)

Consumer authentication presents quite a challenge. It's a big world of consumers out there. That's both the good and the bad news. Lots of business possibilities, but lots of potential problems if a consumer is not who they claim to be. When it comes to applying a digital signature to an electronic document and have it considered as legal as an ink signature on a paper document, identity is critical. Non-repudiation is what a challenged digital signature will need to prove - that the consumer was identified and that they cannot refute that they indeed showed intent by applying the digital signature.

A tried and true way to establish the identity of an anonymous individual, such as someone on the phone or someone on-line, is to establish a set of shared secrets they have in their head. When it's someone already known but you need to tie the on-line individual to a known member in your repository, things like social security number, mother's maiden name, address, birth date are the shared secrets normally used. But when the individual has never been registered into your system, what are the shared secrets that can be used to establish their identity? One answer is the set of information in your credit file securely stored at one of the regulated credit bureaus such as Equifax or Experian. Both of these fair credit reporting act (FCRA) regulated firms have an on-line credit-file-based authentication solution that can be integrated into the managed service providers offering.

The paperless transaction process for a consumer, when it is time to establish who this consumer is, must smoothly transfer over to the credit bureau (who must directly control the process due to federal regulations). The consumer is told they will be dealing with Equifax under the FCRA and that credit data will be used for shared secrets confidentially. The consumer will be asked multiple choice questions such as who is their mortgage provider, what is their car payment.

The end result is a score (probability that this person is really who they say) provided back to the managed service provider. If the score meets the criteria established by the hosting enterprise, the certificate is issued on behalf of the consumer. Usually the certificate is for digital signing and the certificate is single-use only so it goes directly into a signing application and is never seen or managed by the consumer.

Certificate Delivery and Lifecycle

After the individual has been authenticated - be it employee, partner or consumer - the certificate that gives them a digital identity must be delivered to them. They receive an email with an HTML link in it that takes them to a page at the managed service provider (Figure 7) . This page can be branded identically to the look-and-feel of the enterprise's pages for consistency. The certificate is delivered to the user's browser. The browser is the standard way to get a new certificate into the operating system's certificate store.

Certificates nominally have a lifetime of one year. At that time, they must be reissued to keep that individual credentialed. This means the managed service provider must keep careful track of all active certificates and just prior to their expiration, their owner must receive an email notification to renew. Prior to the automatic renewal time two things can occur that require active participation by the managed service provider. Individuals lose certificates. That can occur if they forget the password they created to activate their own certificate when they imported it into their machine. Or, they may have lost their machine completely. In this case, they need to get a new certificate - a process that must be supported through the operational interface. If the individual is an employee who is fired, their certificate needs to be revoked.

Revoking a certificate makes it invalid for any purpose whatsoever. It is the responsibility of the enterprise administrator to quickly revoke a certificate. And it is the responsibility of the managed service provider to provide both a mechanism the administrator can use and an up-to-date list of revoked certificates back to the enterprise.

We have explored the True Credentials second-generation enterprise managed security service and the applications it enables. Now we will describe the infrastructure behind True Credentials that make it secure, scalable and available.

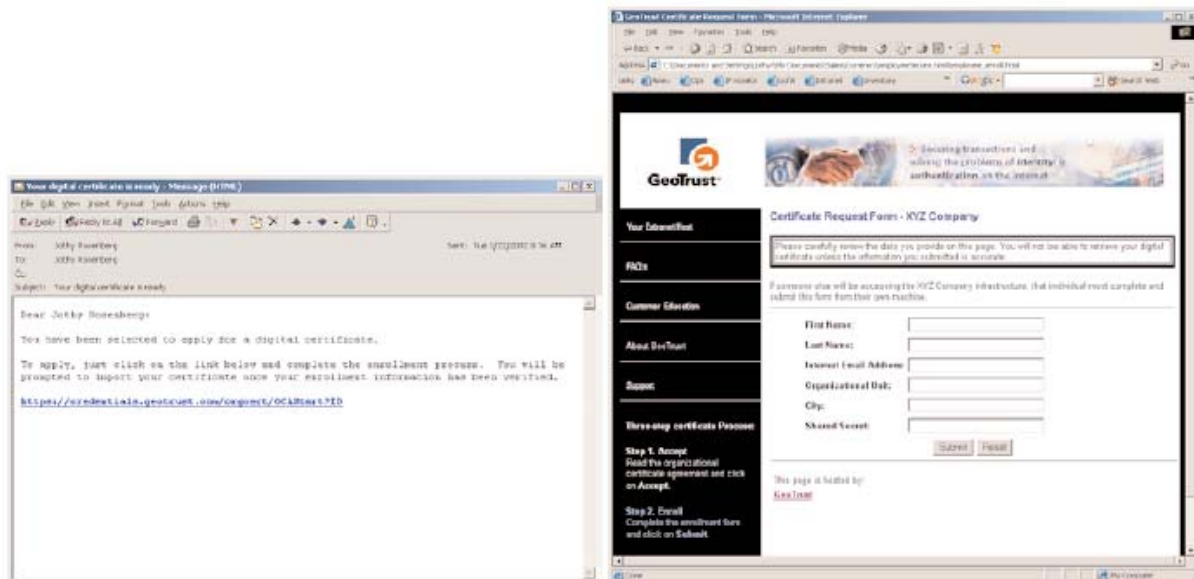


Figure 7

GEOTRUST EXPERTISE AND PRODUCT PERFORMANCE

GeoTrust leverages many years of experience, patented technologies and significant customer deployments. State-of-the-art, audited security systems and processes are deployed throughout the managed service. All systems are built to be redundant for high availability and are carefully architected for full Internet scalability.

