SANAtech

Advanced
Software Solutions

Digital Signature and Secure Sign Solution

SANAtech
4 Emad El-deen Kamel St
Nasr City, Cairo, Egypt
Tel: (202) 403-4407
Fax: (202) 405-5027
www.sana-tech.com

SANAtech

SANAtech understands that delivering new standards of trusted secured computing is a challenging issue. SANAtech's Security Policy goes far beyond the simple idea of "keep the bad guys out". It's a very sophisticated policy, meant to govern data access, web-browsing habits, use of passwords and encryption, email attachments, and more.

Secure Sign
Overview

Electronic commerce enhances business efficiencies, enabling electronic data to be stored, accessed or transmitted with great ease. These efficiencies, however, and the dramatic growth of the Internet as a medium for communication, have raised new issues and concerns related to the security of electronic information. For example, when exchanging documents over the Internet, users (both corporate and individual) are concerned by such factors as eavesdropping (information remains intact, but privacy is compromised), tampering (information in transit is changed or replaced) and impersonation (information passes to a person who poses as the intended recipient).

To provide a complete solution, SANAtech has sought to provide solutions for three main areas, namely:

1) Secure Identity Management
2) Secure Data
3) Add value through newly provided security to traditional applications

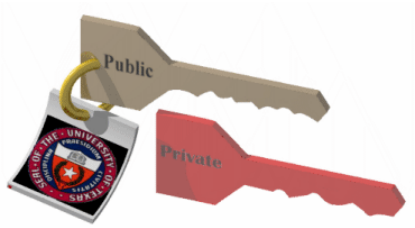
1. Secure Identity Management

Organizations need to extend access to sensitive corporate resources to an ever-growing number of employees, partners, suppliers and customers. Effectively managing this increasing number of users is a challenge in itself and, the responsibility for deploying and managing identities on these systems is spread across your organization, challenging you to keep identity data consistent.

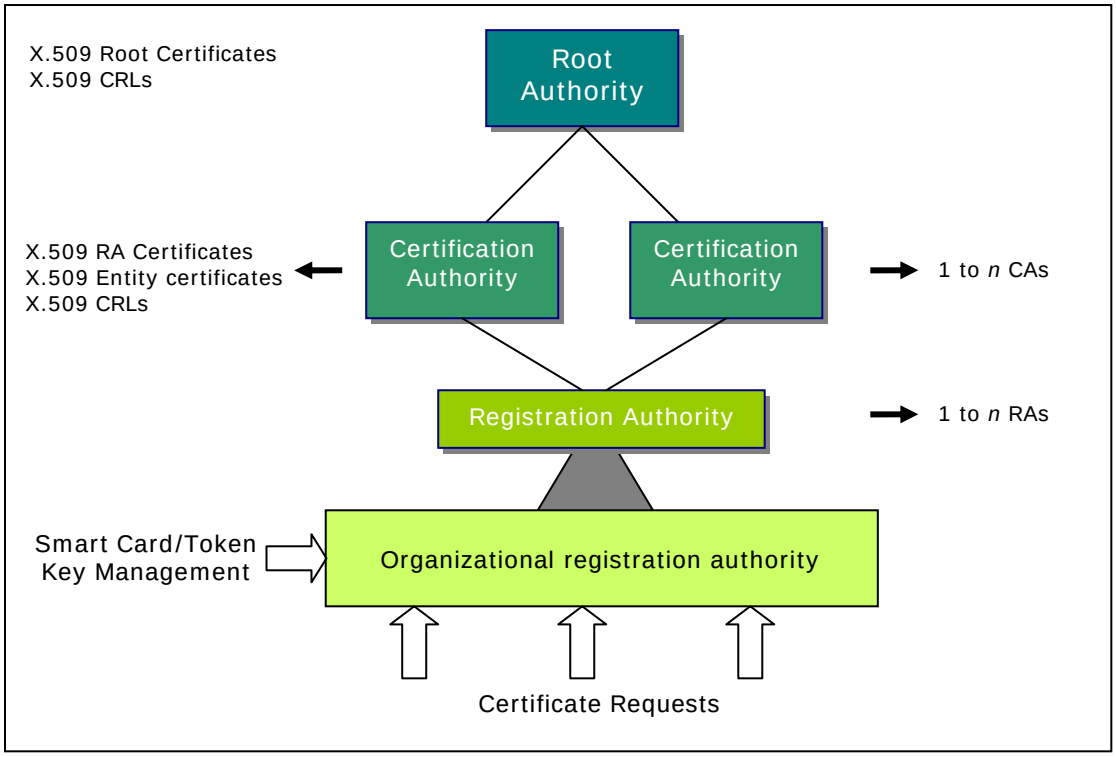
Furthermore, unique identities are required for Web services applications and devices that undertake transactions both inside and outside of organizations. You need to manage who, or what application, has access to what parts of your business, how it is being used, and what you can do to make this access deeper and better. This is secure identity management.

