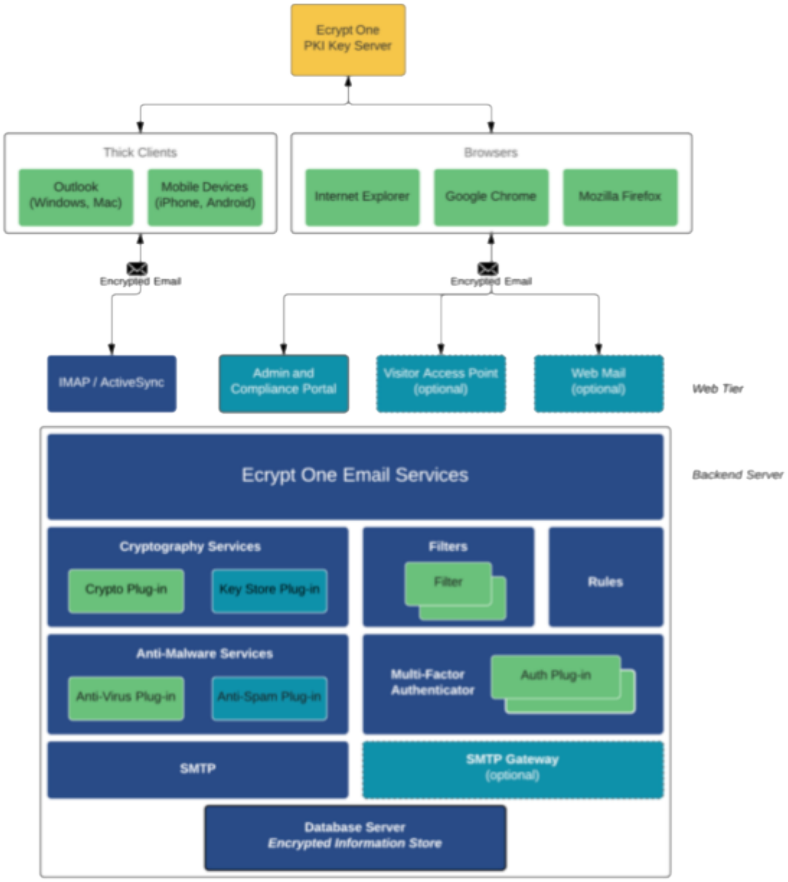
Ecrypt One for Military and Intelligence Agencies

A solution designed to meet the email security needs of the most privacy and security conscious organizations.

Full service, multi-protocol email

Ecrypt One MI is a complete email solution with innate security.



System Landscape

Benefits

Reduce administrative burden of email

A single management console for email system and its built-in security allows administrators to be more efficient.

Eliminate the human vulnerability in email communications

Dependable and automated security and eliminated exposure to email borne attacks like phishing, enhance security, improve the end user experience and reduce workplace stress.

Enable interoperability between disparate organizations

Encrypted links, content filtering and security rules secure email communications while ensuring absolute control and the ability to restrict communications to an “as needed” basis to prevent unauthorized connections and exchanges.

Variable risk tolerance

Configure the system to your specific risk tolerance thresholds depending on the sensitivity of the operation.

Safely expose some groups to Internet email, while entirely restricting exposure for others.

Features at a Glance

Email

- Multiple server support with variable crypto private link
- IMAP/SMTP and Active Sync protocols
- Contacts and Calendar synchronization
- Embeddable and secure Web Mail and Secure Visitor Access Point
- Standard and custom content filtering
- Rules engine for information rights management

Cryptographic Key Storage

- Windows Keystore, and Ecrypt Encrypted Keystore
- Hardware Encrypted Keystore and custom Keystore plug ins supported

Encryption

- AES, Blowfish, Elliptic Curve encryption algorithms
- PKI, PGP
- SSL

Authentication

- Two factor: SMS, email, Google Authenticator,
- Compatible with Smartcard and Biometric authentication
- Custom authentication plug ins supported

Standards and Compliance

- Extensible reporting
- FIPS compliance mode
- Government Cloud hosting option

Mobility

- Compatible with iOS, Android, Windows Phone, BlackBerry
- MDM integration
- Mobile PKI security

Secure implementations of popular push email protocols – ex: ActiveSync - and common protocols - IMAP, POP and SMTP - provide cross-platform compatibility.

Enterprise calendaring, meetings and address book management ensure a seamless transition for workplace and mobile users.

