SMBsecure™ Addin for Microsoft® Outlook

Guidance Notes

SMBsecure™
Document Version 1.0

Password Considerations for PDF Email Encryption

When sending password-encrypted **Secure PDF** correspondence with a password Hint embedded in the body of the same email, it is important to use a password based on the context of who you are sending it to. We can categorise the context types as follows:

1. Business to Consumer correspondence to a single recipient. (**B2C**)
2. Business to Business correspondence to a single recipient or group-mailbox. (**B2B**)
3. Correspondence to Multiple Recipients on the same email thread. (**Multi-Recipient)**

Giving some thought to the password you use prior to sending the email with a password-encrypted **Secure PDF** + the *Hint* (which describes reference for that password) will make a crucial difference to the recipient's experience when receiving and accessing **Secure PDF** files.

Recommendations & Best Practice:

1. B2C to a Single Recipient

Use a password which is personal and known to the recipient i.e., something that they will know *off-hand*, or have, or can be referenced without much effort by them, but one that is not easily attained or attainable if the email is intercepted or by an unauthorised device user.

The password and the *Hint* which refers to it should not be included anywhere in your email signature nor in the body of the email which you are sending.

Examples include their ID/Password Number, their Date of Birth, their Account/Entity Number, etc.

2. B2B to a Single Recipient or a Group Mailbox

Use a password which is known to the recipient as well as to other members inside that business if the email is to be forwarded internally and the **Secure PDF** is required to be opened by multiple people (or by multiple groups of persons) for example when sending to Accounts, Operations, Order processing, Claims processing, etc.

The password should be something that the recipients will know *off-hand*, or have, and can be referenced without much effort by any of them, but one that is not easily attained or attainable if the email is intercepted or by an unauthorised device user.

The password and the *Hint* which refers to it should not be included anywhere in your email signature nor in the body of the email which you are sending.

Examples include their or your Account/Entity Number, a Practice or Registration Number, a contact number of someone in common, Customer/Client/Patient ID Number, or a "secret" that you have discussed and communicated with the recipient(s), etc.

3. Multiple Recipients on the Same Email Thread

Like B2B, the password used for the **Secure PDF** with multi-recipient emails should be a password known to ALL the recipients on the email thread(***To/CC/BCC***) requiring access to it.

Examples include their or your Account/Entity Number, a Practice or Registration Number, a contact number of someone in common, Customer/Client/Patient ID Number, or a "*secret*" that you have discussed and communicated with ALL the recipients included in the email, etc.

Using Simple Mode

A simple out-of-box experience for your recipients, easy enough for any sender to use!

The recommended default is **Simple Mode** and is ideal for sending attachment files as password-encrypted **Secure PDF**.

Simple Mode incorporates preconfigured default settings to individually convert attachment files to portable document format (**PDF**) and encrypts them with a password. Additionally, Simple Mode removes the need to deliver the password to a recipient. Instead, it always includes a ***password hint*** in the body of the email for the recipient(s) to reference. This aligns to what recipients are already familiar with when receiving encrypted correspondence from Banks, which usually includes a note in the email body of what info to use to open the password-encrypted PDF, for example, an ID Number. Not the most secure practice, but indeed very recipient-friendly!

Simple Mode requires minimal input by senders. The user needs only to specify the **password** and a **hint for that password.**

A password-hint is *a descriptive reference for the actual password to use to open the encrypted PDF and what the typed-in format should be – if any – for example: Your Date of Birth in the format DDMMYYY*

With just basic input there's a lot of reward for using Simple Mode which dramatically improves the out-of-box experience for any recipient receiving password-encrypted PDFs. Simple Mode strikes a balance between ***usability, productivity, and security*** whenever correspondence is being sent with encryption.

Remember you can always switch to **Custom Mode** to get full flexibility and granular settings options to enhance security, or to meet specific needs for your business and any user who requires it.

Templates

Templates can be accessed from inside the application Settings panel and can be customised and modified for how the password and/or hint is presented to the recipient in the emails.

Thank you for using the SMBsecure™ Email Encryption Software.

For any training, help or assistance please contact your Service Provider or IT Administrator.
For more information, please visit https://smbsecure.co.za