WestGate, Inc.
White Paper

All information in this document is subject to change without notice. This document is provided for informational purposes only and WestGate Software Security makes no warranties, either expressed or implied in this document.

Security Suit, Protected Disk, Personal Security Assistant, CryptoKey, Remote Client Authentication, Security Suit Lite are trademarks of WestGate, Inc. WestGate currently holds a patent pending on Audio and Video Real Time Encryption Method. All other company and product names may be trademarks of their respective owners.

Introduction

Rapid Internet development has enabled corporations to move their processes onto one large public network called the World Wide Web; and while this has helped tremendously in improving productivity through communication with partners, suppliers and customers it has left all businesses with major security holes.

Although most companies today have defensive security measures in place (Firewalls, VPN as well as various antivirus products) they are still left open to security breaches from internal employees, former employees, hackers and crackers.

Computer Crime Bleeds U.S Corporations[1] :
Based on responses from 503 computer security practitioners in U.S corporations, government agencies, financial institutions, and medical institutions, universities the "2002 CSI/FBI Computer Crime and Security Survey" confirms that the threat from computer crime and other information security breaches continues, and the financial toll is mounting.

1. 90% of respondents detected computer security breaches with in the last twelve months
2. 44% (223 respondents) were able to quantify their losses at $455,848,000
3. As in previous years, the most serious financial losses occurred through the theft of proprietary information.
4. 75% of the respondents identified internal employees as a security threat: they build up access to systems over time moving from one position to another.

New government laws and regulations aimed at protecting consumer information set the stage for the way certain companies will have to do business. A California Law went into effect July 1, 2003 requiring any company, regardless of location, to promptly notify its California customers if that company suspects that hackers had stolen personal data. Companies that do not notify the customers could get fined $5-$25K.

This same bill "Notification of Risk to Personal Data Act" was just introduced into the Senate.

Now more than ever it is imperative for corporations to integrate stronger security measures into their infrastructure or else they will stand to lose thousands of dollars, not just through government imposed fines but through bad press, lost credibility and fallen stock prices.

Defensive security measures are no longer enough. It's close to impossible to keep the bad guys out, but businesses can work harder to authenticate (identify) and authorize (provide access) from within. These solutions should be flexible, cost effective and easily integrated with a company's existing protocols. These solutions need to provide advantages over current systems based on PKI.

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables businesses to protect the security of their communications and

[1] Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey" Computer Security Issues & Trends. VOL.VII.NO.1 Spring 2002

business transactions on the Internet. These systems are complex and expensive to implement.

This white paper describes:

- the philosophy behind the design of WestGate's family of products
- how the WestGate technology works
- advantages over current technologies based on full featured PKI.
- Brief descriptions and applications for WestGate's products

What does WestGate do?

WestGate, Inc provides a set of reliable methods and technologies for data protection and secure digital communications. Our solutions and security products protect the most popular file formats (Microsoft Word, Microsoft Excel, Microsoft Outlook, plain text email, Adobe Acrobat, mp3, avi, jpg, bmp, WMV/WMA, HTML, etc) and control (limit) access to confidential information retrieved or sent through the Intranet/Internet network with a smart, physical "key."

Our mission is to ensure that your data is completely secure and that only intended recipients have "the key" to access.

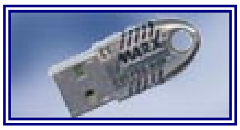
I. Basic principles of WestGate Products & Solutions

1.1. Combining software and hardware based protection

WestGate's security products and solutions are based on the usage of a personal hardware security device called CryptoKey™..

Due to a universal software layer called CryptoKey File System (CKFS) WestGate is flexible with almost any implementation of the CryptoKey™: full range of popular hardware security devices can also be used, including USB hardware tokens and various smartcards.

Current WestGate software is designed to work with an inexpensive USB smart key that is small enough to fit on a keychain.
WestGate supports both MARX USB and Rainbow iKey1000 series.



The advantages of having a hardware + software based solution:

1.2. Two-factor authentication and two-tier security

Westgate utilizes a two-factor authentication system for access:

1. Something that you have (a password)
2. Something that you need (a CryptoKey).

A two-tier security is used for document protection:

1. The content itself is encrypted
2. It requires a physical key for decryption (CryptoKey™).

WestGate's approach is much more reliable than typical authentication schemes that rely on usernames and passwords. Even if your username or password is compromised, your data is still safe. Only the CryptoKey can unlock your information. And it is impossible to fabricate the CryptoKey.

