The Biometric Solution to Digital Security

"Bio-PKI"

Enterprise "Biometric PKI Network Solution"

Ezra Hedaya
Ezra@indexsecurity.net

Eli A. Safdieh
Eli@indexsecurity.net

Index Security
500 Parker Avenue, Suite "G"
Deal, New Jersey 07723-1435
Phone: 732- 531-9209 Fax: 732-531-2307
Toll Free in USA: 866-INDEX89 (866-463-3989)
www.index-security.com
info@index-security.com

Index Security Inc. is a biometric company with supporting security products. We are devoted to introducing simple, durable, cost effective, and user-friendly security solutions with an acute focus on our customers.

Index Security is a CCR & Pro-Net Registered Company
D&B#:134622831; Cage Code:3HXP1; NAIC Codes: 334119,421430, 421610,541519

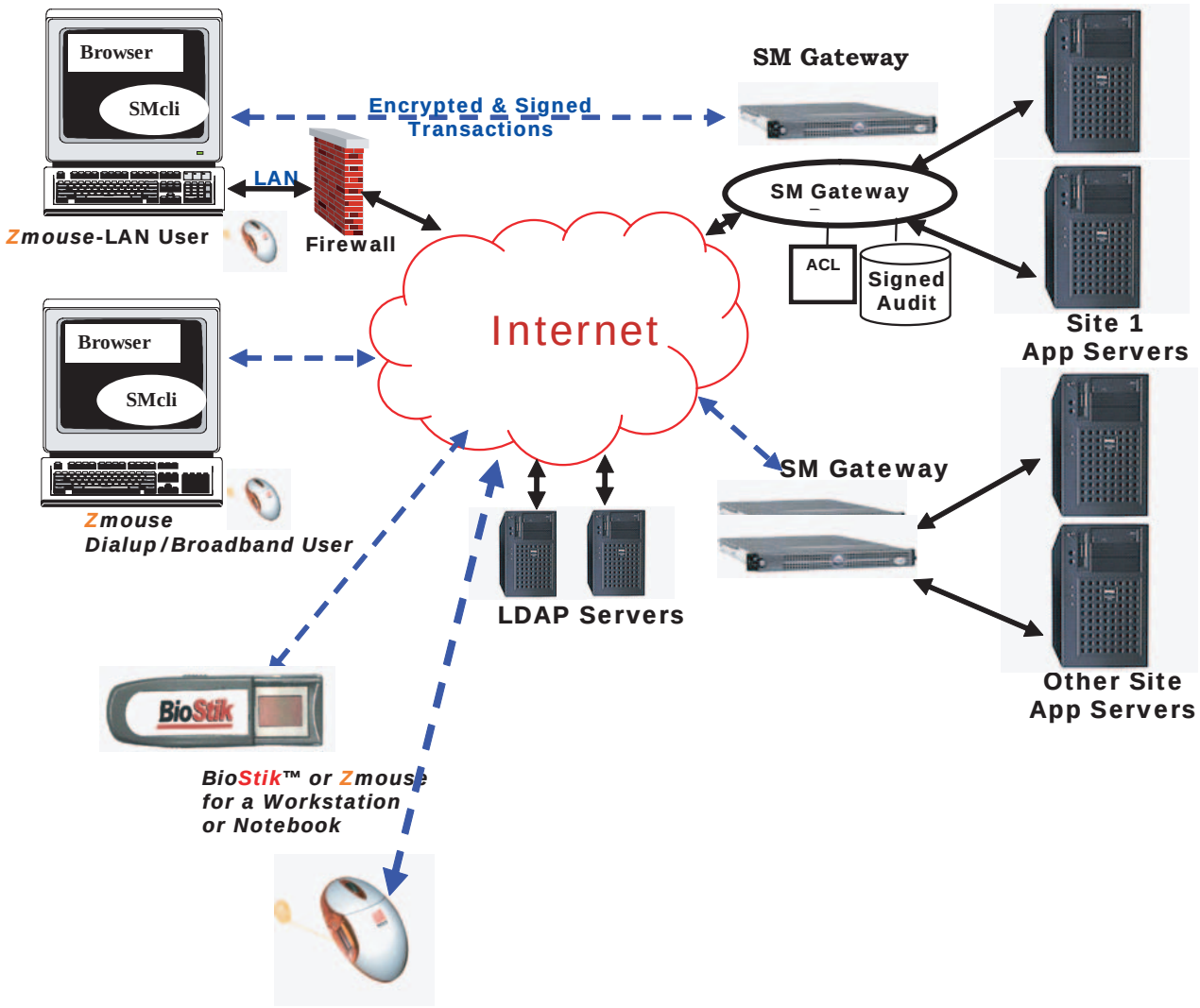
Printed 8/2004 V-1

INDEX™ SECURITY

The Biometric Solution to Digital Security

"The Next Generation of Security"

Biometric PKI enabled Network Solution



Using the ***BioStik***™ with SecureMethods PKI solution; data is biometrically PKI secured and eliminates passwords by the user at the same time insuring identity.

Triple Factor Authentication- Bio PKI

INDEX™ SECURITY

The Biometric Solution to Digital Security

"Bio-PKI Enterprise Network Solution"

Objective

- Role Based Single Sign-on
- Strong Authentication and Secure Audit
- Compartment Mode Authorization
- Rapid Deployment Scalability and Low Cost
- Transparent Support for Multiple Applications

The Bio-PKI Solution mentioned is an appliance based mechanism to grant your users biometrically, digitally signed and encrypted, remote access to servers via the web and at the same time leave a complete audit trail of transactions, file accesses, including who, what, when, where, and how they did it. For a very long time this kind of solution was only talked about in theory, now Index Security with SecureMethods has made it a reality. Further, a single appliance can seamlessly provide this level of security for multiple application servers without the need for modification.

We, Index Security Inc, and SecureMethods Inc. have established a close partnership to offer an Enterprise "Biometric PKI solution" using Index Security products like the BioStik™(www.biostik.com), or the Zmouse and IZzy devices for workstations (www.index-security.com). We can control your servers' access for all applications, files, downloads and audit all transactions with the utmost security using a PKI server/client application that can be launched by our BioStik™. Biometric- PKI - enabled for a whole secured network solution...especially the web. This gives answers as to how to leave all data on your servers and still monitor when data is securely accessed or needed to be downloaded for off site use. Using the BioStik™ with SecureMethods solution; data is biometrically PKI secured and eliminates passwords by the user at the same time insuring identity, especially when offsite.

