

Call Us Today

Canadian Headquarters
4101 Yonge Street
Suite 708
Toronto, ON, Canada
M2P 1N6
416.226.8600

North American Toll Free:
1.888.697.3246

United States
1870 The Exchange
Suite 1000
Atlanta, GA
30339
1.770.578.6540

Europe
27 Old Gloucester Street
London, United Kingdom
WC1N 3AX
+44.020.7419.8763

ABOUT ECHOWORX™

Leading Provider of Encryption Software

Echoworx is a leading provider of managed encryption services to protect confidential information from unauthorized viewers and makes the encryption of digital information easy. Echoworx' complete encryption strategy for privacy encompasses much more than just data loss prevention. It protects all forms of disparate email data, whether on mobile devices, desktops, in the cloud or on exchange servers.

Echoworx is Deloitte, Microsoft, CCTM and PCI certified. As a SaaS (software as a service) model; is built on best-of-breed technology. Echoworx is the encryption service provider of choice for leading security software and telecommunications and hosted exchange providers, including BT Global Services, Symantec Hosted Services, AT&T, McAfee, Verizon, and Aptix among other global businesses.

www.echoworx.com



Underlying Technology The Power Of Encryption & Credentials

Echoworx Encryption Platform Standards Based Technology

All Echoworx privacy applications leverage the Echoworx Encryption Platform which encrypts data using industry standard PKI (Public Key Infrastructure) and S/MIME technologies providing military grade encryption and digital signatures using standard X.509 certificates.

The Encryption Platform enables rapid deployment and streamlined management of multiple encryption applications all on a common security framework.

The Encryption Platform hides the technological complexities from the end user ensuring ease of use. In most cases the user is not aware of the underlying encryption technology and sends emails as they usually would.

The Encryption Platform resides in high-availability data centers operated by world class application service providers. These data centers optimize data communications, message processing and storage of large volumes of data and offer fully redundant and uninterrupted service levels to users around the world.

BENEFITS

Flexible Deployment

The Encryption Platform is designed to run as a managed service from one of our high availability data centers or on-site within your existing IT infrastructure.

Applications requiring client software can be quickly deployed using a Microsoft Installer (MSI) package.

Centralized Service Delivery

A common administrative console is used across all applications which facilitates centralized management of users, credentials, policies, branding and reporting.

Further reductions in administrative overhead and ultimately cost savings are achieved with automated administrative tasks for deployment, configuration, management, and maintenance activities.

Simplified Key Management

Automated and hosted key and trust services facilitate a better user experience and minimize the operational requirements of an on-site key-management system.

Works with Your Existing Infrastructure

Recognizing that encryption is just one facet of enterprise data protection, the centralized platform architecture has been designed to be flexible and extensible allowing for interoperability with existing email hygiene applications, archiving agents and policy management engines.

Standards Based Technology

Leverage Public Key Infrastructure (PKI), X.509 certificates and S/MIME for strong authentication and encryption. Seamlessly interoperate with governments and business partners who have already adopted solutions based on PKI technology.

Low Total Cost of Ownership

Zero to low up-front capital costs, rapid deployment, minimal operational requirements and metered pricing for each privacy application translates to a low total cost of ownership.

Data Centers



For secure communications Echoworx has data centers in the US, Europe, and Canada, ensuring that customer data stays close to home.

All the data centers are engineered to the highest standards and are designed and maintained without compromise for security or redundancy. What this means is that we provide our customers with the highest level of security for their data.

Our data centers are SAS70 and ISO certified and provide physical, system and operational security. Servers are locked down and all physical access to the servers are logged. Servers are also locked down from the inside with hardened operating systems and up-to-date patching. All business processes follow security best practices and limit access to customer information.

Echoworx continuously reviews the security and services provided by their data centers to ensure the best possible security for their customers.

CENTRALIZED SERVICE DELIVERY

The Administration Console controls how Echoworx encryption applications are used within an organization. Administrators can easily enrol and manage large numbers of customers and employees; control application access; manage policies; credentials; branding; key escrow; and reporting.

Additional capabilities include automated administrative tasks that reduce the complexity of day-to-day operational requirements.

Deployment

The security infrastructure can be hosted as a managed PKI service or can be deployed and managed in-house.

Administration

The Administration Console employs role-based security and enables the enterprise to console functions through a common interface for all encryption applications.

User Management

Supports individual or batch provisioning of end users and system administrators. Administrators can easily manage the status of any user and the encryption applications they have access to.

Credential Management

Facilitates full credential lifecycle management including revocation and recovery. Integrated key escrow enables enterprises to optionally gain authorized access to the PKI keys of its employees.

Policy Management

Customize security policies and application policies to meet email and data protection requirements specific to an organization and industry.

Branding

The branding module enables customization of any email, web or application interfaces with your brand, corporate color scheme, company logos and more.

Reporting

Allows for logging, monitoring and reporting across multiple encryption applications using a consistent interface.

SIMPLIFIED KEY MANAGEMENT

To reduce the complexities of key management, the Encryption Platform relies on core functions provided by Key Services and Trust Services. These services automate functions related to authentication, encryption and digital signatures to ultimately provide a better user experience and minimize the operational requirements of a public key-based system.

Key Services

Key Services is a stand-alone service supporting all encryption applications. It consists of a dual key-pair PKI model (cipher and signature) system and a network-based repository of subscriber's credentials (certificates). Key Services also performs key functions related to subscriber registration and password recovery as detailed below.