1.3. Powerful encryption

WestGate applies 256bit AES symmetric encryption combined with 1024bit RSA asymmetric encryption. This combination provides reliable protection and is an unbreakable security standard. It is widely used today (PGP, HTTPS, SSH, IPSec, S/MIME).[2]

13.1. Symmetric encryption

WestGate uses 256bit "**Symmetric" encryption** to protect the most popular data formats (HTML, Word, Excel, Acrobat, Outlook, Audio and Video files, etc.) and to secure remote server-client communication.

"**Symmetric**" means that the same key value will is used to encrypt and to decrypt information. Each document is encrypted with a random 256-bit encryption key.

[2] PGP Corporation develops secure-messaging and data-storage products used by thousands of corporate and millions of individual users worldwide to protect their confidential, sensitive, and proprietary information.

HTTPS is **hypertext transmission protocol, secure.** A secure protocol used to request and transmit files, especially web pages and webpage components, over the Internet or other computer network.

SSH is a Unix shell program for logging into, and executing commands on, a remote computer. SSH is intended to replace rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network.

IPSec is a protocol that provides security for transmission of sensitive information over unprotected networks such as the Internet.

S/MIME is **secure multipurpose internet mail extensions.** A specification for secure electronic mail, S- IME was designed to add security to e-mail messages. The security services offered are authentication (using digital signatures) and privacy (using encryption).

Each time when a user needs to encrypt a certain document a random 256 bit encryption key is generated and the document content is encrypted using this key.

1.3.2. Asymmetric encryption: controlling document access

The Challenge: Where should this symmetric encryption key that is generated to protect certain documents be stored? How can access to the encrypted document be limited only for intended users?

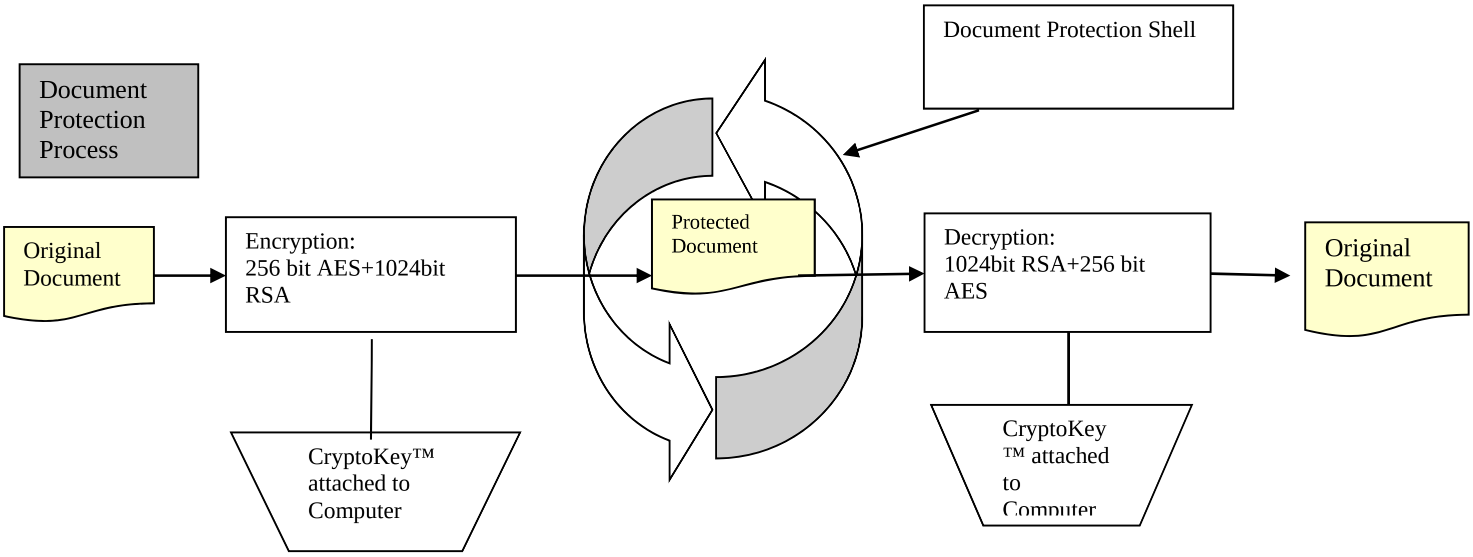
The Solution: **Asymmetric encryption**. Every user gets his/her own unique RSA key, which is actually a couple of (keys: a **private key** (stored in the most secret place – CryptoKey's protected memory) and a **public key** (freely redistributed).