SANAtech Secure Sign Solution enables customers to deploy comprehensive identity management security and manage multiple types of identities across heterogeneous, complex environments.

Public Key Infrastructure (PKI)



The purpose of Public Key Infrastructure is to manage keys and their associated certificates. By the use of encryption, PKI provides confidentiality and access control. By leveraging digital signatures, PKI provides trusted authentication and data integrity. Trusted authentication is whereby users can securely identify themselves to other users or systems without sending private information over the network. Data authentication is provided by message authentication algorithms. This means that the verifier of the digital signature can easily determine if the data has changed in transit.



As the foundation for the security of transactions in SANAtech's Secure Sign, a PKI solution must protect information assets. This is achieved through:

- Identity authentication. Digital certificates issued as part of the PKI allow individual users, organizations, and web site operators to confidently validate the identity of each party in an Internet transaction.
- Verify integrity. A digital certificate ensures that the message or document the certificate "signs" has not been changed or corrupted in transit online.
- Ensure privacy. Digital certificates protect information from interception during Internet transmission.
- Authorize transactions. A PKI solution, should allow control of access privileges for specified online transactions.
- Support for non-repudiation. Digital certificates validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction.

Trusting two individuals implicitly; even though they have not met or shared information happens through a common third party that vouches for the two participants. This third party is commonly called a Certificate Authority.

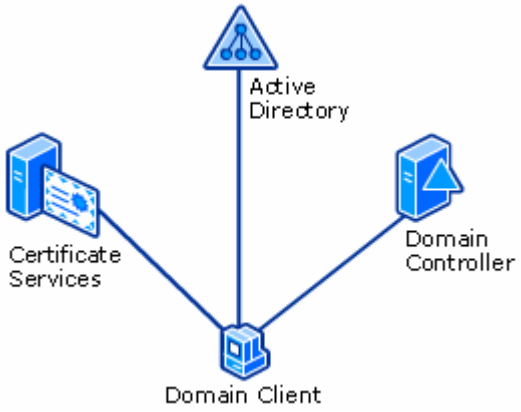
A Certificate Authority (commonly referred to as CA) can provide certificates to two individuals who establish a trusting relationship based on the relationship they individually have with the CA. A digital certificate binds an identity (or subject) to a public key.

A certificate authority (CA) is a trusted organization that issues certificates. Conceptually, the process of issuing a certificate is: the subject uses Web server software to generate a key pair and a certificate signing request (CSR); the subject applies for a certificate directly to the CA and includes the CSR along with application information; finally, the CA verifies the identity of the subject and then issues the certificate to the subject. By signing the issued certificate, the CA vouches for the subject's identity.

PKI Technologies Architecture

SANAtech's PKI solution is based on MS Certificate Services provided as part of the Windows 2003 Enterprise Server Edition.
The architecture of a PKI involves implementing various interdependent technologies and processes to make it possible to issue, validate, renew, and revoke certificates. These technologies include:

- One of more servers running Certificate Services and that provide certificate enrollment, revocation and other certificate management services.
- Active Directory service or another directory service that provides account management, policy distribution, and certificate publication services.
- Domain controllers that can authenticate end users and computers when they request certificates.
- Domain client computers and users, who request, receive, and use certificates for specific purposes. Although certificates can also be used by services and by non-domain clients, in most Windows PKI environments, domain users and computers are the primary recipients and users of certificates. In some cases, the domain client can be a subordinate CA that requests and receives a certificate authorizing it to issue certificates of its own.