Thick Client and Browser Compatibility

Ecrypt One MI email is secure on all commonly used email clients and web browsers - whether on desktops, smartphones or tablets - without additional software.

Security and Privacy First

Ecrypt One MI brings a new paradigm in email by offering a complete and consolidated email and email security system, tailored to the most security and privacy conscious organizations.

Deployments can be configured to suit risk tolerance and compliance needs, including new ways to safely expose email to the Internet… if such exposure is needed.

Always-on Encryption

Whether in motion or at rest, Ecrypt One MI data is persistently and automatically encrypted.

All internal system traffic is encrypted. Thick client and browser connections to the server are exposed over secure SSL only. Push mail and standard protocols such as IMAP are only allowed over secured connections.

Role Based Access Controls

Role based access controls prevent arbitrary administrator access to email system resources/services and data.

Information Rights Management

Server side security rules enable control over what information is sent, when, and to whom. They further define the level of access granted to email contents (including attachments): can information be copied?

Downloaded? Forwarded? Perhaps it can only be viewed a single time.

Security rules leverage technology to force compliance with email security policies.

Two-Factor Authentication

Ecrypt One MI offers multiple two-factor authentication options. From basic ones like SMS and email, to more advanced ones like Google Authenticator and Enterprise Sentinel. It also supports Smartcard systems, and advanced authentication solutions like biometrics.

Ecrypt One MI will even work with custom solutions not commercially available.

Securing Mobile Devices

Integration with Mobile Device Management and Mobile PKI solutions enables greater control over access from smartphones and tablets.

Laptop physical security devices available exclusively through Ecrypt protect against physical threat by actively detecting attempted theft, or tamper, and responsively invoke protective actions.

Yes to PKI

The system also offers a PKI option. But if you already have one in place, it can interoperate with existing PKI systems, including PGP and Open PGP.

Variable Risk Tolerance

Not every role is equal. Some groups have lower risk tolerance thresholds than others based on their objectives and the sensitivity of the information circulated over email.

Define varying risk tolerance thresholds for multiple intra- and interconnected groups. Customize permissions, restrictions and features based on risk tolerance.

Smart Data Loss Prevention

A combination of server-side security and information rights rules, and content filtering leverage the power of technology to prevent email borne data leaks.

Automated and persistent, Ecrypt One MI’s data loss prevention capabilities eliminate the human factor in the security decision-making process, and force compliance with policies.

Variable and Flexible Data Encryption

Ecrypt One MI offers multiple encryption algorithm options: AES, ECC and Blowfish come standard. It’s also fully compatible with custom implementation.

Ecrypt Encrypted Keystore

The Ecrypt Encrypted Keystore is a double-encrypted dual-authentication storage vault for valuable crypto secrets.