If something is encrypted with user's public key it can be decrypted ONLY with his/her private key (second half of the couple) and vice versa. This is why the algorithm is called asymmetric.

When it becomes necessary to encrypt any document, the algorithm (WestGate's Encryption Engine) generates a random symmetric key first, encrypts the document using this key, then encrypts the key itself using public keys of those users, to whom access has been granted.

This data (symmetric encryption key encrypted with various asymmetric public keys) is appended to the encrypted document.

When a user wants to open a protected document, the program first checks if this document was encrypted for this user and if so, it is possible to use the private key of this user (stored in his/her CryptoKey) to decrypt the symmetric encryption key and to do the rest. If not – there is no way to decrypt the document for this user.



1.4. Certificate Model

At the heart of WestGate security products and solutions there's is a unique data protection engine, called the **Certificate Model**. It is tailored specifically for the needs of small to medium-size businesses and it provides strong cryptographic protection for both intra-enterprise and inter-enterprise document exchange while requiring only minimal administration.

1.4.1. Freely redistributable certificates

Users can export their public keys to other users and also import public keys to their own database.
To simplify public keys exchange/distribution a special object, called **certificate** is supported.
In addition to the user's public key, his/her certificate also includes:
user name, issue date, expiration date.

In its Office Security products WestGate provides users with a convenient and natural way to store & manage external certificates: **Certificate Book**.

The Certificate Book is a personal database used to simplify selection of recipients when encrypting documents. Its owner can easily encrypt any document to a subset of users from his/her Certificate Book.

1.4.2. Super user

Special users called "Super Users" can access all encrypted documents at a particular company. These users have a Master Key – the very first asymmetric key generated for a particular company.

The WestGate Certificate Model includes a special notion/object called **Super User**. The Super User has unlimited access to all encrypted company documents. The Super User has its **Master Key** – the very first asymmetric key generated for this company (customer).

The public part of the Super Key is stored in every user's CryptoKey formatted for this company.

Any encrypted document automatically includes Super User public key in the list of its recipients.

1.4.3. Protection Rings

WestGate also includes **Protection Rings** support.
The main idea of Protection rings is to simplify encrypted documents exchange between users inside the customer's company.

WestGate Certificate Model provides four predefined protection rings, representing typical management hierarchy for most small to medium businesses:

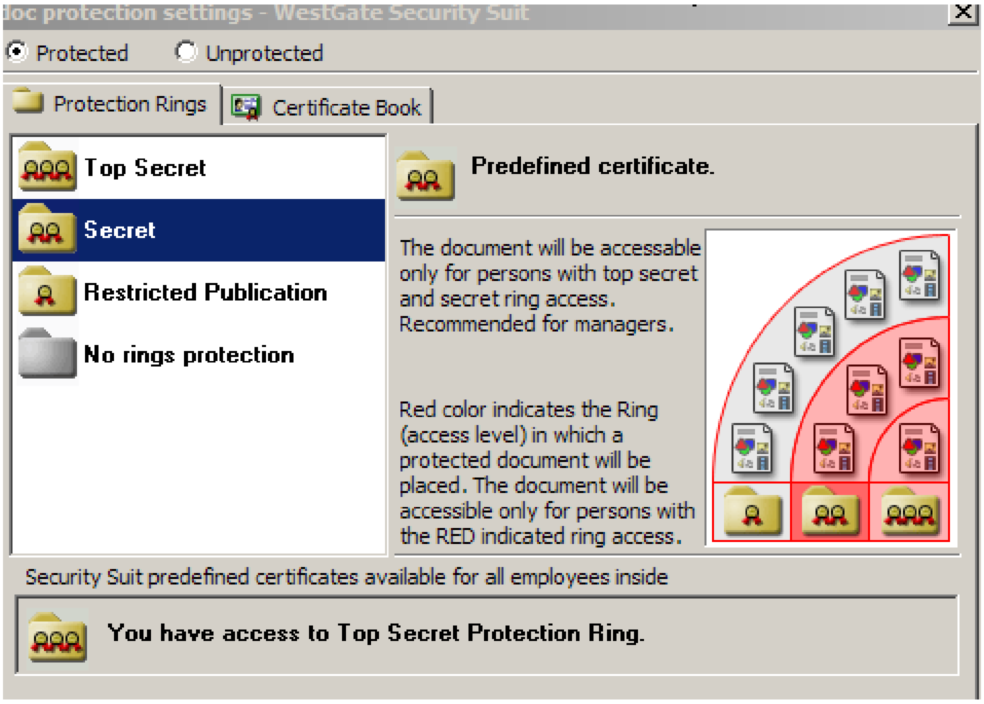
- **top secret**, **secret**, **restricted**, **unclassified**