SANAtech provides a combined suite of solutions and services in support of a certificate/registration authority which offer many benefits to the customer including:

- Centralized management of different types of users, across multiple environments which helps streamline processes
- Centralized identity management and policy enforcement reduces the risks of unauthorized users or applications receiving inappropriate access to specific resources
- Secure audit and workflow capabilities detail business approval processes and highlight managers who are accountable for these approvals
- Flexible architecture enables organizations to easily add incremental security to further enhance information privacy and access controls
- Enterprise and Web single sign-on
- Advanced architecture and well integrated components enable rapid deployment, improve project delivery without compromising flexibility
- Identity management for a broad range of client-server, Web and Web services transactions enables used beyond the enterprise and helps future-proof the investment

Secure Sign PKI Features

Secure Sign PKI solution is comprised of the following modules:

1. Enrollment Entity Module
2. Admin Access Module
3. Certificate Authority Module
4. Registration Authority Module
5. Internet Directory Module
6. Logging Module
7. Key Escrow Module
8. Time Stamping Authority Module
9. OCSP Responder Module
10. Renewal Notification Module
11. Reporting Module
12. Backup Module

Amongst the features of the PKI are:

- Support both English and Arabic interfaces for end users and management interfaces.
- Handling of UTF-8 based certificates for Arabic support.
- Robust, proven core of certificate and cryptographic services.
- Open and highly customizable core, no black box system.
- Secure and resistant to tampering and malicious attacks.
- Not constrained by licensing issues that could affect scalability.
- Enhanced Certification Authority – traditional CA features are extended to allow the following:

    - Digital IDs can be issued to any device or application supporting the X.509 certificate standard, enabling a single infrastructure to support all users, devices and applications
    - Certificates can be customized on a per-user basis, providing the flexibility to include user-specific privilege and access control information in a user's certificate
    - Revocation list (RL) attributes — including expiry time, issuance frequency, and the format of CRL distribution points — can be customized to best suit the organization's management policy
- Enable organizations to establish and enforce flexible corporate-wide security policies, including policies for controlling:
    - Certificate extensions per policy of RA
    - User profiles and associated attributes
- Digital certificates and keys can also be stored on a hardware token, to enable two-factor authentication to the desktop, VPN/WLAN or Web portal. The digital certificates used on the token for authentication are extensible to enable digital signatures and encryption in security-aware applications
- Digital certificates and keys can also be stored on a hardware token or smart card, to enable two-factor authentication to the desktop, VPN/WLAN or Web portal. The digital certificates used on the token for authentication are extensible to enable digital signatures and encryption in security-aware applications
- Supports high availability and disaster recovery environments
- Users can cache certificates and certificate revocation lists (CRLs), reducing the need for directory communication over the network
- Digital IDs are available to the Microsoft Windows® operating system through Microsoft's CryptoAPI interface, meaning a wide range of CryptoAPI-aware applications (such as Microsoft Outlook®, Internet Explorer, and Microsoft Word) can seamlessly become security enabled
- Enables users to monitor digital ID and certificate status information and immediately address issues, thus helping to reduce down time
- Supports a wide range of algorithms and encryption strengths available in both North America and Europe. It can also be extended thus enabling high security organizations to make use of their own algorithms
- Users authenticate to a Microsoft Windows domain using digital identities stored on smart cards, which provides tamper-resistant storage of the digital identity and protects private keys and other forms of personal information using native Microsoft Windows security capabilities

Technical Requirements

- Microsoft®: Windows® Server 2003 Enterprise
- MS SQL Server 2K or later
- MS SQL Server reporting services

2. Secured Content

Non-Repudiation – Proving WHO did WHAT and WHEN

The fact that electronic data can be easily altered necessitates a system by which parties can trust the information they share and use in everyday transactions. This requirement for trust is referred to in both the legal and crypto-technical worlds as non-repudiation.

Non-repudiation is important in e-commerce to prevent parties to a transaction from disputing or denying the transaction after the fact. The primary goal of a non-repudiation system is to prove WHO did WHAT and WHEN, and maintain evidence of such information to resolve disputes, or for auditing and compliance.

Non-repudiation should be viewed from both a legal and a technical perspective. From a legal perspective, the term non-repudiation is to provide sufficient evidence to persuade the ultimate authority (judge, jury or arbiter) as to such origin, submission, delivery, and integrity, despite an attempted denial by the purported sender. In general terms, to repudiate something is to deny its existence, and therefore non-repudiation services use cryptographic methods which prevent an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority, providing proof of origin; for proof of obligation, intent, or commitment; or for proof of ownership.) From a technical perspective, the term non-repudiation is used within authentication technology to describe a service which provides proof of the integrity and origin of data which can be verified by any party at any time.