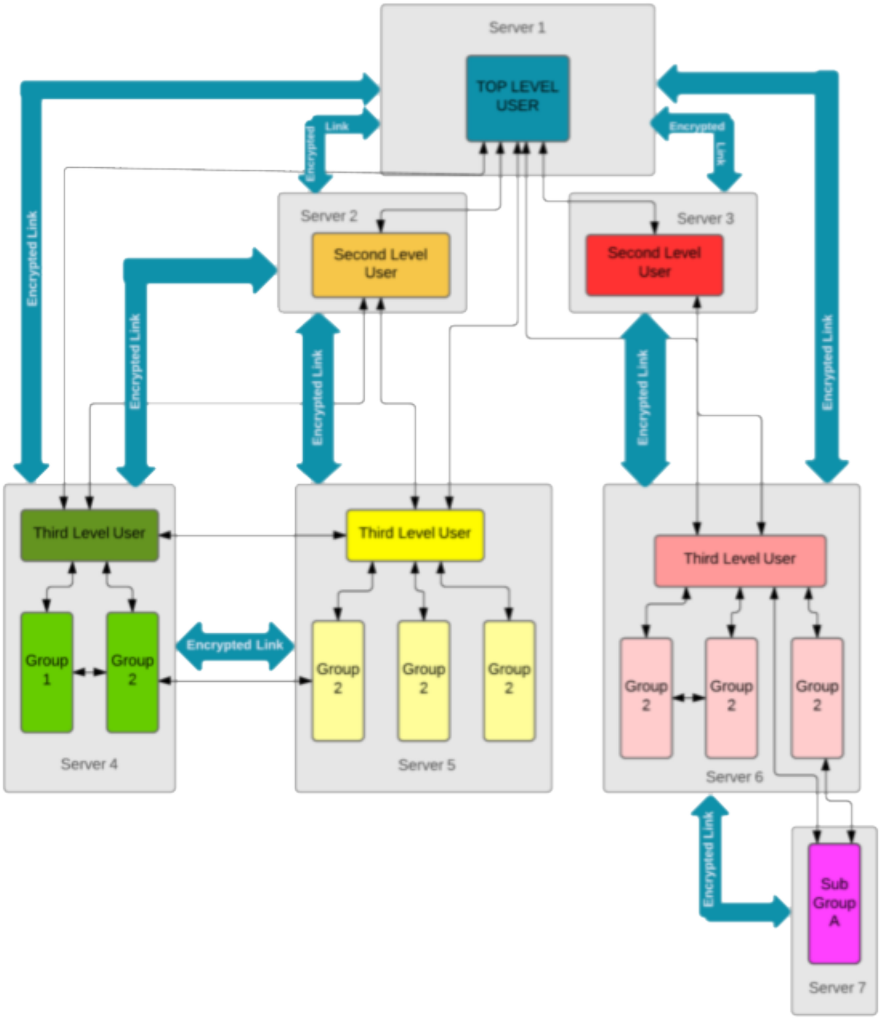
Hardware Encrypted Keystore

Ecrypt One MI is compatible with hardware security modules to offer security that exceeds the scope of purely software-based technology.

Custom Keystore Plugins

Using a custom encryption keystore solution? Ecrypt One MI can work with that too.

Hierarchal Email Routing



Hierarchal Mail Routing Using Encrypted Links and Security Rules

Hierarchal email routing enables agencies to communicate securely with each other without compromising internal security, group leadership, and personnel divisions.

It enables multiple groups to selectively and securely co-operate, while maintaining a self-contained, security isolated, and secure environment using variable encryption, technical security controls, permissions, and smart delivery mechanics.

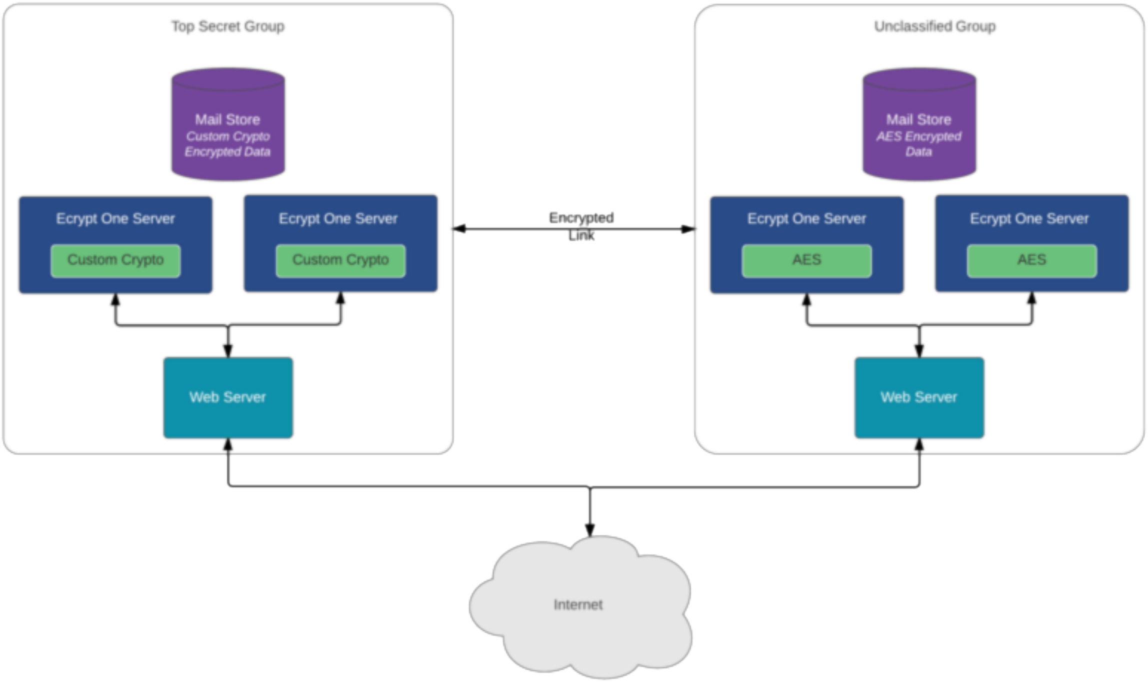
Encrypted Links

Software-generated, private protocol encrypted links between servers ensure control over the end-to-end security of a connection. They can be used to connect disparate groups, departments, agencies and even governments.

