Secura

SECURA FILE EXCHANGE

Easily transfer any file securely to anyone

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 31 00
E info@secura.com
W secura.com

Follow us on

Secura File Exchange

Easily transfer any file securely to anyone

Secura delivers world-class security tools. Secura File Exchange is a sophisticated web platform developed for any organisation that has the need to easily make files available to external people in a secure way, without the hassle of installing any software or exchanging keys or passcodes.

Introduction

Sending or receiving large or sensitive files over the internet is a task many of us struggle with on a daily basis in our operations. Often, users resort to the tools that they know, such as e-mail, WeTransfer, Dropbox or OneDrive. In corporate environments, Managed File Transfer (MFT) solutions are often used. However, these tools are not all suitable for sensitive information or for communication with external users or customers. Many lack basic and advanced security features.

This is why Secura has developed a secure and easy way to transfer files between users on the internet, suitable for high-secure applications and when dealing with personal data that falls under the GDPR or other privacy regulations. In this article we analyse the problem, look at the weaknesses of existing solutions and present the case for Secura File Exchange (SFE).

The Problem

We are all accustomed to sending e-mail attachments. However e-mail is not a suitable medium for many types of data such as large files, personal data, sensitive financial information or company confidential information. There are several main reasons for this, the most obvious being that e-mail can only transfer files as attachments to a certain limit (usually around 12MB). Sending or requesting a PDF scan of a document from a customer or relation can already easily surpass this limit.

A further technical reason for e-mail not being a suitable is the fact that even in 2019, it is not guaranteed that an e-mail is sent securely over the internet with encrypted transport. While websites can easily be identified as using encrypted transport (the URL starts with HTTPS:// and therefore uses TLS security), this is not the case with e-mail. There is no way for a user to know or check how the e-mail is transported, and since regulations such as the GDPR and local regulations like the Dutch AVG require protection when sending personal information, you should not be using e-mail for *any* personal information. Does your HR department still send out salary statements or contracts by e-mail, or ask for copies of passports or other ID-cards by e-mail? If so, this is a violation of the regulations and could potentially lead to fines.

Exacerbating this problem, is the fact that any time you send an attachment by e-mail, you are effectively creating multiple (maybe five, six or more) copies of that attachment, all of which are no longer under your control (the sender), or the recipient, increasing the risk of leaking information. There will potentially be a copy of this data in:

- Your outbox
- The sending mail server
- The receiving mail server
- The E-discovery archive (if present)
- The inbox of the recipient
- All the backups of the above mentioned systems

And of course, you do not control most of these. All of them can be hacked. This effectively increases the risk of leaking information by an order of magnitude or more.

Furthermore, there is the ease with which mistakes can be made when addressing e-mails. A very large number of data leaks are caused by simple typos in e-mail addresses[1], made worse by e-mail clients that provide type-ahead functionality (e.g. start typing "John…' and the e-mail client will automatically fill that up to the most used e-mail address starting with "John". But it is up to the user to check if that is the intended address). The data protection authority in The Netherlands has analysed that up to 63% of all data leaks of personal information was caused by simply sending the data to the incorrect recipient , often caused by this autocomplete function in e-mail clients.

Add to all this the fact that e-mail is weakly authenticated (both for access controls to the mailboxes, as well as for the actual content of the e-mail) and it can be concluded that e-mail should be avoided. E-mail is simply no longer fit (if it ever was) for the professional communication of files between businesses and consumers, and between businesses and other business partners.

File Sharing Platforms

These limitations and risks have led to the growth of a large number of solutions for sharing (large) files, but most solutions are lacking in other ways and are focused on consumer-to-consumer type transfers and not on professional use. Users are keen to resort to solutions they know from personal use, because they are easy, such as WeTransfer or Google Drive. Alas, in the free and personal versions of these services, there are no confidentiality guarantees whatsoever, and in fact Google states in their use policy that Google is allowed to use any data shared through Google Drive:

> *When you upload, submit, store, send or receive content to or through Google Drive, you give Google a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our services), communicate, publish, publicly perform, publicly display and distribute such content.*

From: Google Drive Terms of Service, effective date: January 22, 2019

WeTransfer and many others do not offer authentication options beyond a simple password. None offer audit trails and logging capabilities. Further, since passwords are often weak, re-used and transported over insecure channels themselves, such file sharing platforms and cloud drives are also not fit for professional communication of files.

1. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2018

	E-mail	File Sharing platforms	MFT solutions	Secura File Exchange
Large files	✗	✓	✓	✓
Confidentiality	✗	✗	✓	✓
Control data storage	✗	✗	✓ / ✗	✓
Overall security posture	✗	✗	✗	✓
Ease of use	✓	✓	✓ / ✗	✓

Professional MFT solutions

There are quite a few solutions for the problems as described above. Managed File Transfer (MFT) products, such as Accellion, Axway and MOVEit neatly fill the most common requirements and sometimes offer advanced features such as integrity checks, Google Authenticator or even virtual keyboards to prevent keyloggers from seeing passwords being typed into the application. Other MFT environments are based on integration with existing environments such as TIBCO or Oracle, or are network share or folder based solutions for internal Windows domains.