So, instead of encrypting:

- document#1 to users: A, B (say, top management of the company)
- document#2 to users: A, B, C, D (top executives + managers)
- document#3 to users: A, B, C, D, E, F (extended auditorium inside the company)

The user can simply encrypt:

- document#1 to all top secret ring owners
- document#2 to all secret ring owners (will be automatically available also for top secret ring owners)
- document#3 to all restricted ring owners (automatically available for all top secret and secret ring owners);



● Protected ○ Unprotected

Secret (selected)

Predefined certificate.

The document will be accessable only for persons with top secret and secret ring access. Recommended for managers.

Red color indicates the Ring (access level) in which a protected document will be placed. The document will be accessible only for persons with the RED indicated ring access.

Security Suit predefined certificates available for all employees inside

You have access to Top Secret Protection Ring.

1.4.4. Digital signatures, managing certificates

In many cases it is important not only to encrypt a document (protecting it against unauthorized access), but also to assure its recipients that this document was created by its author. It is done by adding a special **digital signature** of the author to the document: a special hash value calculated for the document's file is encrypted with its author's private key and appended to the document.

However, this step can not provide us with 100% assurance regarding the document's author. Still there is a chance of certificate fabrication.

To eliminate this situation and to provide those customers, who really need it with a truly trusted environment, WestGate Certificate Model supports **trusted** certificates – certificates digitally signed by the Master Key.

Besides digital signatures WestGate Certificate Model also provides customers with general certificate management functionality: certificate revocation, granting/revoking protection rings and, expiration date control, etc.

1.4.5. Summary: WestGate Certificate Model versus standard PKI (Public Key Infrastructure)

Public Key Infrastructure (PKI) is a family of security models that provide strong and flexible protection based on asymmetric cryptography. The majority of modern security systems rely on PKI.

However, along with the flexibility of PKI come high administration costs. Any PKI-based solution requires at least one dedicated secure server for issuing certificates and enforcing access control policies – and the staff to run the server. Large organizations that rely on security in every day business transactions are willing to pay the huge overhead costs. However, small companies that want to add cryptographic protection to their document flow are seeking for cheaper solutions.

WestGate provides that solution. Our software and hardware security products provide strong and flexible security without the cost of dedicated servers or technical staff.

In order to meet the security requirements of small companies Westgate Certificate Model requires neither dedicated servers nor any technical stuff to support it, while still providing strong protection and high flexibility.

Security is as simple as choosing one of four “protection rings.” These **security stamps** have been used in paper-based workflow for decades: *Unclassified*, *Restricted*, *Secret*, and *Top Secret*. Each piece of data to be secured, e.g., a text document, media file, or email, is assigned to one of the rings. Each company employee or customer is also associated with a certain ring. A user has access to all documents belonging to his ring and lower (less restricted) rings.

Protection rings are implemented by means of asymmetric cryptography. A ring is represented by a public/private key pair. Each user holds private keys of his ring and lower rings. Each document is encrypted with a public key of a corresponding ring. In order to decrypt the document a user must belong to the same or higher (more restricted) protection ring. Private keys are never operated by users explicitly. User’s private keys are stored in personal CryptoKeys™ that must be attached to computers every time the WestGate security software is used. Access to CryptoKey™ is protected by password.

The main advantage of protection rings is that they are static. Once generated, they never change. This property allows building a completely decentralized security infrastructure without a specialized server.

The WestGate Certificate Model also allows for more flexible security implementations. Users can exchange certificates and create a protected communication channel.

Conclusion: WestGate's security products and technologies based on the Certificate Model and encryption engine described above provide affordable and reliable solutions for small to medium businesses comparing to expensive high-end PKI implementations.

II. WestGate Software Security Product Descriptions

1. THE OFFICE: Security Suit (Full Version)

Current Applications: For Small to Medium Sized Businesses with a need to securely transmit and store data, voice, audio, and emails.