Links are automatically managed by the system to prevent misconfiguration errors. Automated crypto negotiation capability facilitates the application of various algorithms - from AES and ECC to custom implementations - based on need.

This mechanism can be used to select between available encryption algorithms in order to differentiately secure email communications depending on their classification or destination.

Unlike standards such as StartSSL, Ecrypt One MI encrypted links are *always* secure and cannot be compromised.



Deployment using Encrypted Links with Variable Crypto Negotiation

Embeddable Secured Web Access

Ecrypt One MI comes standard with two secured, embeddable, white-label web access portals:

Secure Web Mail

Designed for incidental access by internal users to their email accounts.

Secure Visitor Access Point

A secure web based email access portals for outsiders. Offering limited features and imposing stringent information rights controls, the Visitor Access Point was designed for email communications with those external parties that do not have an Ecrypt One server.

Compliance and Reporting

Ecrypt One MI's advanced security methods and technologies ease compliance with regulations such as HIPAA, GLBA, PCI and FISMA. Federal security requirements like FIPS and IPv6 are supported.

The system is fully auditable and provides a Security and Compliance Officer dashboard for easy access to reports and other vital information administration.

The solution design enables compartmentalization within a single system while supporting distributed auditing and reporting.

Open Standards

Ecrypt One MI uses open standards where possible - for example, the system integrates with Windows Active Directory using Secure LDAP - to ease transition and ensure the highest levels of interoperability, availability, and compatibility with existing and future enterprise infrastructures.

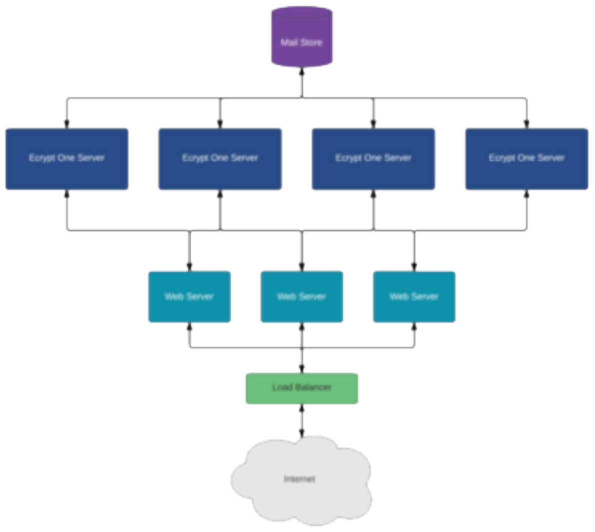
Software-based Solution

Easily conforms and integrates into existing network enterprise equipment.

Ecrypt One MI is a software appliance upgrade to ensure the confidentiality, integrity, and non-repudiation of government data.

Flexible Deployment Options

Ecrypt One MI can be deployed on-premises, in the cloud, or a combination of both. It is designed to be scalable through support for load balancing.