Time stamping services are an aspect of non-repudiation services which provide a strong and verifiable cryptographic statement that a specific digital record existed at a specific moment in time. Time stamping a digital record provides the relevant parties with a verifiable statement of when the digital record was known to exist. Time stamping a digitally-signed record can further provide the relevant parties with a verifiable statement that the digital record was signed while the signing certificate was valid e.g., that the signature was formed before the expiration date of the signing certificate. Time-stamping services thus provide the technical basis for general non-repudiation services.

Hash Codes prove WHAT

To prove that the contents of a file have not been tampered with, **SANAtech EM** stores a hash code of the file, without actually seeing or storing the file. A hash code, also referred to as a “file signature” or "message digest", is a number that uniquely represents (is sufficient to identify) a particular file. Hash codes are unique in the sense that two

different files will never have the same hash code, except in the unlikely event of a hash collision. The likelihood of a hash collision decreases exponentially as the bit length of the hash code increases. With the 160 bit SHA-1 hashing algorithm (the industry standard) used by **SANAtech EM**, the odds of a hash collision are exceedingly remote (1 in 280). And because the hashing function is 'one-way', no portion of the original data can be reconstructed from the file signature (in the same way an individual cannot be "reconstructed" from his signature or fingerprint). Hashing functions are superior to their technical counterpart the checksum, in that it is not possible (or at least extremely unlikely using today's technology) to find a second file with different contents that has the same hash code. Thus, if a user can present **SANAtech EM** with a hash code, it can be assumed that the person who computed that hash code had in their possession a certain file.

Digital Certificates Prove WHO

PKI (Public Key Infrastructure) uses the concept of public and private keys to prove identity at a distance in the electronic world, where "face to face" authentication is impractical. A digital certificate is comprised of two "keys", one public and one private key. The public key is freely distributed, and serves to verify a signature as being created by its matching private key. The private key is held secret by the owner, and is used to sign digital transactions. Certificate Authorities (CAs) control the issuance of digital certificates, and are responsible for properly identifying the owner (also known as vetting).

Digital Signatures Prove WHO did WHAT

A digital signature is created by signing a hash code of a file with the user's private key. Since the public key is distributed as part of the digital signature anyone viewing the signature can now verify that it was signed by the corresponding private key. In this way, both senders and receivers can associate the sender's identity with a specific file.

Time Stamps Prove WHAT and WHEN

Time-Stamping is a process whereby a trusted third party signs a hash code with the current time. There is a protocol for time stamping – the Internet Engineering Task Force (IETF) 3161, that defines how hash codes are signed with a time stamp. This protocol is an anonymous protocol, meaning the identity of the submitter of the hash code is not associated with the file. The private key used for signing is that of the Time Stamping Authority (TSA). The TSA certifies that the time stamp issued is accurate. This avoids the problem of relying on an individual computer clock for

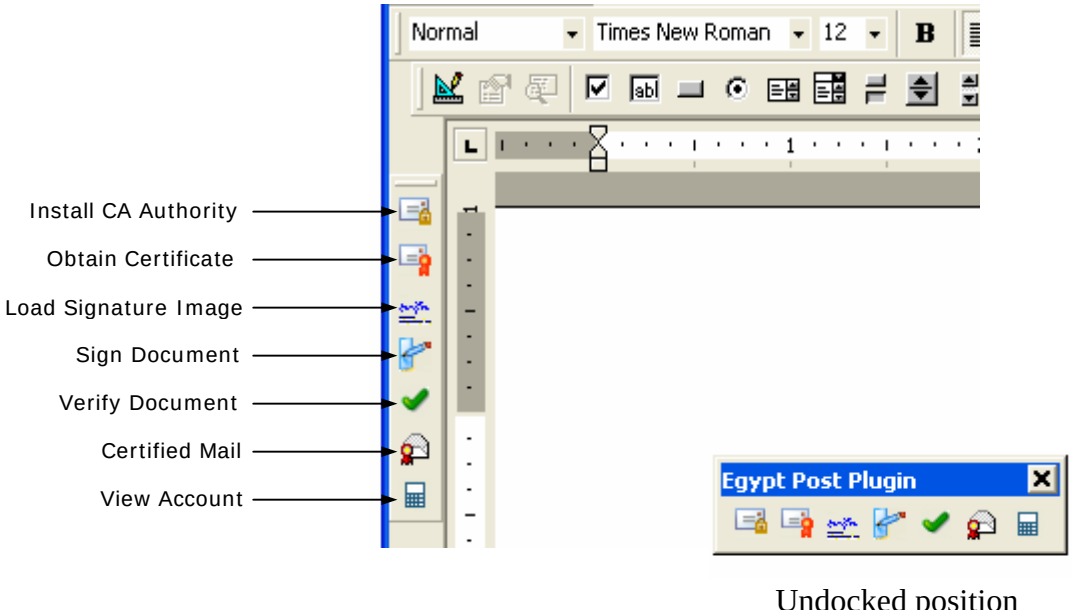
time stamping, since the time and date functions in a computer are relatively easy to manipulate.