SecureMethods specializes in the design, implementation, and deployment of advanced secure network applications for commercial and Government clients -- including classified DoD. SecureMethods provides a comprehensive, scalable, COTS-based secure architecture, implemented through the use of SM Gateway. SM Gateway is available on UNIX-based platforms using commercial, Government, and Type I cryptography, implemented in both hardware and software. The PKI and company information is on their web site at www.securemethods.com . They will be using our BioStik™ Zmouse and IZzy to carry their user credentials, thus making a biometric PKI solution a reality. Their solution is hardware based with gateways and supporting software. As implementation of the system is transparent to both users and application servers, deployment is fast and cost effective.

The ultimate combonation for true Identity to your network

INDEX™ SECURITY

PROTECTED BY Secure methods

Revised 8-2004-EJH

INDEX™ SECURITY

The Biometric Solution to Digital Security

Which Government Act effects you?

Graham Leach Bliley Act

Over 238,000 firms are governed by seven federal agencies auditing GBLA compliance

Regulation could easily extend to ANY organization handling non-public information

Independent Bankers Association - $21-43 Billion cost

First rounds of audits have begun … heavy fines and jail time (board level) for non-compliance

Sarbanes Oxley Act

Impacts all public companies – 14,000

Compliance has been postponed for year

Projections vary

- AMR Research - $ 2.5 billion spending 2003
- Enterprise Storage Group - $6 billion in four years

HIPAA

Health care and insurance providers impacted

Major privacy provisions deadlines April 15, more to come … penalties to $50K and jail time

Estimates of market size vary

- American Hospital Association - $22 billion cost
- Blue Cross - $47 billion cost

USA Patriot Act

USA Patriot Act is anti-terrorism legislation has strong money laundering impact

Eventual projections vary

- TowerGroup - $700mm for brokerage firms alone
- Citigroup & Merrill Lynch expected to spend $30mm

Related regulations like the Anti-Money Laundering Act (AMLA) add more requirements

Security Levels with BioStik and SecureMethod "An Enterprise Bio-PKI Solution"

Configurable and secure for a wide range of applications and access policies:	Rank	Secure Level	Encryption
– Encrypted token based digitally signed biometric transaction	Best	10	STL
– Encrypted token based digitally signed transaction	Better	6	STL
– Encrypted digitally signed transaction	Better	5	STL
– Encrypted one time password session	Good	4	SSL or VPN
– Encrypted password session	Good	3	SSL or VPN
– Password session	Fair	2	
– Public	Risk	1	

The Solution

SecureMethods Embedded PKI secures transactions using a robust new architecture. It overcomes the limitations of PKI and SSL by providing the level of security appropriate to each organization and each transaction.

Index Security and SecureMethod's Bio PKI Network Solution provides a complete transaction based triple factor authentication with a DOD grade security level; which ensures secure, encrypted, audited, digitally signed access --

Easy to deploy, cost effective and without individual client licensing charges.

Revised 6-2004-EJH

INDEX™ SECURITY

The Biometric Solution to Digital Security

"Enterprise Bio-PKI Network Solution"
Security Levels for Accessing the Network.

Index Security and SecureMethod's, Bio PKI Network Solution, provides a complete transaction based triple factor authentication, DOD grade security level infrastructure; which ensures secure, encrypted, audited, digitally signed access.
Easy to deploy, cost effective and without individual client licensing charges.

Distribution PKI Security Levels within your Network

Organizations now require a low-cost, easy-to-deploy PKI solution that provides the increased level of security required to operate safely in today's complex threat environment.

For Top Management or where a Legal binding signature is required:

The Best- Triple Factor Authentication- Encrypted token based digitally signed biometric transaction.

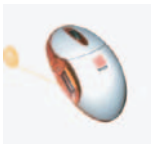
For Company, Agency Personnel and Associates:

Better-Encrypted token based digitally signed transaction-

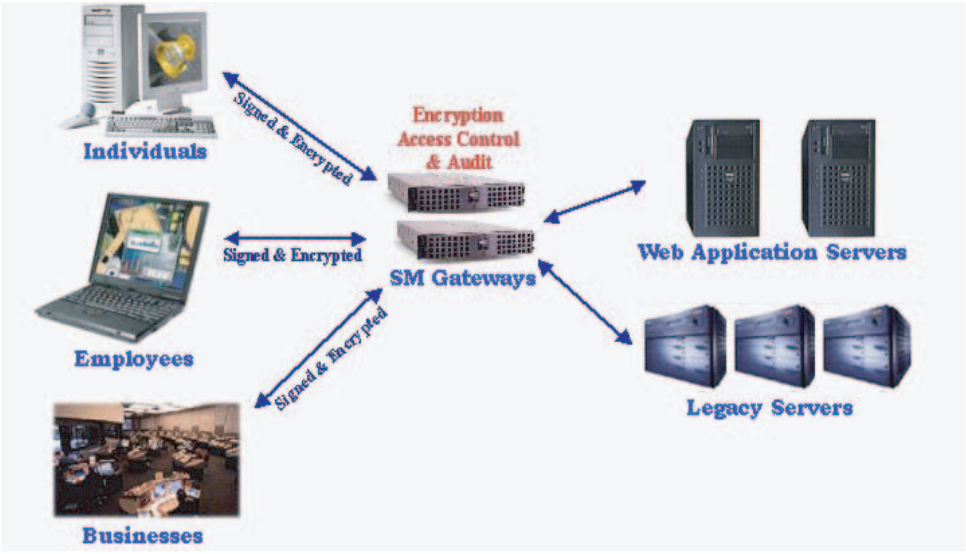
For anyone using the Network:

Good-Encrypted digitally signed transaction-

Biometric PKI Enablers



Bio-PKI Network



SecureMethods PKI Solution provides a low-cost, easy-to-deploy embedded PKI infrastructure that allows organizations to create the highest level of security possible. SecureMethods provides encryption, authentication, authorization and audit capabilities for all transactions. In addition to providing these benefits, SecureMethods also eliminates the need for passwords while protecting you from the problems inherent in IIS and Windows™ server flaws.

INDEX™ SECURITY

The Biometric Solution to Digital Security

Benefits of Index Security Bio PKI Technology
How True Identification Can Increase Profitability with Biometric PKI Solution!

- Triple Factor Authentication with a legal binding Digital Signature
- Complete Audit trail -Track every user on the Network by each transaction, not by a session
- DOD grade security
- Free SM Client without constant client licensing charges.

Index Security and SecureMethods "Biometric-PKI Solution" can have a positive impact on your bottom line, whether you implement our solutions for business-to-consumer e-commerce, business-to-business e-commerce, or internal corporate data and applications. The BioStik™ can be used for your mobile needs and the Zmouse at your workstation assures fingerprint verification to your SecureMethods PKI protected network. Here are the key areas where our solutions affect profitability using the BioStik and SecureMethods PKI solution.

