Ecrypt One Light for SME's and Single Location Organizations

A solution designed to compensate for human weakness and augment human capabilities, enabling companies to reclaim control over information system resources, limit exposure to threats, support compliance, and significantly reduce risk tolerance.

Full service email

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

Thick Client and Browser Compatibility

Ecrypt One Light 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 Light 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.

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

Content filtering and security rules secure email communications while ensuring absolute control and the ability to restrict email use to an "as needed" basis to prevent unauthorized communications.

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

Email

- Multiple server support with private link
- IMAP/SMTP protocols
- Secure Web Mail and Secure Visitor Access Point
- Standard content filtering
- Rules engine for information rights management

Cryptographic Key Storage

- Windows Keystore,
- Ecrypt Encrypted Keystore

Encryption

- AES, Blowfish, Elliptic Curve encryption algorithms
- SSL

Authentication

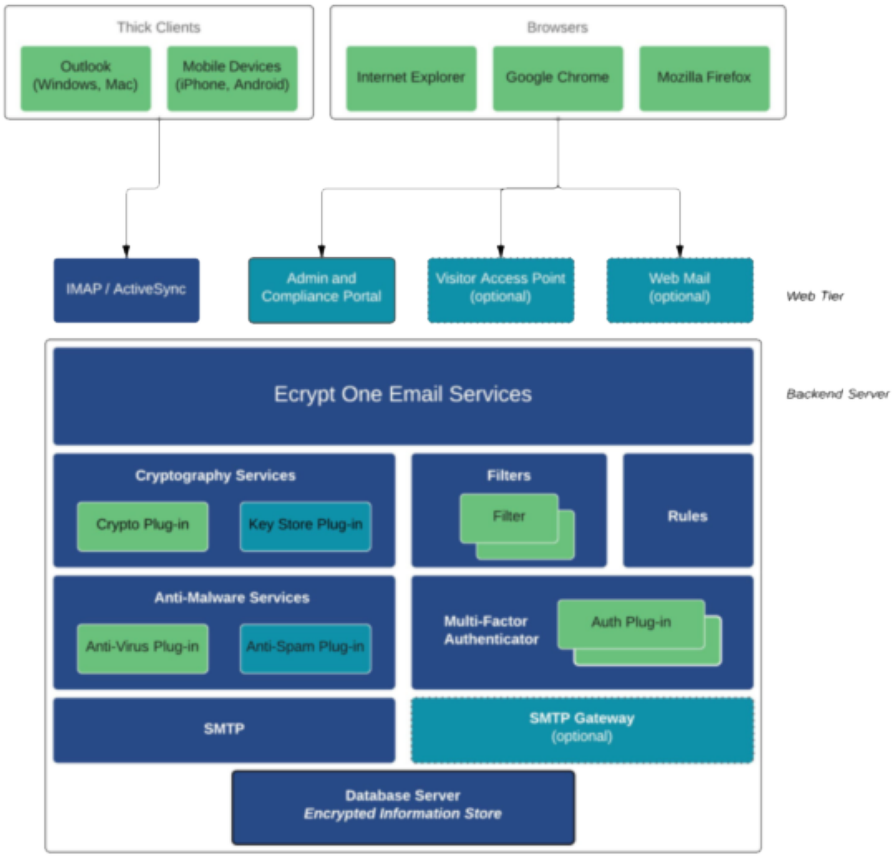
- Two-factor authentication via SMS
- Two-factor authentication via email

Standards and Compliance

- Auditing and reporting
- Compliance and Security Officer dashboard

Mobility

- Compatible with iOS, Android,



System Landscape

Always-on Encryption

Whether in motion or at rest, Ecrypt One Light 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 Light offers two-factor authentication via SMS and email.

Securing Mobile Devices

Optional integration with Mobile Device enables greater control over access from smartphones and tablets.

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 Light 's data loss prevention capabilities eliminate the human factor in the security decision-making process, and force compliance with policies.

Flexible Data Encryption

Ecrypt One Light offers multiple algorithm options: AES, ECC and Blowfish.

Smart and Secure Key Storage

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

Secured Email Web Access

Ecrypt One Light comes standard with two web access portals for email:

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.

The VAP is an ideal platform to connect with customers, vendors and contractors.

Compliance and Reporting

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 Light 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.

Flexible Deployment Options

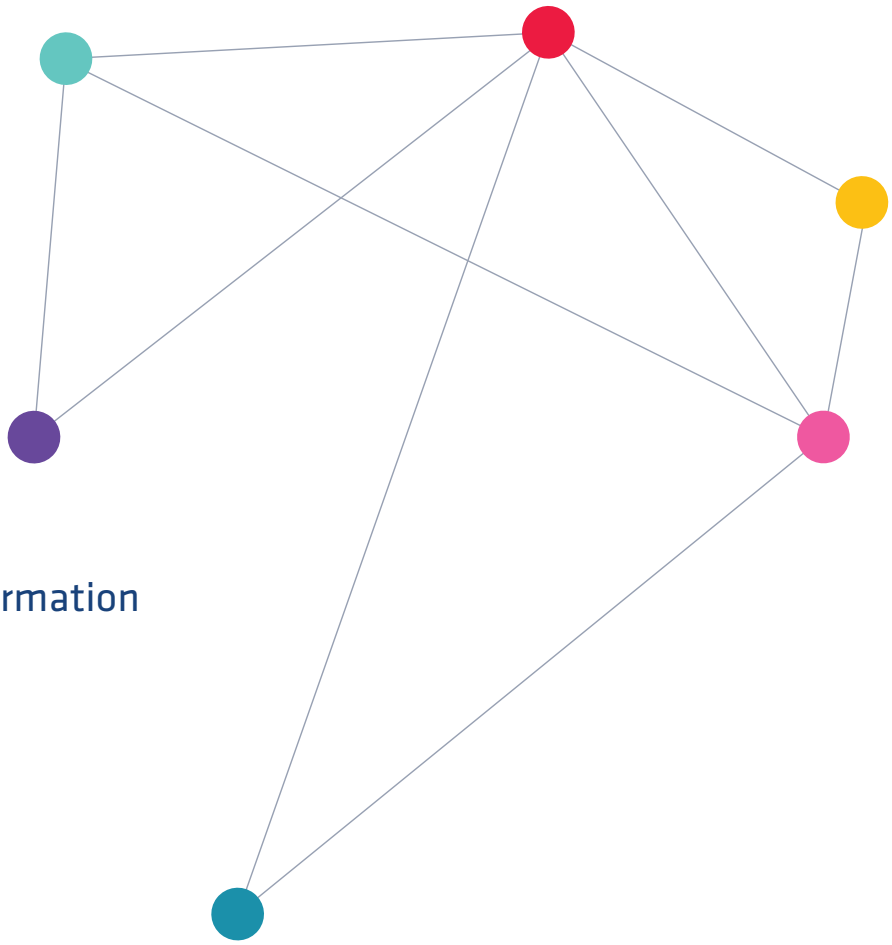
Ecrypt One Light can be deployed on-premises, in the cloud, or a combination of both. It is designed to be scalable through support for load balancing.

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