NINA

Personal, highly secure access to shared confidential documents

THANKS TO NINA YOU CAN SAFELY SAVE DOCUMENTS SUCH AS CONTRACTS, PATENTS AND SALARY STATEMENTS TO YOUR INTRANET, DOCUMENT MANAGEMENT SYSTEM OR OFFICE 365 WITHOUT FEAR THAT THE FILES COULD BE READ BY AN UNAUTHORIZED USER OR AN ADMINISTRATOR.

Description

NINA is a tool for encryption of documents stored in Microsoft SharePoint running both in the IT infrastructure of the customer, in cloud or in the Microsoft Office 365 storage. Thanks to the unique approach, NINA extends the features of the standard document storage with a secure storage solution for sensitive and confidential documents. It is designed to eliminate not only access of unauthorized users/staff, but also, for example, of your system administrator.

How it all works

A personal certificate with a password (set by a user) is generated for each user of NINA. The user's certificate is an essential element to encryption/decryption of the selected document. When encrypting the document, the user can select who shall be able to decrypt the document.

To decrypt the document, NINA requires a two-factor user identification. That is, on the one hand a classic username and password from Sharepoint (1st factor) and then the PIN for the personal certificate (2nd factor). Only the successful identification shall ensure that the document will be decrypted.

Such a mechanism, therefore, ensures that NOBODY can gain access to the documents unless they are identified by the two-factor system. Even the administrator who has an access to the database cannot do so.

Target Group

NINA is beneficial for all organizations which want a unified and safe storage for all electronic documents regardless of their sensitivity, nature or location.

Specific features

- The so-called Crown jewels - enable you to decrypt documents using a predefined number of accounts for example of Managing Director, Financial Director or Production Director in cases where the user who encrypted the documents is no longer employed in the organization.

- The audit log - logs activities associated with encrypting and decrypting documents in detail.

- Policies - for the definition of the parameters for the personal certificate PIN

- Optional encryption key size is 64 - 256 bit

System components

- **NINA encryption server** - custom core providing encryption and decryption. It is designed as multi-tenant technology which requires Windows and SQL server for operation. It can run both in cloud (AC Cloud / Microsoft Azure) and on the customer's server.

- **NINA application** - can run in Microsoft Office 365, Microsoft Sharepoint running in a customer's environment, or in cloud.

- **NINA application services** - advanced interface for programmatic transfer of documents to the encryption e.g. from a human resources system