- **Protection against data loss: Using the BioStik with SecureMethods solution; data is biometrically PKI secured and eliminates passwords by the user at the same time insuring identity. When you integrate biometric technology into your applications, your employees, customers, or business partners no longer need passwords, cards or tokens that can be exchanged or stolen. Your proprietary data is more secure when protected by biometrics.**

- **Lower administration costs: Once users register their fingers in Index Security fingerprint device, no ongoing administration is necessary. Unlike passwords, which require regular updates and changes, fingerprints are good for life**

- **Lower support costs: Index Security fingerprint verification systems eliminate help desk calls for forgotten passwords or PINs. (A national survey showed that help desk calls for forgotten passwords cost $150 to $300 annually per person for every person on the system.**

- **Protection against fraud: With Index Security fingerprint verification devices and SecureMethods PKI solution, there is no question to the identity of your buyers, associates vendors and even customers. Sensitive information is protected from the LAN to over the Internet.**

- **Consumer confidence: Although many individuals participate in Internet Data Exchange and Commerce, many more are afraid because of discomfort with security levels. The superior security provided our Biometric PKI technology increases consumer confidence and helps you get and keep customers. Your information is secure!**

- **Signature guarantee: If you accept digital signatures or e-sign, can you be sure that the signature really belongs to the party using it? BioStik with SecureMethods can be employed to guarantee digital signatures.**

- **Speed! Our algorithm identifies users in 1 seconds or less, regardless of user network size. This makes our BIO-PKI solution an ideal security solution for companies both large and small.**

- **PKI Flexibility. Our technology works with either PKI keys or any biometric reading devices.**

- **Highly accurate. The performance rate of our finger identification algorithm reaches far beyond industry standards**

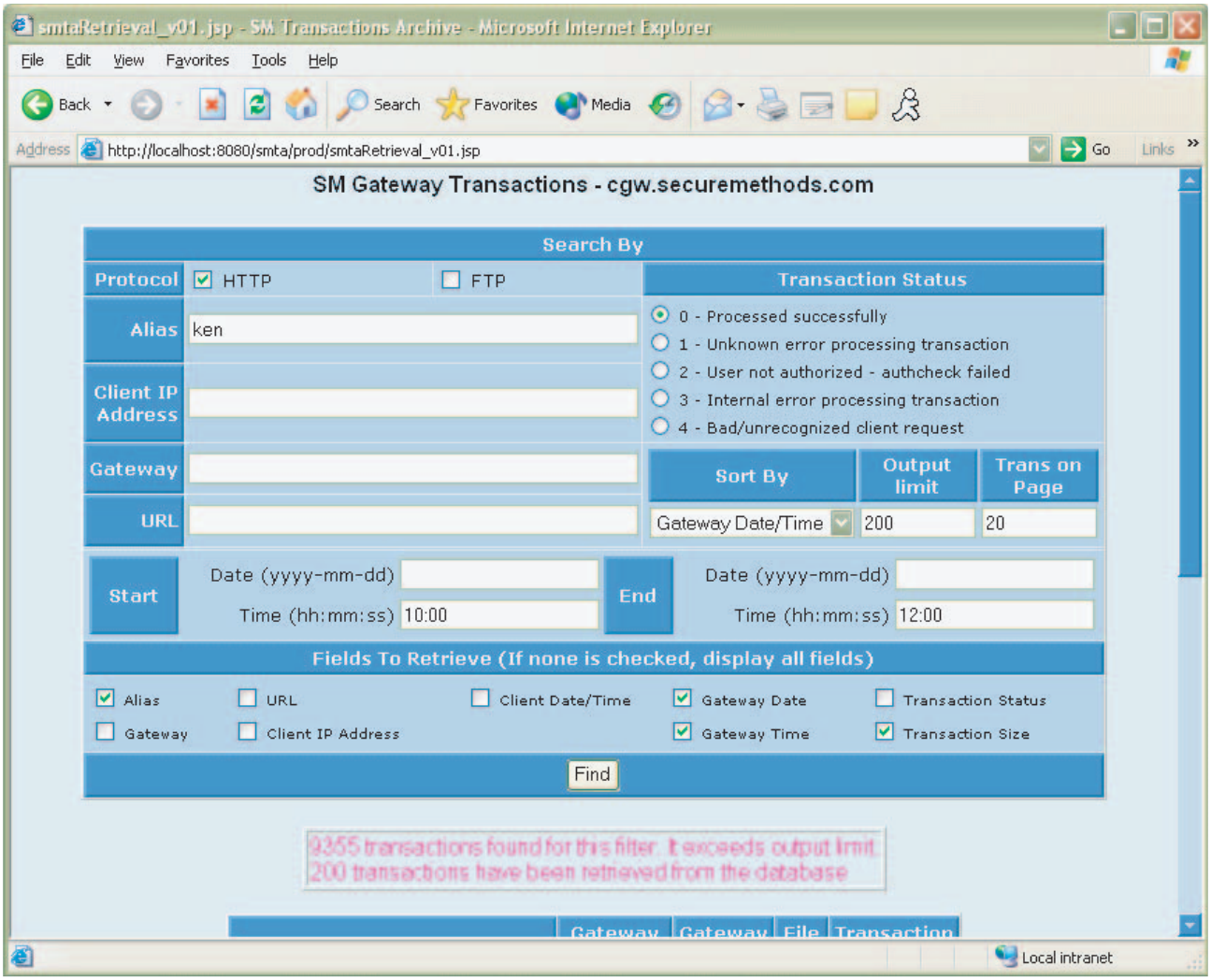
- **Accountability. Audit trail of transactions, file accesses, including who, what, when, where, and how they did it.**

INDEX™ SECURITY

The Biometric Solution to Digital Security

Audit trail Application

A complete audit trail of transactions, file accesses, including who, what, when, where, and how they did it.



The Biometric Solution to Digital Security

Enterprise "BIO PKI Network Solution"
Demo together with Index Security and SecureMethods

Basic instructions for the PKI demo for evaluation
If you wish to see how easy our PKI is to use; the SMclient may be downloaded at no charge from http://www.securemethods.com/SMClient.exe. When prompted, check the Demo client to download. Install client and restart computer. Go to the test page: http://demo.securemethods.com>.

Test 1 - PKI --> Two factor Verification test:
With the demo registration installed, it will provide protected (digitally signed, encrypted and audited) access to Go to SM Gateway Protected Applications and test the links.