How it works: Data (documents, files, emails, voice mails, text, etc.) is protected using a strong encryption algorithm. Only users with the hardware keys (CryptoKeys™) who are assigned access can read the encrypted data. Managers can create child keys for their subordinates, clients, etc. and assign access to the data. When a child key is created a new certificate with the user's profile is automatically added. The Security Suit also allows for every certificate to be expired, backed up/restored, imported and exported.

Applications:

1. Encryption of emails for Outlook Professional and plain text emails (any email client)
2. Encryption of document files created in Word, Excel, and Adobe Acrobat.
3. Protected Disk: Creates a hidden and encrypted directory on the PC. Files can be accessed only with the CryptoKey™.
4. Encryption of audio & video files (Microsoft Media Format WMV/WMA is supported),
5. File Protector: any type of data files are secured through 256 bit strong encryption and two factor authentication method.

System Requirements: **Windows /2000/XP/Vista/Win7**
MS Office 2000/XP/2003/2007/2010

2. YOUR IDENTITY: Personal Security Assistant

Current Applications: Personal Security Assistant works like a secure digital organizer by encrypting and storing Internet usernames and passwords, credit card information, bank accounts data and other information. etc. on the CryptoKey™.
Benefit: The PSA eliminates the need to keep re-entering personal information on ecommerce websites. It also severely reduces the chances of identity theft.

How it works: Encrypts all passwords, logons, credit card numbers and other sensitive data, and stores them on the CryptoKey™. Access to the key is provided through a small application on the users' PC. Anytime access is required to certain websites or systems –the key is inserted in the USB port and the PSA software is launched from the user's PC. Two key strokes transfer sensitive information from the PSA to the web page. Backups of the sensitive data can be made and stored in a safe place in case the key is lost.

System Requirements: Windows 2000/XP/Vista/Win7

3. BUSINESS/PERSONAL: Security Suit (Lite Version)

The Security Suit Lite is a light version of Security Suit and has two (2) of the components described above:

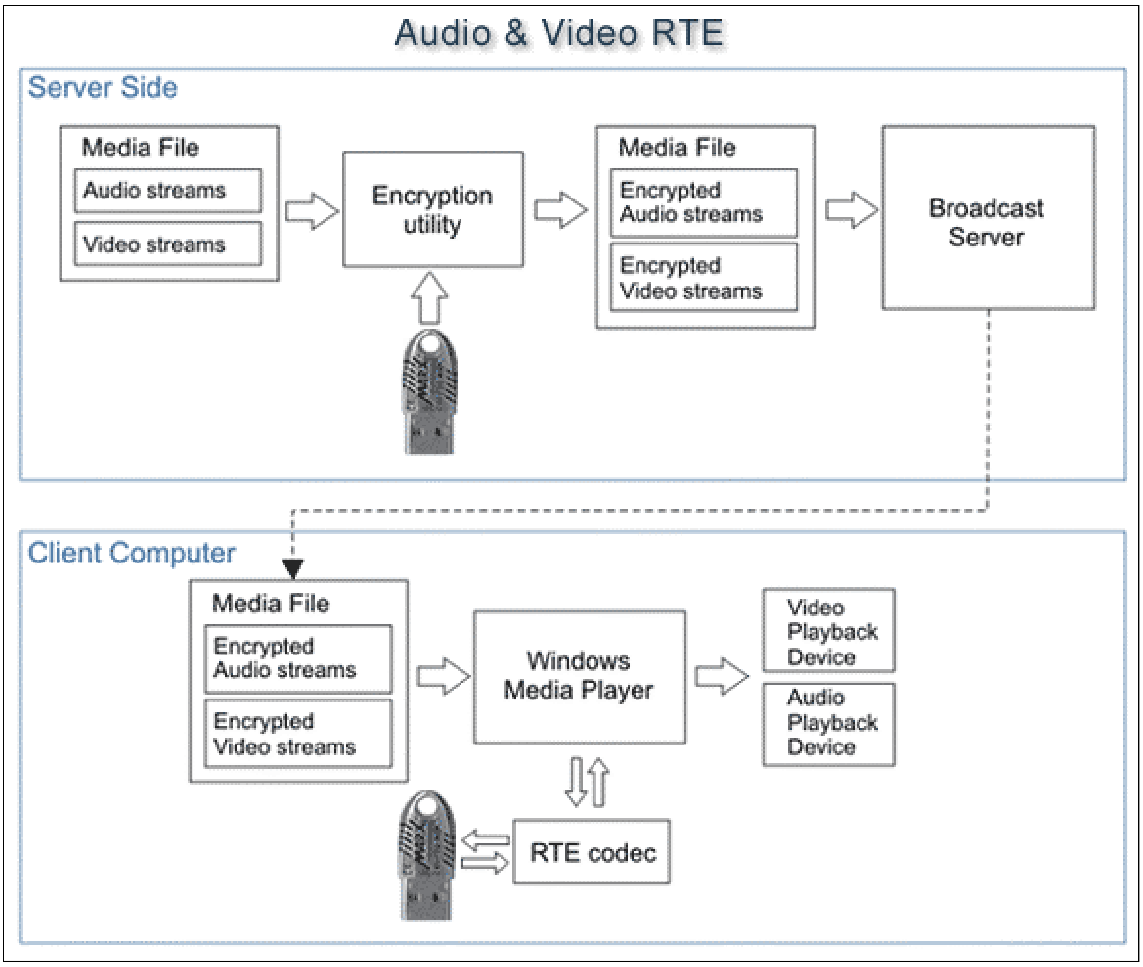
1. Protected Disk
2. Personal Security Assistant

