



WHITE PAPER

## Filemail Corporate Security

November 2009

Copyright © 2007-2009 Filemail.com AS.

The information contained in this document represents the current view of Filemail.com on the issue discussed as of the date of publication. Because Filemail.com must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Filemail.com, and Filemail.com cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for information purposes only. FILEMAIL.COM MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Filemail.com may have patents, patent applications, trademark, copyright or other intellectual property rights covering the subject matter of this document. Except as expressly provided in any written license agreement from Filemail.com, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Filemail.com, the Filemail.com Logo, are trademarks of Filemail.com in Norway and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Filemail.com AS, Brugata 1, 0186 Oslo, Norway (+47 24 10 28 28)

# Contents

- Introduction..... 4
- Intended audience ..... 4
- Basic overview of Filemail.com ..... 4
- General website communication and security ..... 4
- Security Mechanisms when sending files - from the sender’s perspective ..... 5
- Security Mechanisms when downloading files - from the recipient’s perspective ..... 6
- Physical server security and integrity ..... 6
- Backup ..... 6
- Handling of credit card information ..... 6
- Security References..... 6

## Introduction

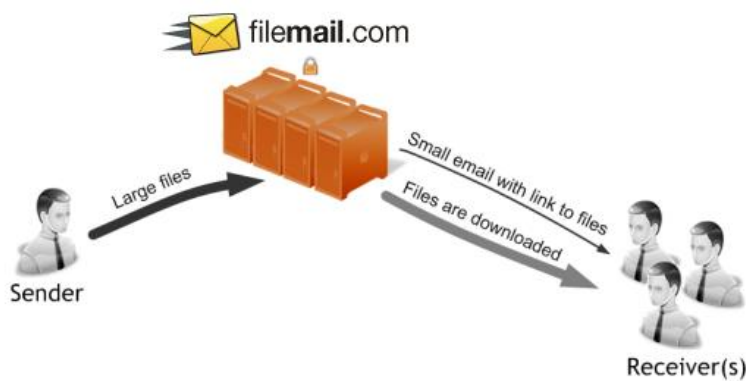
Security is a top priority of Filemail.com, its employees and of course its users. For this reason, we have had this issue in mind ever since we started to plan and design this service back in 2007. This whitepaper provides an overview of the security mechanisms implemented in order to ensure the security and integrity of our system. Internal/sensitive security features and principles are not described here, as this could be abused by hackers/crackers.

## Intended audience

This paper is intended for the following audiences:

- IT managers and system administrators who are interested in the security of Filemail.com
- Network administrators who are interested in the network / communication aspects of Filemail.com

## Basic overview of Filemail.com



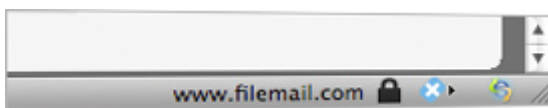
First, the files you want to send are uploaded to one of several filemail.com fileservers currently located in Oslo (Norway), Frankfurt (Germany) and St. Louis (USA) and Johur Baharu (Malaysia). The location of the sender will determine what fileserver that is to be used (the closest one).

1. A small e-mail is delivered to the recipients, containing a short message from the sender and a hyperlink where the files can be downloaded.
2. The recipients click the hyperlink in the e-mail, and are taken to the download page. After the specified number of days/number of downloads, the files are removed completely from our servers.

## General website communication and security

After logging in with a premium or corporate account - all communication with the Filemail.com website is done over HTTPS/SSL. Free users browse the website using plain http - thus less secure. Filemail.com has acquired official HTTPS/SSL certificated for all its servers from Equifax Secure Inc.

This can be observed in the browser - a lock is displayed.



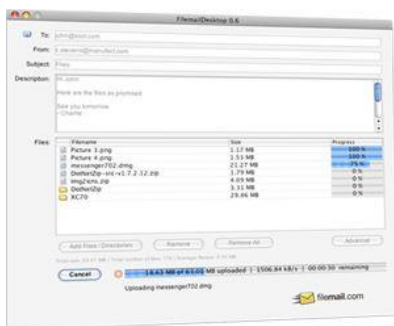
## Security Mechanisms when sending files – from the sender’s perspective

### Sending files from the website

When using the website to send files to or from a premium or corporate account - the content of the file is sent to the fileserver using HTTPS/SSL. This means that the content of the file is encrypted with an asynchronous 128bit key, then transmitted, and finally decrypted on the fileserver before being written to disk. This (HTTPS/SSL) is the de facto standard for transferring sensitive content on the internet today, and is being used in a variety of solutions - e.g. net banking, stock trade and commercial sites such as ebay.com.