Test 2- BIO PKI > Three Factor Verification test:
To demo the Bio-PKI solution you must have a BioStik™; (If you need a sample, please visit the web site at: www.biostik.com;)

1. Enroll your fingerprints onto the BioStik .
2. Once the demo registration SMclient is installed, you can right click on the icon in the system tray; go to "Configure SM Client, and "Move Registration" to move the client PKI to the BioStik™, thus protecting your credentials and having a "Biometric PKI" enabled secured solution.
3. Unplug your BioStik™ and restart your computer one last time.
4. Congratulations! You are all done; Please note access to the following will only be available after you plug in your BioStik™ and authenticate yourself; to test your access to the STL test link: SM Gateway Protected Applications or STL file access with web folders

With your SM PKI credentials protected and stored on the BioStik; your fingerprint becomes the enabler for "Triple Factor Authentication". All accesses are verified, individually digitally signed, FIPS140 encrypted, authorized, and audited.

Test 3 - STL file access with web folders
To access the STL web folders demo:
(for Windows XP and 2000)
1. Open My Network Places
2. Double click Add Network Place
3. Enter the location http://webfs.securemethods.com/demo. Enter a name for this web folder and click Finish
4 Go to http://webfs.securemethods.com/demo to drag and drop test files to your desktop.

For your information on Encrypting, Digitally Signing & Sending Secure Email:
Right click on any file and go to the "Lock" option in order to Encrypt & Digitally Sign it. Now you also have the ability to send it via email securely.

Please let us know if we can be of further assistance at 866-463-3989, or you can e-mail directly to support at support@securemethods.com <mailto:support@securemethods.com>. Their experts will quickly help you accordingly.

INDEX™ SECURITY

Biometric Secured Flash Storage

BioStik™

Secure and protect your personal data...

...keep out unwanted users with individual fingerprint identification!

NO SOFTWARE Needed!

Multi-platform

USB

- It Reads your fingerprint.
- Flash Memory... with Individualized Access Only!
- Just plug into any USB, and be operational. NO SOFTWARE Needed!

BioStik is a portable storage Flash Drive combined with Biometric fingerprint-scanning Technology for a Secure way to Transfer, Store, & Transport your information.

Typical Applications for Storage of sensitive, confidential, private information or data files:

- Finance & Banking
- Insurance
- IT Security
- Medical Records
- Corporate Data
- Personal Files
- CAD Files
- Multimedia Presentations
- Accounting Data
- Pictures

- "Administrative Feature" (Black casing)

The 2 first fingerprints enrolled are permanent, for overide ability and deployment control.

128 MB
256 MB
512 MB

USB Flash Storage Capacity

BioStik 128 MB product # BSK-M-128-V1-Black
BioStik 256 MB product # BSK-M-256-V1-Black
BioStik 512 MB product # BSK-M-512-V1-Black

INDEX™ SECURITY

Biometric intelligent security system

BioStik™

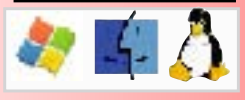
USB Secured

128 MB
256 MB
512 MB

Storage Capacity

NO SOFTWARE Needed!

Multi-platform



USB

Compatible with:

- Windows® XP
- Windows® 2000
- Windows® Me
- Windows 98
- Mac OS 8.6 & up
- Linux 2.4x

Easy as 1,2,3

1 Insert *BioStik*™ into USB port NO Software needed

2 Scan fingerprint to access your *BioStik*™ flash drive

3 Transfer your information onto your *BioStik*™ and remove

The Best way to secure your Data.

Carry your *BioStik*™ containing your stored information securely.

CE FC

SPECIFICATIONS:

- USB 1.1 (includes USB Cable)
- Data Transfer Speed: (Read/Write) up to 900kb/s
- Dimensions: (L) 3 " x (W) 1 " x (H) 1/2 "
- Weight: .95 oz
- Sensor: Capacitive
- Certification: FCC, CE
- Cross platform

"Administrative Feature" (Black casing)

The 2 first fingerprints enrolled are permanent, for override ability and controlled deployment .

- Biometric Secured Portable Storage Device
- 6 Fingerprint enrollment and verification for Black BioStik Units (5 for Gray Basic)
- Scans your finger in less than 1 second
- * Hot "Plug & Play"- Software free
- Cross platform, can go from any of the supported operating systems.
- USB 1.1 (includes USB extension Cable)
- Small & easy to carry around with protective covering
- Includes neck strap for carrying device
- Biometric security ensures you are the only one who accesses your information.

INDEX™ SECURITY
500 Parker Avenue , Suite "G"
Deal, New Jersey 07723-1435
Phone: 732- 531-9209 Fax: 732-531-2307
Toll Free 866-INDEX89 (866-463-3989)
www.index-security.com

from the Technology-makers at...

INDEX™ SECURITY

BioStik™

Multi-platform

NO SOFTWARE needed!

Why *BioStik*™ ?

- NO SOFTWARE NEEDED!
- Secured data storage with fingerprint verification
- Multi-OS Platform Capable
- Hot Plug and Play
- Tamper proof flash memory
- Easy to use!

BioStik™ is a portable flash memory storage device combined with biometric fingerprint-scanning technology for a secure way to transfer, store and transport your information. The BioStik™ reads your fingerprint in less than 1 second for individualized access to your sensitive or confidential information and data files. No passwords used. Simply plug into your USB port, authenticate your fingerprint, and the removable hard drive on your PC becomes available for file storage. Just "Drag and Drop" your files. Transporting and securing data has never been so mobile and efficient .

Easy as 1 2 3 4

Insert *BioStik*™ into USB port
NO Software needed

Scan fingerprint to access
your *BioStik*™ flash drive

Transfer your information
onto your *BioStik*™ and remove

Carry your *BioStik*™ containing
your stored information securely

As reported in:

FCW.COM

Friday, April 9, 2004 Issue
Portables sizzle at FOSE
Tablets, handhelds expand in new directions
BY Michelle Speir April 5, 2004
http://www.fcw.com/fcw/articles/2004/0405/tec-fose-04-05-04.asp

BioStik

If you regularly use different computers in different locations, a portable flash memory device makes it easier to take your work with you. One problem with this type of device, however, is that it's relatively easy to lose due to its small size. And if the data is not protected, anyone who finds the device could access your files. This is where the BioStik from Index Security Inc. comes in. It protects your data with a fingerprint, which, unlike passwords, can't be forgotten or hacked. The fingerprint scanner is integrated into the unit and protected with a plastic cover when not in use.

The USB 1.1 device is available with 128M of memory, but a 256M version will be released soon. The 128M BioStik sells for $170. Information is at www.index-security.com

The SecureMethods Legal_ID™ Solution

Legal_ID

The Business Need

In the practice of law, constantly evolving documents and contracts must be shared and signed by multiple parties located in multiple places. Electronic digital signatures make it possible to easily and securely conduct these private electronic business transactions using the Web and e-mail. Today, large and small law firms alike require a digital signature solution that is painless, cost-effective and easy-to-use.