However, most MFT solutions fail badly when it comes to overall security posture. Security starts with secure sign-up and enrolment. Therefore sending e-mails with plaintext login credentials (even if it is only once at the start of enrolment) completely breaks the security chain of multi-factor authentication. In addition, requiring a minimum password length of eight characters is insufficient for the present day where passwords hashes of eight and even nine or more characters can be brute-forced or cracked. Also, the MD5 hash algorithm used for integrity checks has been fully broken for over a decade, yet is still used in some major MFT platforms, where it is described as 'secure'.

Secura's MFT Solution

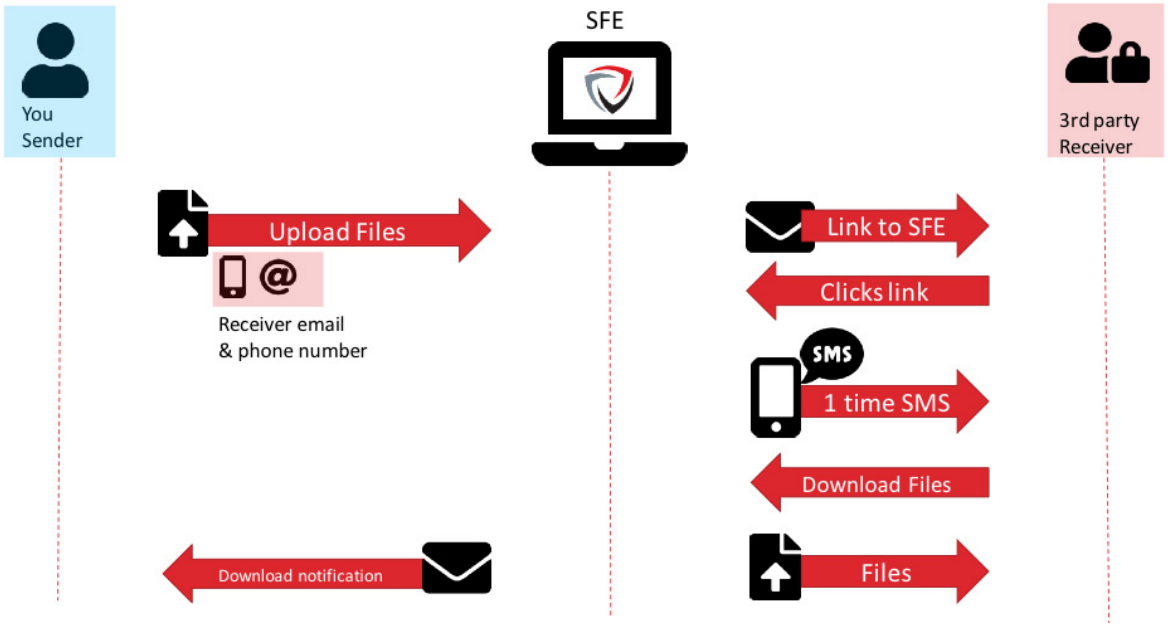
Secura performs several hundreds of application security tests every year. During these tests we get the opportunity to hack applications and systems, and give our customers advice on how to improve the security of the systems. It is therefore no surprise that Secura knows how to build a high quality, secure application. We know very well that all security measures are a trade-off with usability, and that compromises sometimes must be made to ensure that the security is not circumvented by users who feel burdened by these measures.

This is why we designed Secura File Exchange (SFE). SFE is the only MFT solution in the world built by a specialist security company, with security as the central pillar of development. We have built this product from scratch, and integrated many state-of-the-art security features including secure enrolment, secure hashing algorithms (SHA256), audit trails and many options for multi-factor authentication. SFE supports SMS text messages, Yubikeys and TOTP as second factors and will integrate many more in the very near future. But above all, we have made it very simple to use, both by recipients and senders of files, and admins. We also understand that there might be reasons that you need to keep the files in your own possession and not uploaded to someone else's cloud. This is why we offer our MFT solution in multiple deployment models: on premise and as a hosted dedicated service. A multi-tenant SaaS-solution will also be available in the future.

Ease of Use

How does it work? Let's go through a common use-case: an ad-hoc request to upload. Let's say you are a recruiter, busy on-boarding new candidates. As part of the process you must validate the identity of the candidate and you ask him or her to send a copy of their photo-ID. You open your web browser and surf to SFE. Here, you fill in your username and password. Since you have set up Google Authenticator as your second factor, you also type in the 6-digit code from the app on your mobile phone. After login, you click on 'Request file upload' and enter the candidate's e-mail address and mobile phone number. You add a little message asking for a copy of their ID, and click 'Send upload request'.