How does SANAtech's Electronic Mark solution work with PKI?

The core strength of PKI is strong user-level authentication and digital signing (proving WHO did WHAT). **SANAtech EM** actually extends the trust of PKI by adding trusted time stamps, checking that the signing certificate is not expired, and archiving the transaction for long term non-repudiation. Therefore, **SANAtech EM** is complementary to PKI, but the user does not need to use PKI in order to use **SANAtech EM.**

The **SANAtech EM** is a web-based security service that enables users to verify authenticity, provide tamper detection, and date and timestamp electronic documents and files. Evidence of content authenticity is stored in the **SANAtech EM** repository for several years to ensure trusted non-repudiation of content.

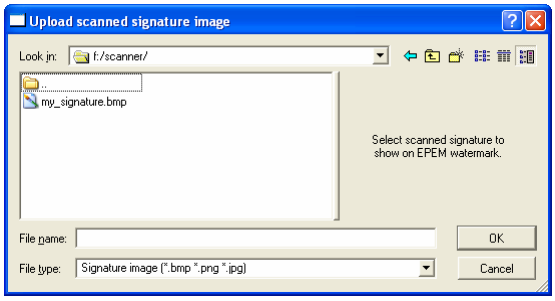
The solution is integrated with the most common user productivity tools, namely; Microsoft office which thus enables users to easily sign and authenticate Word, Excel and Outlook emails.

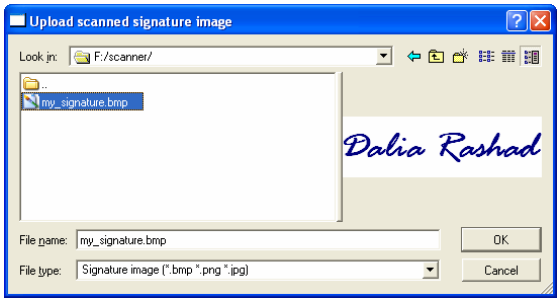


Undocked position

Docked position (default)

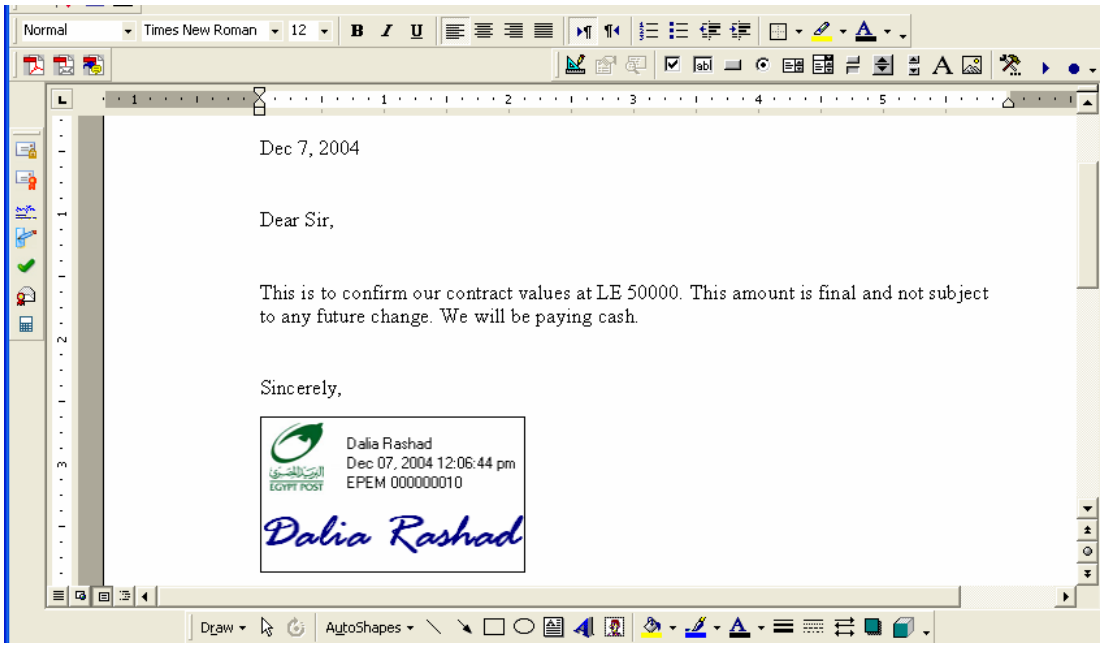
The **SANAtech EM** allows the user to attach a visual signature image which could be obtained using a scanner or otherwise. This image can be easily attached to a user's digital signature such that any use of the digital signature would automatically embed the visual signature together with it.