The SecureMethods Legal_ID™ Solution

SecureMethods Legal_ID™ is an easy-to-deploy embedded PKI solution that enables digitally signed and fully auditable transactions without any user intervention or business process changes. The SecureMethods Legal_ID™ solution is unique in its ability to significantly reduce the cost of deployment and increase the ease-of-use of advanced security.

Perhaps most importantly, the solution seamlessly protects the integrity of documents and end-user applications; and it seamlessly integrates with existing security measures.

In addition to providing a complete digital signature solution using the most secure user credentials, Legal_ID™ also provides encryption, authentication, authorization and audit capabilities for all transactions. Unlike other solutions that only provide digital signatures for each session, Legal_ID™ digitally signs each transaction to provide the highest level of security possible.

The SMart choice for information security

secure methods

Legal_ID™ Solution

The SMart Digital Signature Solution

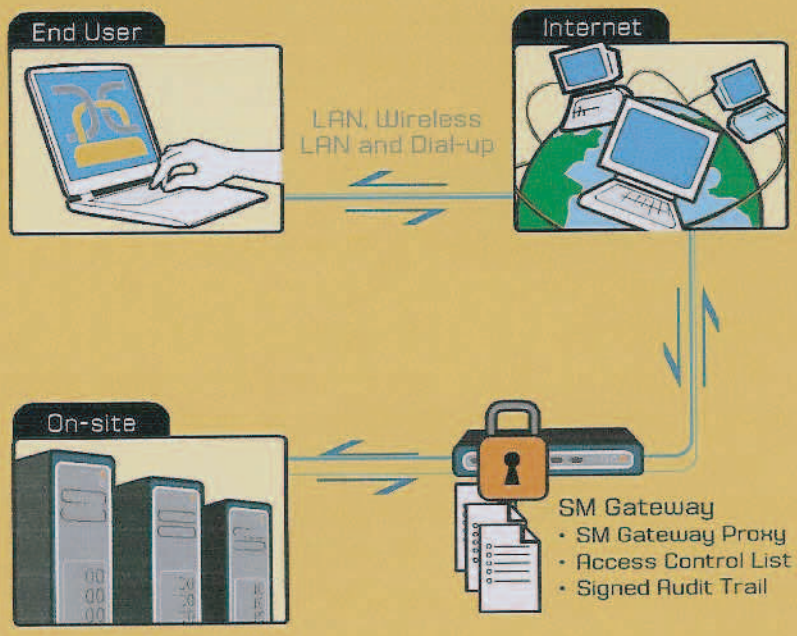
Legal_ID™ ensures people are who they say they are and protects documents from forgery, corruption and repudiation.

Whether you want to implement a basic digital signature capability, or to provide a sophisticated token or biometric solution, SecureMethods can help you get there quickly and easily. The system interfaces with any USB-capable device.

The SecureMethods Legal_ID™ solution:

- » is transparent and easy-to-use
- » integrates with legacy and custom applications
- » is approved for top-secret intelligence data
- » conforms to the Digital Signatures Act of 1999
- » handles co-signature transactions
- » increases efficiency by reducing paperwork, travel and delays in processing and delivery costs
- » reduces possibility of fraud, forgery and impersonation
- » provides enforceable proof of access
- » offers automated security management tasks which ease administration

The advanced security features of the SecureMethods Legal_ID™ solution are transparent to the user, requiring no change in user behavior. All transactions from the user through the Internet to the SM Gateway and ending at the remote application are authenticated, authorized, encrypted and digitally signed, enabling a legally-enforceable audit trail.



Success Story - Cahn & Samuels, LLP

"SM's LegalID™ solution allows us to provide our clients and partners with digitally signed and encrypted documents, ensuring the integrity of our sensitive information traveling over the Internet. Digital signatures not only offer convenience but they are also legally-enforceable and improve security practices.

The solution was installed and running in just a couple of hours and we didn't have to train our staff to use it or recode our legacy apps."

BioStik™ is an Index Security product, used to verify the users ID with a fingerprint. Index Security provides the ultimate in data sharing security with SecureMethod's Enterprise Solution.

www.biostik.com or www.index-security.com

866-463-3989 govsales@biostik.com

The ultimate combonation for true Identity to your network

from the Technology-makers at...

INDEX® SECURITY

PROTECTED BY secure methods

SecureMethods for Highly Secure Digitally Signed Transactions

SecureMethods Benefits

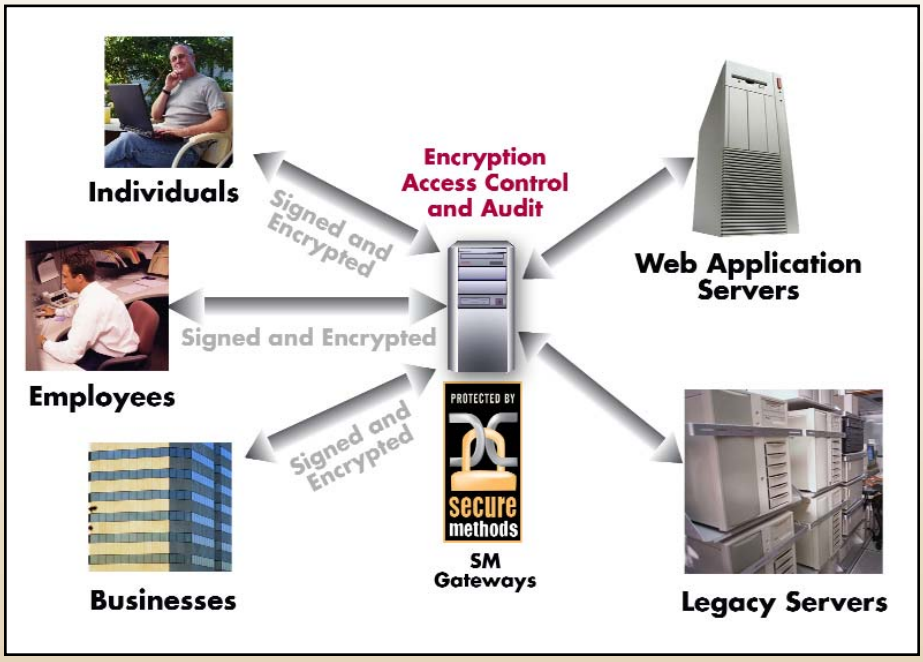
Using SecureMethods, you can:

- Provide legally enforceable, auditable digital signatures for each transaction, not just a session
- Assure that each transaction includes strong encryption to ensure privacy
- Provide an embedded PKI capability for comprehensive security and easy deployment
- Easily protect e-commerce servers and desktops
- Secure e-mail and desktops without creating a breach in firewalls

SecureMethods overcomes the many limitations of existing security solutions by making it easy and safe to implement transaction-level security without requiring an expensive PKI implementation or making the end user become a "security expert."

