

Ahsay™ Backup Software

Whitepaper – Data Security

Version 6
Apr 2011

Table of Content

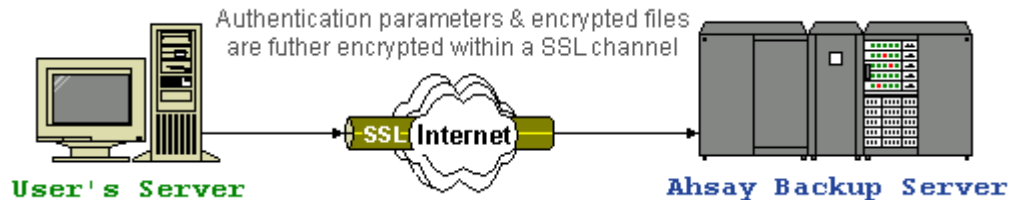
1	Introduction	3
2	Ahsay Offsite Backup Server – “Secure, Robust and Reliable”	4
2.1	Secure 128-bit SSL communication	4
2.2	Backup data are securely encrypted.....	4
2.3	Encrypting key are well protected	5
2.4	Best encryption algorithm is used.....	5
2.5	Require 1.46×10^{54} years to crack the 256-bit encryption	5
2.6	Restrict access to data by IP addresses	5

1 Introduction

This document describes the security measures available in Ahsay Online Backup software from the user's perspective. It serves as a reference for partners when addressing customers' queries on security.

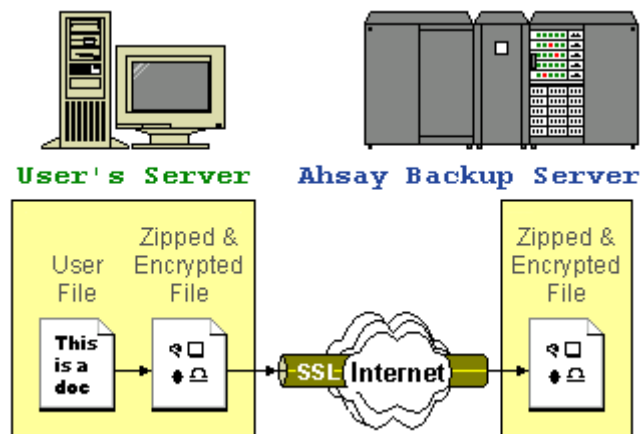
2 Ahsay Offsite Backup Server – “Secure, Robust and Reliable”

2.1 Secure 128-bit SSL communication



All communications between Ahsay Backup Server and your computer are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), eavesdroppers have no knowledge of what has been exchanged.

2.2 Backup data are securely encrypted



All of your files are first zipped and encrypted with your defined encrypting key before they are sent to Ahsay backup server. To all people but you, your files stored on Ahsay backup server are no more than some garbage files with random content.

2.3 Encrypting key are well protected

The encrypting key used to encrypt your files resides only on your computer and is known only to you. Thus, even the system administrators will not be able to decrypt and view the content of your files stored on the backup server without your permission. This unfortunately means if the encrypting key is lost, you will never be able to recover your backup files.

Technical Details

The encrypting key for the different backup sets are stored the config.sys file, which is encoded by a proprietary algorithm:

```
(Windows)    %USERPROFILE%\\.obm\config\config.sys
(Linux)      ~/.obm/config/config.sys
(Mac OS X)   ~/.obm/config/config.sys
```

If client software cannot locate the config.sys (due to accidental deletion or logon to a new machine with the same account), it will prompt the user to re-enter the encrypting key for the backup set and then store it in the local config.sys.

2.4 Best encryption algorithm is used

Currently, the algorithm that we are using to encrypt your files is Advanced Encryption Standard (AES), with 256-bit block ciphers. It is adapted from a larger collection originally published as Rijndael. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) of USA for top secret information.

2.5 Require 1.46×10^{54} years to crack the 256-bit encryption

A 256-bit key size has 2^{256} or around 1.16×10^{77} possible combination. Even if you have the world best super computer, Tianhe-1A, with 14,336 Xeon X5670 (6 Core, 2.93GHz) processors developed by the Chinese National University of Defense Technology as of October 2010, it would take 1.46×10^{54} years to test all combinations. Assuming you have the super computer, Tianhe-1A which totals a capability of 2.507 petaflops (quadrillion of operations/second), available to you. Also it just needs one computer operation to test a possible combination (which is already faster than what it can do). To use brute force attack (checking all combinations) on this encryption algorithm, it would take:

$$\frac{1.16 \times 10^{77}}{2.507 \times 10^{15}} \text{ seconds} \sim 4.621 \times 10^{61} \text{ sec}$$

i.e. 1.46×10^{54} years

to successfully try all combinations. Let alone Tianhe-1A cannot process as fast as what described here. You can be sure that your data stored on our server is 100% secured.

2.6 Restrict access to data by IP addresses

You can also restrict access to your backup files from the set of IP addresses you defined. If someone tries to access your data from an IP address not on your defined list, their access will be denied. This additional security ensures backup files are not open to all location, even username and password are known.