The candidate will receive an e-mail with a temporary link and the message you provided asking for the ID. When the recipient clicks on the link, they are immediately logged into the application, where they are asked for an SMS code. The SMS code arrives on the phone and after copying this into the browser, the candidate is logged in to the 'upload' page. They can upload their ID here, and this file is then checked for malware. If it is free of malware, a green symbol appears and if not, a red symbol appears. In both cases the requester of



the file receives a notification e-mail stating that a file has been uploaded. Using the same methods, the recipient can access the newly uploaded file.

Note that both requester and sender log in using multi-factor authentication and that files are scanned for malware, but the uploader never has to enrol on the system. The requester only needs to know the e-mail address and mobile phone number of the uploader.

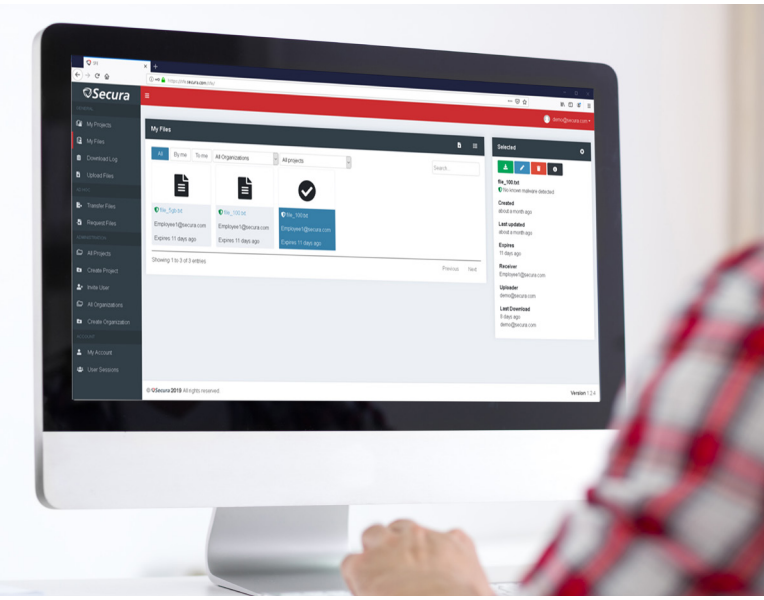
In a slightly different use-case, uploaded files can also be linked to projects so that project teams can easily access files. For this, the uploader must be enrolled in the system however, so that they are known as a part of a known external organisation (to which a project is coupled). The secure enrolment process allows users to choose which second factor they want to use: TOTP (such as Google or Microsoft Authenticator), a FIDO2/U2F token, a Yubikey, or a text message. Following enrolment, the external users can upload files in the context of project teams they belong to, or to download files put there by internal members of the project teams.

There are many more usability features, such as a modern, responsive user interface, enabling use on all types of devices including tablets and smartphones. Bulk upload of files can be grouped into one zip-file for easy download. And internal user authentication can be integrated into Windows domain authentication.

The auto-expiry feature makes sure that in the worst-case scenario (a compromise of the platform the application is hosted on) the exposure is limited to the most recent files, because all older files have been securely wiped (not simply 'deleted'). Obviously, all files are stored on an encrypted medium internally. Furthermore, there are extensive logging and audit trail options.

Finally, there is no limit on the number of users or the size of storage (save for the physical size of the underlying storage devices).

Secura offers support for SFE through our helpdesk during office hours (08:30 – 17:00 CET).



Features

- Highest grade TLS transport
- Windows domain authentication for internal users
- Works on all modern browsers, on all types of device
- Multi-factor sign-up and secure enrolment
- SMS as 2nd factor
- Google Authenticator and other TOTP's as 2nd factor
- Yubikey as 2nd factor
- FIDO2/U2F as 2nd factor
- Invite-to-upload function
- Ad hoc file exchange
- Managed customer file exchange
- Secure audit trail and logging
- Download as encrypted zip
- Malware scan of uploaded files
- Optional on-premise installation
- Secure SHA256 hash to ensure file authenticity
- Encrypted storage
- Configurable auto-expiration
- E-mail notifications
- Unlimited users
- Unlimited files (up to storage capacity of disks)
- *WhatsApp and Signal as 2nd factor (coming Q4 2019*

Benefits

- Easy and reliable secure exchange of files with anyone, without limitations
- Own your own data; control over where data is stored.
- No 3rd party access to your data
- No need for pre-registration, third party software or configuration; files can be quickly and securely transferred
- The best tradeoff between security and usability for exchanging files
- Easy to use two factor authentication.
- Full audit trail

About Secura

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

Secura has the mission to support organisations with up-to-date knowledge to work toward a bright and safe future.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

secura.com/subscribe

Secura