SecureMethods is an easily deployed, transparent transaction-level security solution for high value web-based applications.

SecureMethods' unique architecture provides strong security without requiring any action or intervention on the part of users or system administrators because it runs below the browser and on the edge of the network. The result is a transparent, easily deployed environment that is highly flexible and secure.



How SecureMethods Works:

SecureMethods' patented technology protects critical information by delivering a security solution that is all encompassing, particularly when compared with competitive solutions that are more expensive and typically address only a single area of vulnerability.

SecureMethods consists of two components; a gateway appliance component and a client component that runs in the system tray on the desktop. The SM Gateway enables users to authenticate, authorize, audit, digitally sign, and encrypt transaction data in a legally enforceable manner.

SecureMethods Features:

- Flexible Secure Remote Access via Internet, Leased Line, Broadband, Dialup, and Wireless
- Group and user Access Control by application and URL utilizing embedded PKI digital signatures
- FIPS 140 and Classified DoD Certification at the highest security levels
- Support for Commercial and Government cryptographic algorithms
- Insurance of $100,000 per transaction
- Full audit capabilities at the transaction level
- Ease of use and management
- Seamless integration and deployment
- Digitally signed transaction audit and archive
- Eliminate the need for easily compromised passwords

Utilizing no-cost client software, users can transparently add digital signatures and strong encryption, authentication, authorization and audit services to fully secure all e-business applications. In addition to securing transactions, SM Gateways also provide a level of protection and access control for organizational resources not possible with existing VPN, Firewall, and SSL web technologies.

Ongoing Support & Training

- Tier 1 & 2 level support that includes both remote and on-site support
- Administrative training
- Help Desk
- User registration
- On-site configuration and implementation
- Secure remote administration
- Secure remote system upgrades

Interoperability

- Works across disparate wired and wireless networks
- Interoperable Encryption and Digital Signature for Web, Email, and Desktop
- Interoperable use of Smartcards, Memory keys and Biometrics
- Interoperable with current security applications including firewalls and VPN's
- Compatible with Linux, Solaris, Microsoft and other platforms
- Provide additional security for sites already using VeriSign or Entrust

SM Certificate Authority (CA)

SM Hosted Secure CA Subscription
SM CA Server
Secure remote issuing of X.509 user credentials

Additional Information

For additional information on how SecureMethods can ensure that your business initiatives are operating at the highest level of security visit our web site at **http://www.securemethods.com** or contact us at **sales@securemethods.com** or call us at **703-628-9500**.

secure methods

703-628-9500 or sales@securemethods.com

www.securemethods.com

SecureMethods Embedded PKI™
the Next Generation Security Infrastructure

Secure Methods, Inc.

224 West King Street
Martinsburg, WV 25401-3212
http://www.securemethods.com

SecureMethods Embedded PKI™:
The Next Generation Security Infrastructure

U.S. Patent Pending

Table of Contents

Next Generation Security Architecture – Key Issues 1

How the SecureMethods Architecture Works 3

SecureMethods Architecture Capabilities 6

SecureMethods Security Services 7

Architecture FAQ 9

Summary 11

The Next Generation Security Architecture

Key Issues

Traditional information security approaches such as passwords and user ID's are of dubious effectiveness in many organizations because of inherent weaknesses and reliance on the human factor to make them work. To overcome the limitations of these approaches, many companies have attempted to implement complex encryption-only solutions and Public Key Infrastructures based on outmoded products and architectures.

Little success has been achieved because these technologies are deployed using a session management approach, instead of a transaction-oriented approach. These traditional approaches, based on VPN schemes like SSL, are hard to implement and require complex integration with a variety of web services and application servers – and they still don't get the job done.

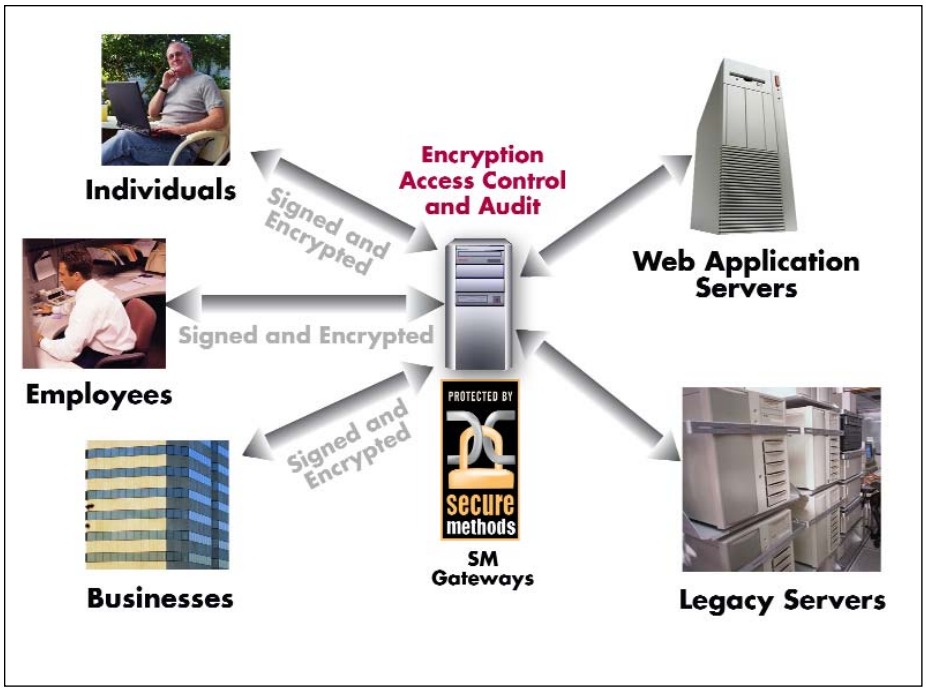
What is now needed is a new generation of security infrastructure based on the concept of securing transactions, not just sessions, and which is transparent to users to significantly reduce the security breaches caused by the human factor. This new approach must overcome the limitations of PKI and SSL implementations and provide an unprecedented level of security appropriate to each individual organization, and to each individual transaction.

SecureMethods has developed a Next Generation Security architecture designed specifically to address these issues. It seamlessly integrates with new and existing applications and provides a wide range of security features, including embedded PKI, encryption, access control, embedded digital signatures and per transaction automatic auditing in one product.

The Next Generation Security Architecture

SecureMethods Architecture

The SecureMethods architecture protects data against four basic threats: disclosure, forgery, corruption, and repudiation. This architecture supports public key cryptographic schemes that provide a high level of security for transmitted and stored data. SecureMethods offers users the ability to secure data and transactions through encryption, strong authentication, digital signatures and and role-based authorization . SecureMethods Next Generation Security Architecture is an easily deployed, transparent transaction-level security solution for the enterprise.