A Complete Line of Tested and Proven Security Products

GeoTrust's comprehensive array of managed services technologies enables organizations of all sizes to secure online identities for people, devices and applications, and include:

Web Security Services offer hosting providers and businesses with world-class digital certificates for fast transaction security and patent-pending 'smart seals' to ensure a trusted identity on the Web.

Enterprise Trust Services offer fully-managed security services for large enterprises. This next-generation PKI technology safeguards network access, online communication and digital transactions - and offers the kind of powerful competitive advantage every organization needs.

Identity Verification Services ensures the identity of business entities and/or individuals in online transactions. GeoTrust products also validate website identities, instilling confidence in consumers and boosting online sales.

Signing Technologies represent the latest in next-generation services for digitally signing applications, binding people and documents, and assuring code integrity to wireless platforms. These services span both document signing and code signing.

The Enterprise Trust Services portion of GeoTrust's business (the topic of this paper) has resulted in the delivery of tens of thousands of individual client certificates so far. A selection of major True Credentials deployments include:

- Secure access for 30,000 remote employees of a F50 computer manufacturer replacing \$55 per person SecureID tokens;
- Secure access for a major credit bureau for its known business partners to access consumer credit files prior to offering loans replacing expensive dedicated leased lines;
- Secure messaging (email) for 130,000 employees of a F50 computer manufacturer;
- Paperless transactions for a top-5 international term life insurance firm; the first to offer completely on-line, paperless term life applications to consumers;
- Paperless transactions to implement the UK government's tScheme initiative that will have all UK businesses eventually submitting all tax documents on-line.

Airtight Physical and Network Security

Enterprises who utilize True Credentials to maintain the systems, network and their data using the best possible physical and network security. Buildings are staffed twenty-four hours per day, seven days per week. All employees and visitors are required to wear access badges. All systems and access doors are under constant video surveillance. Access to the most secure systems require two employees to access biometric entry devices simultaneously. The certificate management computers with associated hardware cryptographic devices reside in a Radio Frequency (RF) Enclosure built to stringent National Security Agency TEMPEST standards. Private keys cut for enterprises are divided into N distinct parts - controlled by N of their company executives - and stored in separately locked boxes in a fireproof vault. All computers and peripherals are powered by uninterruptible power supplies with powerful battery backups that can be indefinitely re-charged by diesel generators.

Network security is equally important. All systems are protected by multiple layers of firewalls. All software systems are kept up to date with manufacturer updates and patches. State-of-the-art virus checking systems are run on all systems. Intrusion detection software protects the networks. The multiple security zone configuration known as DMZ is used extensively to limit exposure and provide sufficient response time if a breach should occur. Independent security auditors have carefully scrutinized the physical systems, the software configurations and the processes and procedures used by all personnel associated with the managed service.

Scalability and Availability

True Credentials must be prepared to handle success. It must scale as more and more enterprises endorse the outsourced approach to digital credentials. Scale is achieved through three architectural principals: automation, replication and processing out at the edge of the net. Automation has been heavily used to create a self-help site for administrators. Provisioning of certificates to individuals proceeds like a highly automated factory. There is no human intervention unless something goes wrong. Email and another self-help site automates the interaction with the certificate recipient. True Credentials leverages the Web standards to help achieve scale and best possible performance. It uses Java (J2EE) for all server components. These components can be replicated because they are independent from all other servers. Load balancers are then applied to replicated servers providing excellent scalability. Wherever possible, True Credentials leverages all possible capabilities already built into the edge of the net. Browsers operate at the edge of the net, already know how to upload certificates, and know how to use certificates to securely access restricted Web servers.

Without fail, a managed security service must have continuous availability. Redundancy is fundamental to high availability. Servers, databases, firewalls, routers, switches, even network connections and power supplies must all be redundant to achieve five 9s (99.999%) availability (down at most five minutes in a year). There is no single point of failure as shown on the network diagram shown in Figure 8. In practice this is providing True Credentials with the five 9s availability enterprises seek.