System Requirements: Windows 2000/XP/Vista/Win7

4. MULTI MEDIA: Audio & Video Real Time Encryption (RTE) <Patent Pending>

How it works: This solution allows media providers/vendors to encrypt video or audio files so they can only be played on computers with valid CryptoKeys.

The Figure below illustrates the Audio & Video RTE solution.



Current Applications: An encrypted digital media can be delivered to clients as:

a) files on CDs/DVDs or through the Internet (file oriented distribution);
b) a stream using Microsoft Media Services (part of Windows Server) or UNIX analogues (stream-oriented distribution), including various internet/intranet oriented scenarios, like:

- encrypted video conferences and meetings;
- protected internal product presentations;
- just-in-time learning;
- video on demand delivery;
- pre-recorded content

The Audio & Video RTE Solution in combination with Microsoft Windows Media Services allows encrypted media content in Advanced Systems Format (ASF) to be distributed in a variety of different ways. Content can be delivered either live or pre-recorded, multicast or unicast.

Benefit: Ensure that only those who have paid for the content have access to it. Protect sensitive information and retain control over its distribution. Track usage, update access rights.

System Requirements: Windows 2000/XP/Vista/Win7

IV. Internet Based Technologies

Two basic technologies, developed by WestGate Software Security Inc.: **HTML Document Protection** and **Remote Client Authentication** can be used together or separately to add security and protection to a wide range of Internet based businesses.

1. HTML Documents Protection

Current Applications: Restricted Access to any data, stored in HTML format (encrypted web pages, html documents, presentations, online courses).
Besides strong encryption it also utilizes WestGate Cetificate Model and provides two-factor authentication for remote clients.

Who needs it? Companies, wishing to distribute or sell information like presentations, courses, etc… For example, one of WestGate customers -Traders International Inc. (www.TradersInternational.com) is currently employing this technology to ensure that only students purchasing their online courses have access to these courses.
This is done through a customized browser built especially for Traders International. Courses can only be accessed if the student has their CryptoKey™ inserted into their PC.

Benefit: Solutions based on this technology allow customers to encrypt their HTML documents (presentations, courses, etc.) and to organize reliable online access to them for their clients/end-users having valid CryptoKey.

In particular a turnkey solution created for Traders International allowed them to program their own keys, create and encrypt their own courses and administer access rights for their students.

How it works: Document encryption on distributor's side: All HTML document files (text files, scripts and images, audio, etc.) are encrypted on the distributor's side with 256 bit AES symmetric key. A special access controlling document (header) contains current user rights table. Each user (client) receives a CryptoKey™, programmed with his/her unique certificate (based on 1024 bit RSA private key). In order to give user access rights to documents – encryption key is encrypted with user's RSA public key and placed in the access controlling document (header). A special front-end application for distributors allows them to:

- encrypt HTML documents;
- add/edit end-users and control their access rights;
- program CryptoKeys

Server-side requirements: After being encrypted, documents should be uploaded to customer's server, or written on CD (if they are distributed offline). Our approach minimizes server side requirements (acceptable Internet bandwidth and enough space to publish encrypted document files this is all what is required). No additional server software development.