The Next Generation Security Architecture

How the SecureMethods Architecture Works

SecureMethods' architecture consists of two components; a gateway appliance component and a client component that runs in the system tray on the desktop.

The SM Gateway decrypts, verifies, authorizes, and audits inbound submissions and requests, and encrypts and signs outbound responses. SM Gateways perform all authorization checking by comparing the originator's signature with a system resource access control list (ACL) to verify validity of the requested submission or retrieval operation. This system supports standard web, email, and other application servers, and authorization checking, transaction, and administrative interfaces. The SM Gateway seamlessly interoperates with both VeriSign and Entrust, and supports X.509 certificates and LDAP at both the client and server.

The SM Client Software resides on the client machine that sits on an untrusted network. It runs under the user interface and secures transactions prior to transmission and verifies received data prior to display to the user. The SM Client Software, which is provided at no cost, performs these functions without the need for any user action or knowledge. This approach not only facilitates deployment and system use, but also allows the seamless and secure deployment of new cryptographic algorithms and communications protocols.

The SM architecture also:

- Combines symmetric cryptographic algorithms with public key-based key exchange to protect data from disclosure.
- Uses public key digital signature algorithms that incorporate a cryptographic hash to guarantee the integrity and origin of the data and prevent forgery and corruption.
- Provides time-stamped digitally signed receipts for all transactions. This prevents repudiation of data.
- Supports FIPS 140 approved standard 168 bit triple DES and AES 256 for bulk encryption of transmitted data.
- Supports the integration of NIST FIPS 140-1level 2 cryptographic mechanisms.

Protecting keys

With any public key cryptographic scheme, protecting private keys used to decrypt and sign transactions is crucial. The SM architecture supports the integration of 1024-bit and higher RSA-capable smart cards to secure private keys and perform public key cryptographic operations. Other removable tokens such as memory keys with and without password protection are also supported.

Managing keys

For public key management, the SM architecture with Embedded PKI™ supports X.509 certificate formats and LDAP distribution protocols. This approach allows client software to cross-certify certificates and makes the certificates widely available without requiring any user knowledge or action.

SM architecture and host security

The user's computer is the weak point in any security infrastructure, and various countermeasures may be employed to harden it and increase the assurance of the overall system. While the user's machine must have the no-cost SM Client™ installed to access systems protected by SM Gateway™, other steps may be taken to protect the platform itself. These include upgrading to Windows 2000 or XP and installing a personal firewall.

Some highly sensitive platforms require individual integrity and access control protection. You can protect these systems with smart card boot systems to provide hardware-based access control and ensure the integrity of these sensitive platforms. As a result, only a user with a properly configured and keyed smart card and the correct password can successfully boot the protected system. The SM architecture supports smart card boot systems.

SM Client™

SM Client™ is a no-cost software module that seamlessly integrates into, and operates with industry standard web browsers to offer full digital signature support and non-repudiation services for transfers executed from within the browser environment. SecureMethods makes these features available fully free of charge.

SM Client™ provides users the ability to encrypt and/or digitally sign any Windows-based file, including office suite, database, graphics, or multimedia files to name just a few. Using the SM Client™'s context

menu additions, users can easily encrypt files for local storage protection, or encrypt data for others before sending over an untrusted network. Files may be encrypted and signed for general receipt or only for designated individuals to decrypt and access the protected content.

Features

- Seamless interface to SM Gateway™
- Public key signatures for data origin authentication
- Data encryption to protect sensitive data
- Permits users to transparently access protected web sites if properly registered and authorized
- Permits users to decrypt files that others encrypted for them
- Easy-to-use graphical interfaces
- Easy to use InstallShield interface

System requirements

- Windows 95, 98, NT, 2000, or XP
- Internet Explorer 5.0 or higher, or Netscape 4.76 or higher
- 2 MB free space

Depending on assurance requirements, the private key can be stored on a memory key, a smart card or on hard disk.

SM architecture and network security

The SM architecture includes SM Gateway™, which mediates network transactions to protected servers and ensures that all data is securely transmitted or received. SM Gateway™ can work either in parallel or in conjunction with your existing firewall . This level of security, ease of use, and rapid deployment is only available with the SM embedded services model.

SecureMethods Architecture Capabilities

Encryption Capabilities

Encryption is a vital part of the SecureMethods capabilities because it is used in existing e-business security to protect all types of data transmission. The SM Gateway™ supports a variety of encryption technologies and securely processes data that has been encrypted and authenticated via digital signatures, smart cards, or biometric methods irrespective of how the transmission was created (out of a web browser, email, or desktop). SM Gateway™ features the same ease of use and operates in the same way without regard for the type of connection – WAN, LAN, wireless, or dialup. SM Gateway™ also enables centralized authorization management, access control, and audit functions. Through the addition of these security features, the level of protection afforded by SecureMethods' Embedded PKI™ technology vastly exceeds the levels available with SSL/VPN and passwords, the most common security technology in use today.

Digital signature and audit capabilities

SM Gateway™ enables organizations to take full advantage of Federal legislation that makes digital signatures legally enforceable. The SM Gateway™ is the only product that provides digital signatures out of web, email, and desktop applications with a single no-cost client. SM Gateway's' tracking and recording technology provides audit and non-repudiation services for all transactions to protect against both internal and external attacks. The combination of security features and the ability to audit transactions provides companies with a legally enforceable and irrefutable methodology for conducting business electronically more securely and at lower cost than they can with paper.

Interoperability

The SM architecture is unique in its ability to add best-in-class security services to existing applications without noticeable degradation of the user experience or requiring modification of the underlying application. SecureMethods technology allows disparate technologies (firewalls, digital certificates, and VPNs) to work without affecting their operation. This technology also integrates seamlessly with point security products from companies such as RSA Security, Baltimore Technologies, Verisign, Entrust, etc.

Infrastructure Efficiencies

SM Gateway™ enables organizations to replace expensive Intranet leased lines with cheaper local Internet and broadband connections. Currently, many businesses maintain dedicated point-to-point connections for the sole purpose of processing high-value transactions with some measure of security.

SM Gateway's™ multiple security layers enable companies to eliminate this expensive telecommunications infrastructure and switch to much lower cost Internet connections while improving security and enabling the enforceability of electronic transactions

Disaster recovery

To provide disaster recovery capability, redundant sites and components are deployed as required. The SM architecture allows transactions to be transparently and securely routed to alternate servers and/or sites. This capability also allows application processing to be distributed across servers without the need to reconfigure client applications.