A user may have multiple certificates as well as define different signatures if needed (such as defining an Arabic and English signature). The scanned image does not have to be of a particular size, it will be scaled accordingly to fit the **SANAtech EM** mark signature area.

On successful transaction the **SANAtech EM** mark is inserted in the document at the chosen insertion location as illustrated below:



The **SANAtech EM** mark displays the following information:

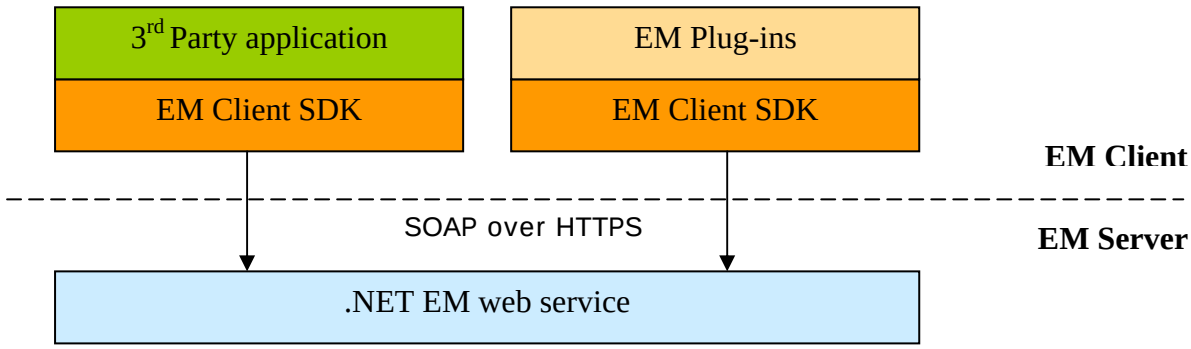
1. Signer name, extracted from the digital certificate.
2. Time extracted from the time stamp token.
3. Visual signature, scaled to fit in the lower half of the EPEM mark.

Advanced manipulation of the Microsoft Word document through its OLE Automation API and published Object Model allows complete control over the visual appearance of the **SANAtech EM**, for example if the **SANAtech EM** was chosen to be inserted over a text area, we allow it to blend with the background document text allowing the text to be visible. We also tested watermark transparency on Office 2003, unfortunately it is not supported on Office 2000 and we think that supporting Office 2000 users is more important (for now).

After successful marking, the document is set as read only; this is to prevent the user from accidentally modifying it. The user can reset it to read/write if he intentionally wants to do so. Also a backup copy of the original unsigned document prior to **SANAtech EM** insertion is also saved with a _backup postfix and is noted to the user.

Solution Architecture

The **SANAtech EM** server is a .NET web service that communicates with the **SANAtech EM** client using SOAP messages over secure HTTPS connection as illustrated in the diagram below:



Any 3rd party e-commerce application can access the the **SANAtech EM** server via the client SDK. The **SANAtech EM** plug-in also use the SDK in the same way, their purpose however is to provide extensions to the most popular desktop software to make it EM enabled.

Legal Strength

The e-Signature law has been approved by the Egyptian Peoples Assembly (parliament) by law 15/2004 in the second quarter of the same year. It will then promote the use of digital signatures and the electronic transactions.