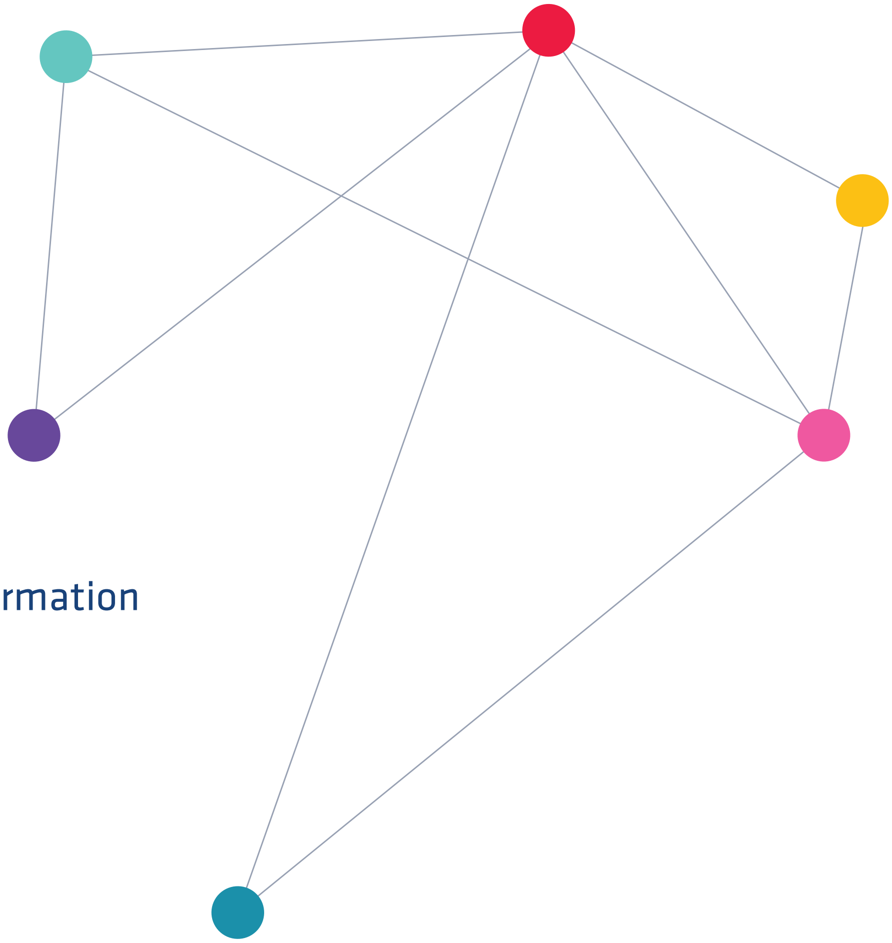
Large Scale Deployment

Server Software Specifications

Installation Platform Requirements
• Windows Server 2008 R2 for x64 with Service Pack 1 • Windows Server 2012 with Service Pack 1 • Windows Server 2012 R2
Database Server Requirements
• Microsoft SQL Server 2008 with Service Pack 3 • Microsoft SQL Server 2012 with Service Pack 2 • Microsoft SQL Server 2014
Supported Client Environments
• Microsoft Windows 7 (Professional and Enterprise) with Service Pack 1 (32-bit and 64-bit) • Microsoft Windows 8 (Professional and Enterprise) (32-bit and 64-bit) • Microsoft Windows 8.1 (Professional and Enterprise) (32-bit and 64-bit) • Apple iOS 7 • Android 4.2.2 and newer • Microsoft Windows Phone 8
Supported Client Browsers
• Microsoft Internet Explorer 10 • Microsoft Internet Explorer 11 • Google Chrome (for Windows and Android) • Mozilla Firefox

Ecrypt One Editions

Email	Ecrypt One MI	Ecrypt One Gov.	Ecrypt One	Ecrypt One Light
Multiple server support with Encrypted Link	✓	✓	✓	
Multiple server support with Variable Crypto Encrypted Link	✓			
IMAP/SMTP protocols (pull)	✓	✓	✓	✓
ActiveSync protocol (push)	✓	✓	✓	✓
Contacts and Calendar synchronization	✓	✓	✓	✓
Web Mail and Visitor Access Portal				✓
Embeddable Web Mail and Visitor Access Portal	✓	✓	✓	
Standard Content Filtering	✓	✓	✓	✓
Custom Content Filtering	✓	✓	✓	
Rules Engine for Information Rights Management	✓	✓	✓	✓
Cryptographic Key Storage				
Windows Keystore	✓	✓	✓	✓
Ecrypt Encrypted Keystore	✓	✓	✓	✓
Hardware Encrypted Keystore compatibility	✓	✓	✓	
Custom Keystore plug-in support	✓			
Data Encryption				
AES data encryption	✓	✓	✓	✓
AES, Blowfish and Elliptic Curve encryption	✓	✓	✓	✓
Custom encryption plug-in support	✓			
Authentication				
Two-factor authentication via SMS	✓	✓	✓	✓
Two-factor authentication via email	✓	✓	✓	✓
Google Authenticator integration	✓	✓	✓	
Smartcard authentication integration	✓	✓	✓	
Biometric authentication support	✓	✓	✓	
Custom two-factor authentication support	✓	✓	✓	
Security				
Outlook Public Key integration (PGP)	✓			
Public Key security services	✓			
Standards and Compliance				
Basic auditing and reporting				✓
Enhanced, extensible auditing and reporting	✓	✓	✓	
FIPS compliance mode	✓	✓	✓	
Government Cloud hosting option	✓	✓		
Security standards compliance	✓	✓	✓	
Mobility				
iOS, Android, Windows Phone, and BlackBerry OS compatibility	✓	✓	✓	✓
Mobile Device Management system integration	✓	✓	✓	
MDM PKI security support	✓	✓	✓	



Contact us for more information

BRAVATEK SOLUTIONS, INC.

Call us at 1.866.204.6703

Email us at sales@bravatek.com

Visit us at www.bravatek.com

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.