SecureMethods Security Services

SecureMethods' encryption, authentication, auditing services, and non-repudiation features are founded on Public Key Infrastructure (PKI) – based trust relationships. Users are issued credentials by sponsoring organizations, such as an employer or agency. Those credentials, which are in the form of X.509 Certificates, are then employed by software agents running on a local PC or access device to verify a user's identity and authorization level. Certificates contain public keys that may then be used by agent software to encrypt and verify digital signatures on communications sessions, files, and other computer-based communications. The private key associated with the certificate is used to digitally sign and decrypt data.

Each user, "internal" or "external," must be issued credentials or certificates through a Certificate Authority (CA). Clients can choose to use SecureMethods' CA services, elect to use another third party CA service, or run their own service. SecureMethods' SM CA™ generates registrations that are used by SM Client™ to access applications protected by an SM Gateway™. This registration consists of an RSA public/private key pair used to enable users to access protected applications. SM CA™ creates X.509 certificates as part of the registration and uses LDAP to distribute the public key information. It packages each registration using InstallShield to provide an easy and commonly recognized installation mechanism for users.

SecureMethods Architecture Capabilities

Application data, which is typically accessed through a browser, is protected between the SM Client™ and the SM Gateway™ in a manner transparent to the user and to the application server. Each transaction between the browser and the server is signed and encrypted. SM Gateway™ verifies the signature, and by so doing identifies the user. The system then determines if the user is allowed access to the resource requested by checking the user's identity against the access control matrix. SM Gateway™ passes the request to the application server if the user is allowed access, or sends a denied message to the user if the user has not been granted permission to access that resource.

SM Gateway™ also signs and encrypts data returned from the application server to the client. SM Client™ then verifies that the data was received from SM Gateway™ and decrypts the data. This unique Embedded PKI™ technology not only reduces deployment time but also is implemented at fraction of the cost. Because the protection services are provided transparently, other security tools used in the environment (anti-virus, VPN, etc) will continue to function normally.

Each transaction is audited by SM Gateway™ to provide an irrefutable digitally signed record of all user actions. SecureMethods also provides detailed reports that highlight usage patterns and failures to provide insight into activities within the enterprise The SM Gateway™ features extensive audit and reporting capabilities that enable administrators to obtain detailed information about HTTP, FTP, SSH, and SSL activity. SM Gateway™ reports provide a per hour usage summary and disk usage information. Each request to SM Gateway™ is logged including detailed transaction information regarding

1. digital signature
2. source (client) IP address
3. timestamp of when the request was received
4. client timestamp on the request,
5. the resource requested.

Thus for every user action it is possible to prove who, what, when, and where on a transaction-by-transaction basis.

SM Gateway™ and the SM architecture on which it is based, provide a highly scalable, flexible, and Commercial-Off-The-Shelf (COTS) -based means of deploying secure transaction-oriented systems that not only encrypt, but also digitally sign web, email attachments, or other transactions. Applications running on SM Gateway™ offer high assurance security that is transparent to the user.

Architecture FAQ

1. Why is the SM architecture more secure than other security solutions?

The SM or SecureMethods architecture provides both network security and web application security. Firewalls only provide network access control. The problem is that to allow public access to your web application, you have to place your web application outside of your firewall or on a DMZ, thereby leaving it vulnerable to attacks.

The SM architecture solves this problem by allowing public access to your web application but vulnerable data remains protected by the SM architecture. This Embedded PKI™ and security removes any risk of data being accessed by unauthorized users by identifying users and authorizing any access they might have. Your security policy determines which users are allowed access to the data that resides on the web application.

2. I understand that the SM architecture provides both network and web application security, what is the difference?

Network security deals with the communication protocols, server access, and the transmission of data packets, whereas web application security ensures that access to your web resources (i.e. servers, programs, files, URLs, etc.) are restricted to authorized users.

3. How does the SM architecture know who the user really is?

The SM architecture authenticates the user via a digital signature on each transaction. This digital signature is used during the authentication process to ensure that the user is who they claim to be. A by-product of verifying the signature is that the Gateway stores the signed the transaction to resolve future disputes.

4. OK, now we know that John Smith is really John Smith. How does the SM architecture prevent someone from reading John Smith's data?

The SM architecture encrypts data for the user via the Public Key Infrastructure (PKI). PKI provides a private key (known only to the user) and a public key (distributed to anyone). The most reliable method of providing keys is to use a smart card at the user workstation whereas a cheaper solution is to distribute the keys on a memory key that can be password protected. The encryption algorithms access the user public key to encrypt John Smith's data before it is sent over the network. Since only John Smith has access to his private key, he is the only one who can decrypt the data sent to him

5. If the user loses his smartcard or memory key, can an unauthorized person who finds it use that smart card to access data?

The smart card may be configured to require a password or other biometric material. This is similar to using the PIN number with your ATM card; if

someone finds your ATM card, they still need your PIN to access your bank account.

6. How many users can the SM architecture support?

Scalability is the key issue here, and the SM architecture is infinitely scalable. Standard reports generated by SM Gateway™ detail usage spikes and can identify bottlenecks. Any component of the SM architecture that becomes overloaded can be seamlessly duplicated without affecting usability or compromising the security of the overall system. A significant benefit of this duplication approach is fault tolerance – if one system experiences an outage, then the other systems continue operating albeit under increased load.

Summary

The SM Gateway™ and its Embedded PKI™ technology offer a unique one size fits all security solution that resolves the largest barrier to ubiquitous electronic commerce. Through implementation of the SM architecture and handling of secure transactions, SM Gateway™ can securely process data that has been encrypted, digitally signed, and even biometrically protected. Already deployed and proven in a variety of sensitive environments, SM Gateway™ can be configured and installed on a turnkey basis to provide hardened security for your network applications.

SM Gateway™ seamlessly uses X.509 certificates that may be stored in a local database or LDAP accessible directories located on the SM Gateway or on a remote LDAP server.

SM Gateway™ decrypts, verifies, and stores all inbound submissions and requests, and encrypts and signs outbound responses. It performs all authorization checking by comparing the originator's signature with a system resource access control matrix to verify the validity of the requested submission or retrieval operation.

Features

- Protection for existing application servers and databases with no modifications to servers
- Security for your LAN, WAN, and Web servers
- Public Key Infrastructure (PKI) through X.509 certificates
- Easy to maintain ACL to restrict access to protected web applications, URLs, and files
- Wide variety of strong encryption algorithms supported, including commercial (1024-bit RSA, triple DES) and Government type 1 classified
- Secure wireless network options
- Remote VPN access
- Turnkey appliances provided and installed by security experts
- Insurance for transactions by Lloyd's of London for up to $100,000 per transaction
- Secure remote administration provided