tabellae
all about documents

SECURING YOUR BUSINESS-CRITICAL ELECTRONIC DOCUMENTS

While the amount of electronic documents is growing, the threat of hacking is unfortunately increasing. Thousands of hacker attacks are officially registered every year and therefore, more than ever, there is a need to evaluate your company's overall IT security.

When it comes to the company's business-critical electronic documents, such as the invoice, Tabellae has compiled 3 measures that are relatively simple to implement.

1 FILE CERTIFICATES

Signing PDF files with an approved Adobe certificate. Signing can be done in bulk and for selected document types - e.g. invoices.

It will be possible to receive the signed documents in an Input Management system - such as Lasernet Input Management or similar. The largest supplier of certificates is GlobalSign, but there are also cheaper players on the market. Signing PDF files requires the "PDF Cloud Security" module from Formpipe.

2 FILE PASSWORDS

Encryption of PDF files with passwords. Can be done in bulk or for selected document types.

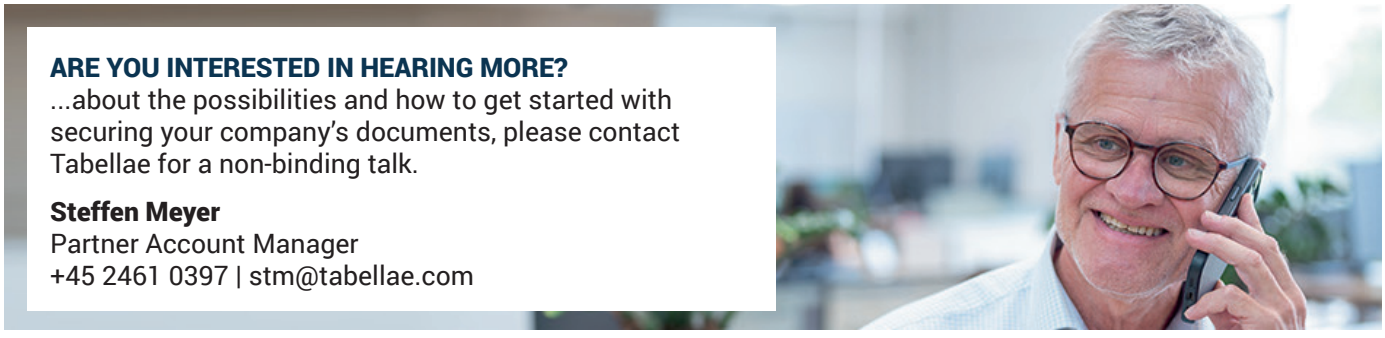
It is not possible to receive the files in an Input Management system, as passwords must be entered manually. Therefore most suitable for e.g. invoices of a certain type/size.

Password protection of PDF files requires the module "PDF Security" module from Formpipe.

3 MAIL CERTIFICATES

Bulk sign emails sent from Lasernet with an approved certificate. Protects both email and attached documents. It is possible to automate the process via Lasernet and sign selected documents and document types.

Requires a "Trusted Root Certificate" approved by Microsoft, as well as the Lasernet module "Mail Output" (the latter is included in the standard Lasernet license).



ARE YOU INTERESTED IN HEARING MORE?
...about the possibilities and how to get started with securing your company's documents, please contact Tabellae for a non-binding talk.

Steffen Meyer
Partner Account Manager
+45 2461 0397 | stm@tabellae.com

WORTH KNOWING ABOUT NIS2

In October 2024, the new EU directive NIS2 (Network & Information Security) will come into force. In many ways, it is a stricter directive compared to its predecessor NIS1 from 2018.There are now increased requirements for the company's risk analysis, measures and supervision, and top management, including the board of directors, can be held personally liable through penalties and sanctions. Primarily socially important and socially significant industries will be affected.