Signature Keys

A principal uses the private signature key in the production of a digital signature.

The message recipient verifies the digital signature using the public signature key. Password authentication to the signature key can be replaced or augmented with additional security factors such as smart cards, hardware tokens, or biometrics.

Certificate Registration

This service interface provides a registration authority i.e. a trusted agent of the certification authority. It first verifies that the subscriber is entitled to a Secure ID (by ensuring that the account has been provisioned in the directory) before it invokes the key provisioning component to generate both dual key-pairs and issue certificate signing requests to be forwarded to the certification authority. Once issued, the certificates are placed in the directory and returned to the client.

Different levels of trust certification can be issued depending on what kinds of transactions the user requires authorization to. Higher levels of certification require additional authentication during the enrolment process.

Password Recovery Service

Key Services also provides the subscriber with the ability to securely store a password in a network-based repository and securely retrieve it from any web connected system when needed (i.e. if forgotten). The subscriber associates a number of memorable hint questions and answers with the password to be guarded; only a valid combination of questions with the correct answers will release the password.

As an added security measure to deter and detect online attacks, a two-stage process requires the subscriber to respond to an instructional message sent to their registered email address; this message contains a temporary web address link to a secure web location where the subscriber is authenticated before the password is revealed over a secure SSL/TLS connection.

The subscriber can register a new password (in place of the existing one) only after successfully authenticating to the service.

Roaming Mobile Access

When using webmail applications, the subscriber is prompted for their password in order to be authenticated. Key Services then allows the subscriber's ID credentials to be transparently downloaded over a SSL connection. When the secure email session is terminated or expires, the cached credentials (notably, the private key) are deleted (i.e. securely wiped) from the client machine.

Trust Services

Trust Services relate to the management of digital certificates within a public key infrastructure. Certificates are digitally signed documents, issued by a certification authority, that attest to the validity of the logical binding between a principal user (identified by a unique distinguished name) and a public key, for which only that principal should have the corresponding private key. A dual-key PKI model is used, meaning that separate key-pairs are logically bound to a principal.

Cipher Keys

A private cipher key is used to decrypt a secure (i.e. cipher-text) message or file encrypted by a correspondent using the associated public key. The rationale for a dual-key model, as opposed to a single-key model, is to separate the management of keys for different purposes. The escrow of cipher key allows for key escrow at the enterprise or provider level without introducing issues of repudiation against digital signatures.

Certificate Lookup

This service interface provides an HTTP-based proxy agent by which the encryption applications can retrieve certificates from a directory server.

Certificate Validation

This service interface provides the client with the ability to check the validity of a certificate. In the context of email, it inspects the validity of the message and provides online certificate validation responder capabilities that checks whether a certificate has been revoked (i.e. published on a certificate revocation list or 'CRL').

THIRD-PARTY INTEROPERABILITY

The Echoworx Secure Content Manager module is a Platform extension that enables message encryption services to seamlessly co-exist with third-party email hygiene applications (anti-virus, anti-spam, content scanning, etc.), archiving agents and policy management engines. It ensures that all inbound and outbound messages adhere to the corporate content policy, remain free of malicious and harmful content and do not interfere with indexing and archiving functions. It addresses these needs through an open application programming interface (API) that integrates with these third-party technologies.

SCM Architecture

SCM provides Java JNI, SOAP, and SMTP interfaces which can accept S/MIME and return n MIME message. Optimized performance is achieved via caching and support for multiple instances; this allows any application to present an email message over any of the supported interface and to return the appropriate version for further processing. SCM communicates over a secure channel with the Encryption Platform for securely accessing cryptographic key materials to facilitate encryption and decryption of email messages on demand using key escrow infrastructure.

INDUSTRY STANDARD ENCRYPTION

Public Key Infrastructure (PKI) was invented more than thirty years ago and is the de facto standard for enabling strong authentication and encryption for businesses and governments around the world.

PKI is used throughout the Internet today to secure data transmission via well know protocols such as SSL and TLS. By binding the identity of a user or device to a certificate and through core functionality that determines which certificates are trustworthy, PKI is inherently more secure than solutions that do not rely on certificates.

Standards

- Echoworx technology leverages industry and internationally recognized standards used by Government, Military and Banks
- Standards include PKI, X.509, SMIME, and SSL
- Echoworx is interoperable with other standards-based systems including Verisign, Entrust, Vontu, and IBM.
- Echoworx also uses the strongest commercially available cryptography known to the industry
- The Echoworx suite of privacy applications and the Encryption Platform are built on the following industry accepted standards for digital signatures and encryption:
 - 1024 bit RSA End-user Keys
 - 2048 bit RSA CA Keys
 - SHA-1 hash
 - PKIX X.509 v3 certificates & CRLs
 - PKCS#10 certificate signing request
 - PKCS#12 key storage
 - 3DES and AES-256 symmetric encryption
 - S/MIME PKCS#7 encrypted e-mail format
 - HTML / XML, HTTP 1.1 / SSL
 - 2048 bit CA keys
 - CA Key Generation/Protection
 - CA Keys generated/stored on SafeNet LunaSA HSM
 - Keys signed by WebTrust certified Echoworx ROOT CA

In addition to providing interoperability with governments and business partners who have already adopted solutions based on PKI technology, standards-based encryption and authentication is also imperative when meeting digital signature requirements and in matters that deal with the legal admissibility of encrypted messages and data.