HTTPS/SSL makes it almost impossible for a hacker/cracker to successfully perform a so called “man-in-the-middle attack” - meaning that an unauthorized party can intercept and get possession of files being uploaded.

### Sending files using Filemail Desktop



Another method of sending files is by using Filemail Desktop - a small desktop application with more features than the web version.

This application does not at the current time (nov 2009) support HTTPS/SSL, but uses another approach to ensure the security and integrity of files being sent.

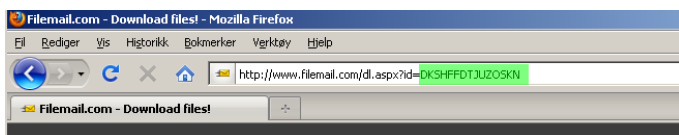
All files/folders that are being sent are broken down in small chunks; each chunk is compressed, a MD5 hash is taken of the chunk (think of this is a unique fingerprint) and finally the chunk is sent to the file server. The fileserver then receives the chunk, and checks the MD5 hash (fingerprint) in order to determine if the file chunk received is intact

and ok. If the fingerprint matches, the chunk is decompressed, and then it takes its place in the file - along with the other chunks sent.

Filemail Desktop will support HTTPS/SSL during the first quarter of 2010 - thus making it even more secure than it already is.

### Upload ID

Every upload that is made using Filemail.com receives an unique ID - which is later used by the recipient when he/she attempts to download files. This id can be observed on the download page - in the address field of the browser.

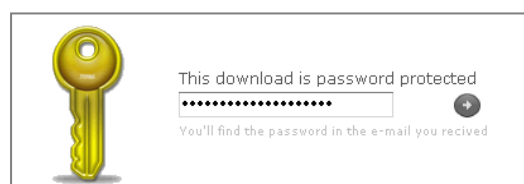


This ID consists of 15 characters - A to Z, and is made up from an algorithm using random numbers, and other input variables such as the ip address of the user - in order to guarantee that this ID is unique. This

algorithm allows for  $26^{15}$  (= 2954312706550833698643) combinations, which makes a brute force attack virtually impossible. If the website uses 1 second to respond whether an Upload ID is valid or not - it would take up to 93680641379719 years to perform a successful brute force attack.

### Password protection

Uploads can also be protected with an additional password in order to increase security even more.



## Security Mechanisms when downloading files – from the recipient’s perspective

When downloading files sent by a person with a premium or corporate account, the file(s) are transferred using HTTPS/SSL - the same encryption technology used when sending files with Filemail.com. This ensures the security and integrity of both the upload and the download.

## Physical server security and integrity

Our web servers are located in Norway in our main office. These servers are secured behind Linksys firewalls, and are continuously updated with regards to security patches etc. They are also physically secured, behind 4 access barriers.

Our file servers are, as mentioned earlier, located throughout the world. These file servers are also secured behind firewalls, and updated on the same basis as our main servers in Norway.

Partners and third parties that host our file servers have document their security principles and features before being approved and used by Filemail.com.

## Backup

A backup of the website and database of Filemail.com is done every night to a secure remote location 300 km (190 miles) away. This ensures that the account details, history and other information of our users are kept intact.

The file servers throughout the world (where the files are stored), does not have such a rigid backup mechanism in place.

The reason for this is twofold:

1. The huge amount of data that is stored on these servers would require a massive backup system. This would lead to increased costs for us - and our users.
2. Filemail.com is not a service meant to be used as a backup system for our end users. It is merely a service user to deliver content from A to B - while the master copy of this content is in the control and possession of the user.

However, it is important to note that Filemail.com has not ever experienced any loss of data at the time this paper is written. This is largely due to Filemail.com’s policy of only using top notch hosting providers, and first class hardware with redundancy!

## Handling of credit card information

Credit card payment is handled by our partner PayPal.com - which means that Filemail.com does not get/store any credit card information at all.

You can find more information about the security policies of PayPal.com here:

[https://www.paypal.com/cgi-bin/webscr?cmd=\\_security-center-outside](https://www.paypal.com/cgi-bin/webscr?cmd=_security-center-outside)

## Security References

The Norwegian Post and Telecommunications Authority (Post & Teletilsynet) is a corporate client of Filemail.com. NPT has found that Filemail.com fulfills all security requirements in order for NTP to use the service to send/receive sensitive information.