

SystemBind Hosted Services Information Security Overview

Version 1.0.1



Last Updated: November 2009

© Copyright SystemBind Consulting and IT Services Inc.

Table of Contents

Preface	3
Web-Based Services and SSL.....	3
Email and TLS (STARTTLS).....	4
Disk Encryption	4
References.....	5

Preface

At SystemBind Consulting & IT Services Inc. information security is a core focus. Being a provider of remote and onsite IT technical support and managed, hosted IT services a great level of detail is utilized when information security policies are derived and the resulting technologies are implemented.

This document is intended to provide SystemBind customers with an overview of the core information security implementations present within the suite of SystemBind's service offerings. This document acts as a base for our core information security offerings and aims to provide a general understanding of the related technologies, but does not cover the full spectrum of solutions offered by SystemBind.

Web-Based Services and SSL

All core web-based services offered by SystemBind are delivered with the recommendation to deliver them via SSL (Secure Sockets Layer) encrypted channels.

SSL, like most modern security protocols, is based on cryptography. When an SSL session is established, the server begins by announcing a public key to the client. No encryption is in use initially, so both parties (and any eavesdropper) can read this key, but the client can now transmit information to the server in a way that no one else could decode. The client generates 46 bytes of random data, forms them into a single very large number according to PKCS#1, encrypts them with the server's public key, and sends the result to the server. Only the server, with its private key, can decode the information to determine the 46 original bytes. This shared secret is now used to generate a set of conventional RC4 cipher keys to encrypt the rest of the session.¹

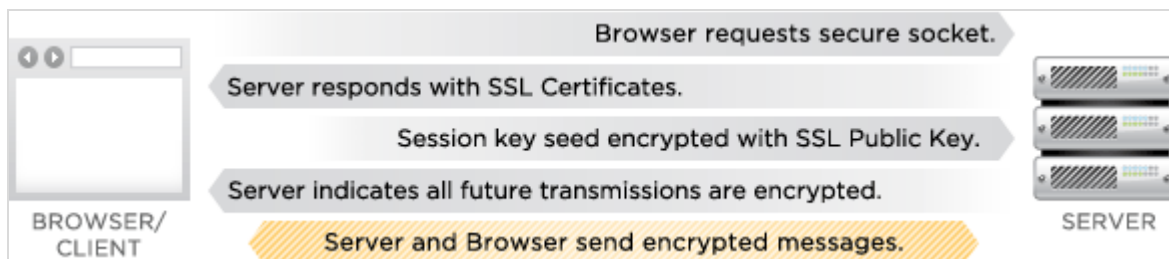


Figure 1: An example of SSL communication²

With SSL-encrypted web-based services, SystemBind's customers are protected from Internet 'traffic sniffers' and are thus immune to malicious attempts at intercepting the data transmitted through these services.

Following are examples of web-based, SSL-protected services that SystemBind offers:

- CRM (Customer Relationship Management) systems
- Collaboration and content management systems
- Custom corporate web-based applications
- Shared calendars and contact 'Free/Busy' information

Email and TLS (STARTTLS)

Similar to SSL, TLS (Transport Layer Security) is used within SystemBind's email-based services to encrypt email transmission. Using TLS, end-users utilizing SystemBind's hosted email services experience secure messaging.

STARTTLS is the ESMTP keyword used to initiate a secure SMTP connection between two servers using the Secure Sockets Layer (SSL) (also known as TLS).

Once the connection has been successfully established all further communication between the two servers is encrypted. This means that the source and destination email address and the entire message contents are all encrypted during transfer.³

Disk Encryption

Dedicated server deployments, virtual server deployments and off-site backup services provided by SystemBind all offer 'Disk Encryption' as an optional add-on. Disk Encryption presents customers an extra layer of protection when storing sensitive data at one of SystemBind's data centre locations.

With Disk encryption, data is stored in an encrypted format and is usually either password-protected or protected with a security 'key'. In the event of theft or other successful malicious actions to obtain the encrypted folder or encrypted physical hard drive the culprit attacker will not

be able to read or use the stolen data. With such technology the contents of the stolen data is rendered unusable by the attacker.

SystemBind generally deploys two methods of Disk Encryption:

File-System Encryption

Filesystem-level encryption, often called file or folder encryption, is a form of disk encryption where individual files or directories are encrypted by the file system itself.

On-The-Fly Encryption

On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc)⁴.

References

- 1) Brent Baccala, Editor, *Connected: An Internet Encyclopedia*
baccala@freesoft.org, April, 1997
- 2) VeriSign, Inc., *SSL Certificates*
verisales@verisign.com
- 3) Gordano Limited, *Gordano Knowledge Base Article Q1450*
support@gordano.com, 29-Aug-2007
- 4) TrueCrypt Foundation
inquiries-other@truecrypt.org