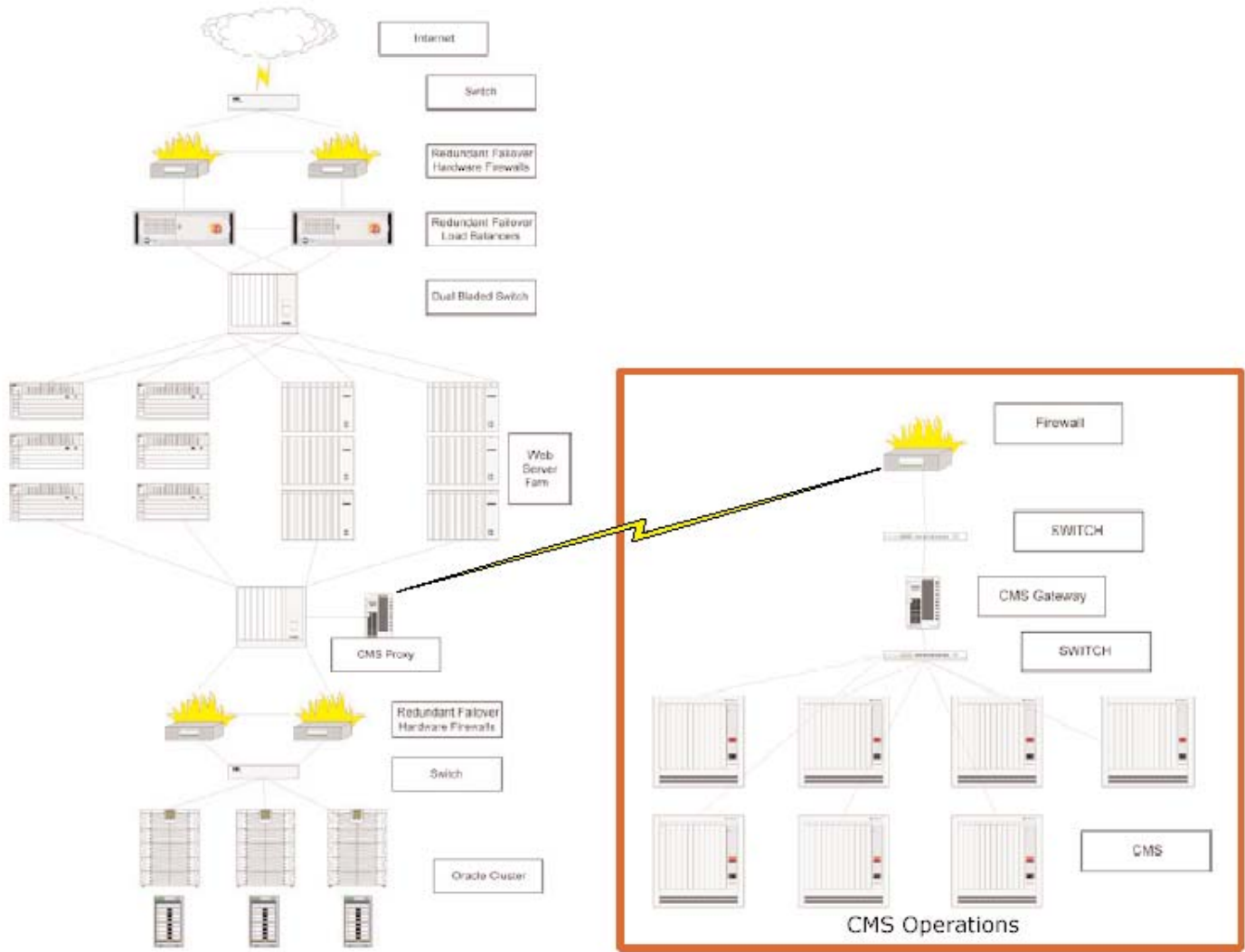


Figure 8

CONCLUSION

Most people's first thought when considering the application of security to existing applications is about reducing risk or costs. But because security credentials enable completely new capabilities not possible otherwise, all three of the application areas we have been discussing offer new revenue possibility. Certainly there are significant opportunities as well to reduce costs especially in the secure access category. Replacing dedicated leased lines or SecureID tokens provides a ripe opportunity to reduce costs by at least an order of magnitude. It is also intuitive that applying secure credentials to existing applications can reduce risks especially if they are replacing a simple password scheme. But the risks of open communications using email are huge when the content includes business critical or intellectual property secrets. Thus, applying secure credentials to close down the risk of open email within and outside the enterprise is compelling.

Overall, it is paperless transactions that provide a glimpse of the future. This is all about opening up completely new revenue possibilities. It actually represents a potential structural change in many industries. The first in each segment will have a significant advantage because of the network effects the Web has delivered time and time again. That's because paperless transactions will frequently involve consumers. Consumers seek convenience and speed as long as they are comfortable with the on-line experience. If they are, they will come in droves to the first to deliver real value, real time, real safe.

Choosing the True Credentials fully managed enterprise security services accrues benefits to the deploying enterprise quickly. True Credentials is the first fully managed security service implemented as an "automated factory" that issues secure credentials for an enterprise's constituents: employees, business partners, clients and other users. True Credentials are electronic security credentials provided to authenticated individuals that use the enterprise's mission-critical networked applications. This second-generation managed service approach allows the enterprise to deploy one newly secure application at a time with no complex software onsite and no specialized talent needed while accruing significant benefits, quickly, easily and cost effectively.



6 Kings Row, Armstrong Road,
Maidstone, Kent, ME16 8NF, UK
E-mail: info@geotrusteurope.com
www.geotrusteurope.com