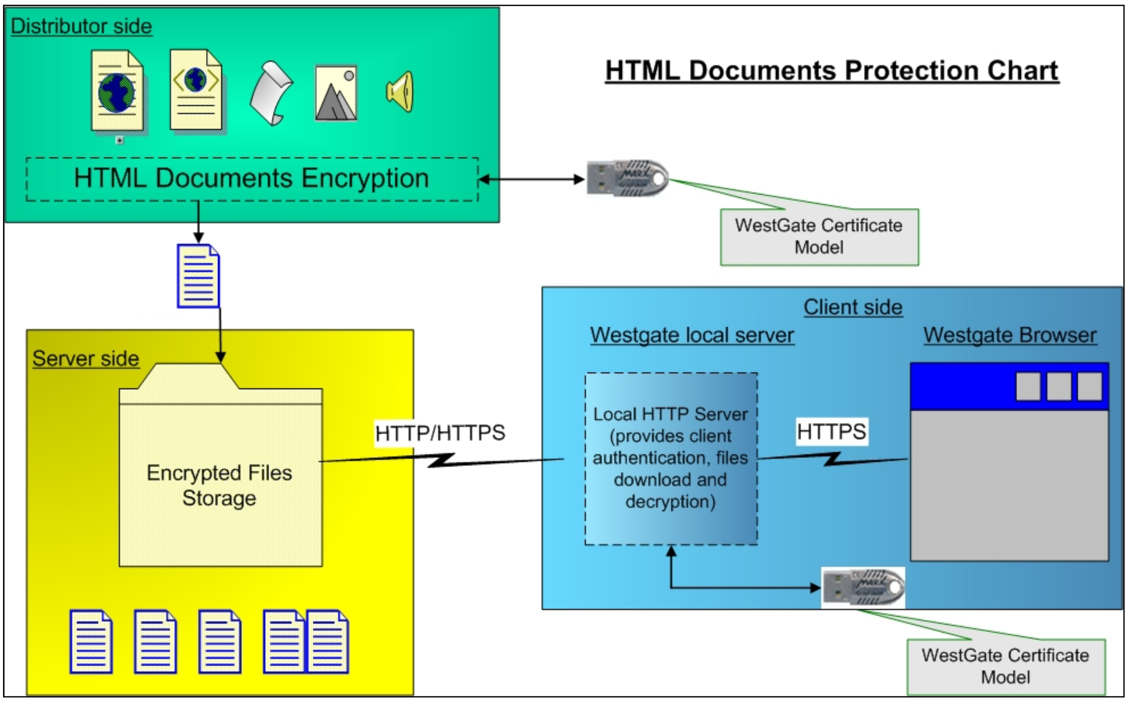
Client-side requirements: On the client side we have dedicated WestGate Browser.

The client authentication is performed by a WestGate server that checks if a CryptoKey™ with valid certificate is attached to the client's computer. If it finds a valid CryptoKey, then the WestGate server downloads encrypted document files the remote server, decrypts them on the fly and sends them to the internal browser shell.

To accelerate the process a special cache for encrypted documents is supported for the client side. If an encrypted document (or any of its internal files) was uploaded recently to the client's computer and is still valid, then its local copy will be used next time when needed.

Two components of the client side of this solution are implemented as parallel threads of one process, communicated with each other via HTTPS protocol.

The following picture illustrates this WestGate's technology:


Distributor side
HTML Documents Protection Chart
HTML Documents Encryption
WestGate Certificate Model
Client side
Westgate local server
Westgate Browser
Server side
Encrypted Files Storage
HTTP/HTTPS
Local HTTP Server (provides client authentication, files download and decryption)
HTTPS
WestGate Certificate Model

Summary: WestGate HTML Documents Protection has significant benefits, comparing to software-based protection and could be extremely useful for various online and offline content distributors, who do not wish to invest money in server-side development.

2. Remote Client Authentication

This technology enables businesses to add security and strong identification features to their Web sites and other Internet-based solutions (Intranets, ASPs). Remote Client Authentication (RCA) becomes a smart and affordable solution in all cases when various online services or dynamically generated information is used: real time trading, online banking any other online services. WestGate Certificate Model allows RCA based solutions to benefit.

Benefit: Online Identification and Access Control for all users with a CryptoKey™. Secure logon to your web site or its restricted areas, intranet, Application Service Provider.

System Requirements:
Server Side: Any platform, Java support for remote authentication
Client Side: Standard Win Environment

How It Works:

The following general requirements are important when thinking about secure Internet solutions:

1. Confidentiality and integrity of transactions
2. Authentication of the server side
3. Authentication of the remote client

First two requirements can be easily met by using HTTPS as a transport protocol. In its RCA technology WestGate focuses on client side authentication, which doesn't depend on the transport protocol to be used. Although HTTPS is highly recommended for security reasons, RCA can be applied over any transport protocol.

