MARGARETAUSER
CERTIFICATE MANAGEMENT

MARGARETADEVICE
CERTIFICATE MANAGEMENT

The new dimension in certificate lifecycle management

MARGARETA Device Certificate Management

The MARGARETA Device Certificate Management module is an add-on for the MARGARETA system. Its task is the lifecycle management of the device certificates

The base functionality of MARGARETA Device Certificate Management is the management of Windows device certificates, which were issued through an auto-enrolment procedure. The auto-enrolment procedure does not cover the full lifecycle of the certificates which can cause serious security problems (for example: there is no automatic mechanism for clearing the associated certificates when a Windows machine is removed from the network, etc.). MARGARETA Device Certificate Management can solve these issues in such a way that it follows the life of the issued certificates and the status of the related AD user. In this way, it can detect changes in the state of the certificates and be able to respond to these changes in the necessary way (clears it, suspends it, etc).

This base system can be later extended to handle other device certificates, by simply adding additional device connectors tailored for the requirements of the individual devices.
A working MARGARETA CORE system is a base requirement to install the MARGARETA Device Certificate Management module.

Contact Us

+36 1 4386380 www.noreg.hu

NOREG

Certificate Management for Mobile Devices

MARGARETA Mobile App (MMA) is a streamlined mobile application designed for both Android and iOS platforms. The application remains dormant until activated by the user and does not run any background services.

Upon its launch, MMA carries out a Multi-Factor Authentication (MFA) process against the customer's publicly accessible MFA server, ensuring a robust layer of security. Once the user has successfully authenticated with the MARGARETA Portal server, the application proceeds to download the two most recent encryption certificates from MARGARETA. If the encryption certificate is not present on the mobile device, MMA prompts a system dialog to import the certificate into the Android or iOS system store, ensuring a seamless and secure user experience.

The imported certificates then can be used by various mobile email applications, so the end users can read their encrypted emails on the go. Furthermore, if signature profiles are configured, users can also sign emails on their mobile devices.

CA Certificate Management extension for MARGARETA

CA Certificate Management extension module connects to the MARGARETA system, as a part of the MARGARETA Device Certificate Management system, but it can be used without the implementation of the Device Certificate Management add-on.

The CA Certificate Management extension ensures that desktop users do not have access to servers certified by not approved CA certificates, avoiding high security risks.

Features

- handles the approved CA's list
- handles the exceptions to handle special CA certificates, which are needed for individual users for their special tasks
- gives a UI to store, approve, and clear CA certificates for the module's authorized users
- defines the necessary AD Groups
- generates the CSV file for the MARGARETA system