3. Added value through secured applications

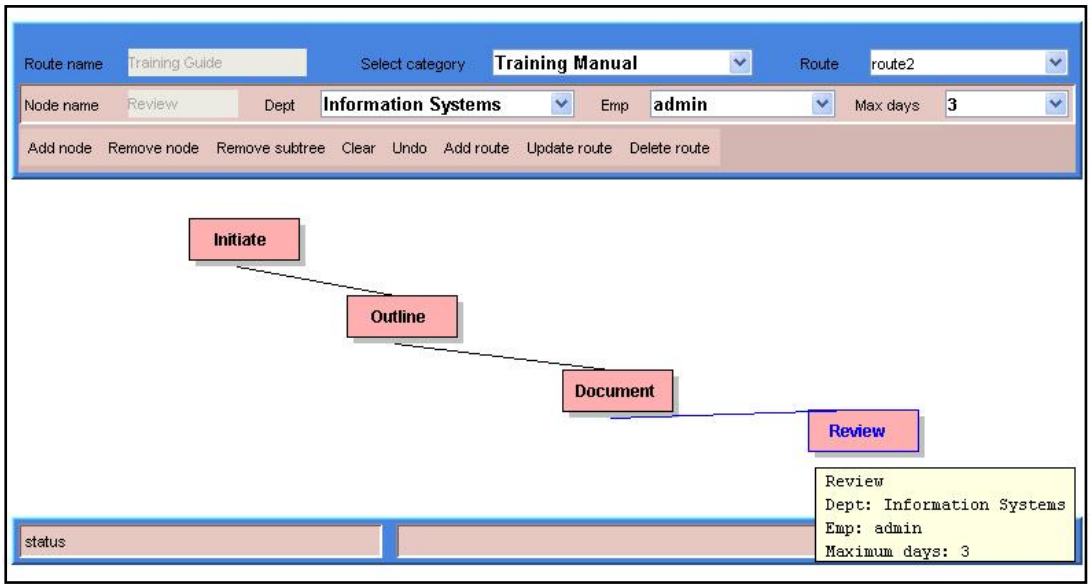
A. Document Workflow

Workflow specifications are descriptions of business processes, which are built from a set of steps called activities. These activities can either be non interactive or bound to an agent (a role or a user). Document workflow can be defined to behave upon certain triggers.
Through these triggers a workflow system can move electronic documents along a routing path from one user to the next throughout your local or wide-area network. You can reengineer and automate the processes by which documents flow through your organization to eliminate unnecessary steps, increase productivity, enhance quality, and speed delivery of services.

By integrating digital signatures with our workflow system, it is possible to define as part of the trigger set whether the document has or has not been signed. Since this information is maintained through the **SANAtech EM** repository, it is accessible to the workflow system.

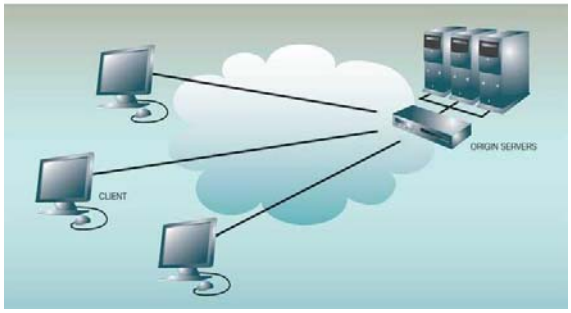
In doing so, we are able to enhance the level of service provided in the form of:

- Added Security
- Increased accountability
- Irrefutable traceability



B. Secured Content Delivery

iCaster is a Content Distribution system designed for high performance, massive scalability and extreme flexibility. **iCaster** gives network managers and service providers complete control over the entire content distribution cycle, it offers the ultimate bandwidth optimization, resource utilization and server offload.



Some of the features of **iCaster** include:

- Unique state of the art bandwidth saving technology providing massive scalability
- High performance communication channels, from 28 Kbps up to 20 Mbps per channel
- Accurate and flexible scheduling functions
- Real time encryption and compression support
- Advanced Forward Error Correction [FEC]
- Allows automatic launching of programs on client reception, such as installers.

Key Applications

- File delivery
- E-Learning
- Web caching
- Software distribution and updates
- Electronic publications
- Corporate communications
- Kiosk updates
- Data replication

By integrating digital security with content distribution, we are able to enhance the level of service by providing added end-to-end security and non-repudiation.