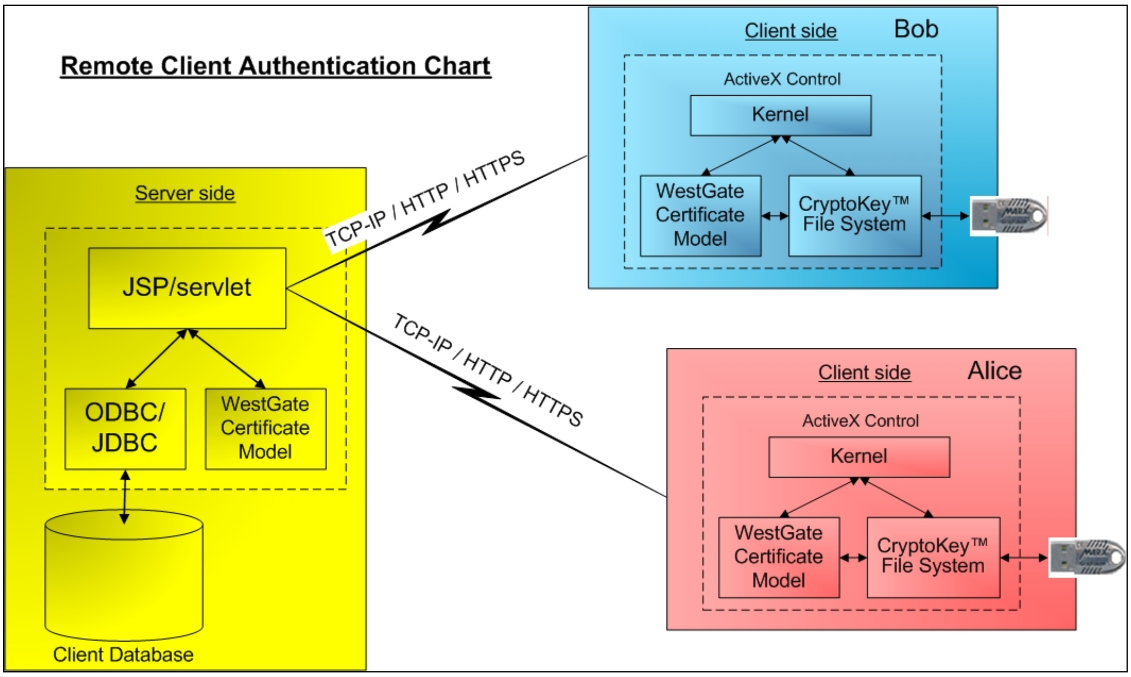
Our client-side solution assumes Win environment and is based on ActiveX component, which could be easily integrated into almost any application: standard Web Browser or customer specific front-end.

Each transaction package is encrypted with 256 bit AES symmetric key, which is randomly generated for every session. In turn the key itself is encrypted with RSA public key of receiver and signed with RSA private key of sender. The usage of 1024 bit RSA makes this approach almost unbreakable. Our "know-how" is to store public server RSA key and private client RSA key (in form of certificates) inside the CryptoKey™. Of course, client certificates must be known on server-side.

The client authentication is the most significant part of the technology. The RCA forces users to enter a PIN code after inserting their CryptoKey (two-factor authentication). The knowledge of PIN gives access to your CryptoKey™, which contains your personal certificate, including the private RSA key (as described above), which authenticates you uniquely.

Furthermore, various secure read/write transactions may be performed in CryptoKey™ memory, to provide track of records, like time of last visit, IP used, etc… For security reasons, even your certificate (RSA key pair) may be generated on the server-side and updated remotely in CryptoKey™. We access the data in the hardware memory via a special CryptoKey™ File System (CKFS), which adds portability and flexibility to the technology.

The benefit of such an approach is that all secure and sensitive information is kept encrypted inside the hardware. No data is stored on your computer, like cookies or certificates. This is a critical element of our business and our security solutions.



Summary: The Remote Client Authentication approach (presented by Westgate Software Security Inc.) has significant benefits, comparing to software-based authentication and can be successfully applied in such fields as online services, general web security, remote software updates, etc. The usage of the CryptoKey™ strengthens a company's security and we provide businesses with a convenient and easy-to-use toolkit to develop their own solution and protect their data.

FOR MORE INFORMATION:

Please visit www.westgate-usa.com or contact info@westgate-usa.com