

# MARGARETA FOR COMPREHENSIVE MANAGEMENT OF CERTIFICATES

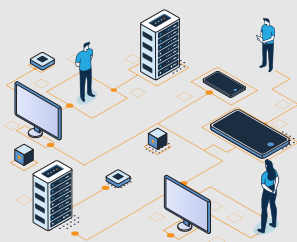
## Growing demand for authentication of users and devices

Businesses are using a growing number of digital certificates in their IT environments: according to Ponemon Institute's 2022 international study, **66%** of the surveyed IT experts answered that they are deploying more keys and digital certificates across their IT landscape from year to year.

Encrypted communication and authentication between users and devices rely on a multitude of cryptographic keys and digital certificates. Providing the necessary trust, however, entails ever more complex challenges for professionals. An efficient solution is needed for the lifecycle management of keys and certificates.

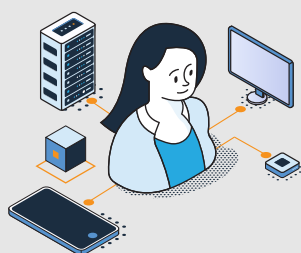


## What are possible consequences of improper lifecycle management of certificates?



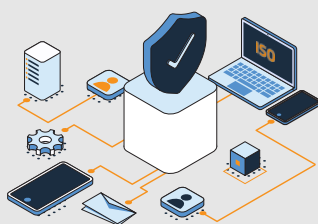
### GENERAL CHALLENGES

- Certificates can be obtained through different processes, even from multiple vendors.
- Certificates in use and their properties are difficult to track.
- Missing information makes incident troubleshooting and efficient resolution difficult.
- Managing certificates and keys requires trained resources at all times.



### EMPLOYEE CHALLENGES

- Encrypted correspondence of a former employee cannot be accessed by management.
- Certificates of a former employee remain valid.
- Unexpected computer failure denies access to encrypted files.
- Leaving a key storage device at home denies an employee the ability to work for the day.
- Issuance of certificates and restoration of encryption keys is done by a single person.

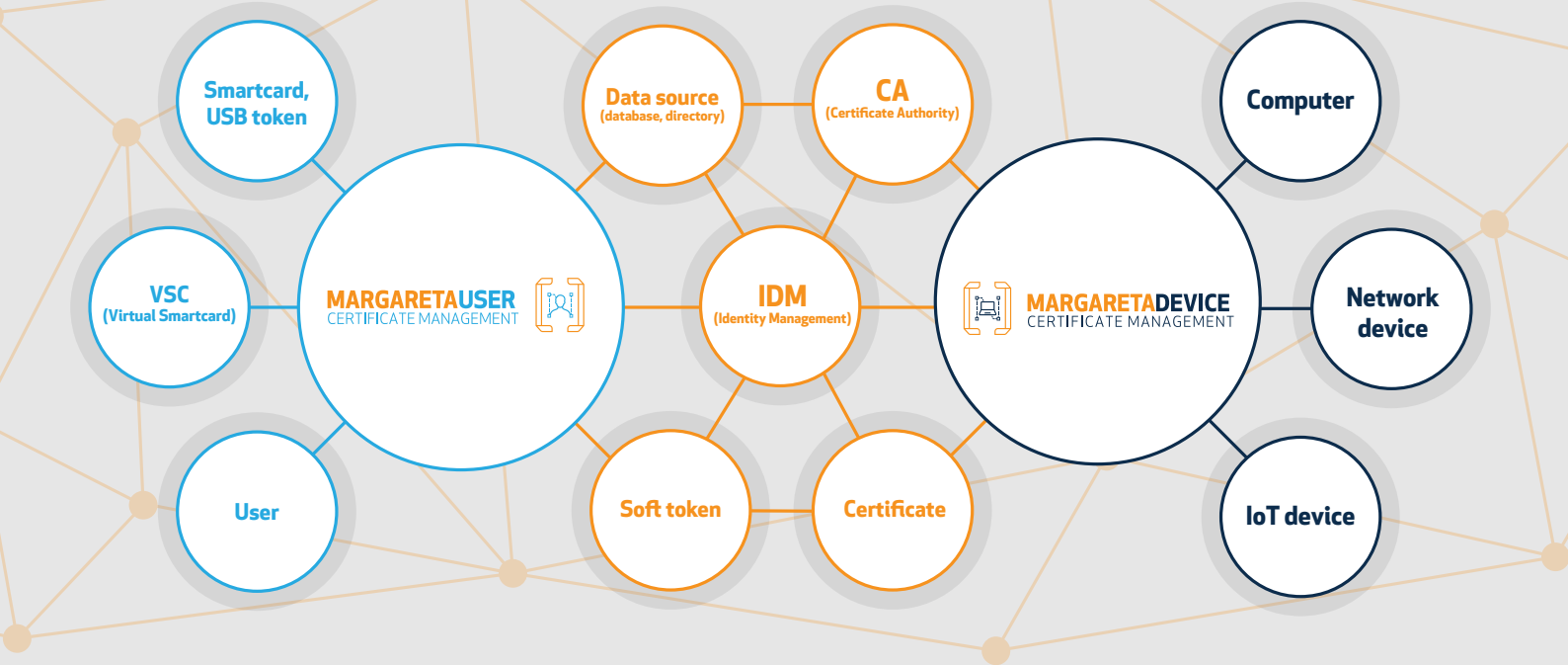


### DEVICE CHALLENGES

- Expired certificates cause operation and service downtimes resulting in damage to reputation and direct financial loss.
- Loading certificates to devices is cumbersome.
- Assigning certificates to operators is problematic.



**MARGARETA PROVIDES A SOLUTION TO ALL MENTIONED CHALLENGES!**

## MODULES OF MARGARETA

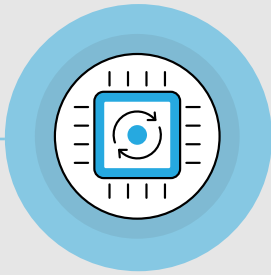


MARGARETA is a unified solution for the full lifecycle management of certificates and key storage devices. It provides a high degree of automation for all certificate management tasks.

MARGARETA connects all systems and devices related to PKI processes with a general-purpose card and certificate management system.

MODUL	MARGARETAUSER CERTIFICATE MANAGEMENT	MARGARETADevice CERTIFICATE MANAGEMENT
 BENEFIT	Visibility, central inventory, and management of all user certificates, regardless of origin	Provides automation for the issuance, revocation, and renewal of certificates for thousands of IoT and other devices. This eliminates the problem of using default or identical certificates on the long run.
 RECOMMENDED FOR?	Ideal for businesses with many users, already having certificates and wishing to increase the security of business processes.	Companies with business and IoT processes utilizing many devices and equipment requiring a secure connection.

## MARGARETA VALUE PROPOSITION

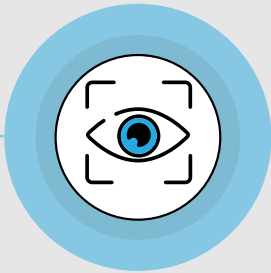


### AUTOMATION

Built-in automation minimizes the need for human resources, reduces operational costs, support needs and room for error.

### EFFICIENCY

Different certificates can be stored in a single key storage device, which can be virtual or physical card, token or even the operating system's key storage. Devices left at home can be substituted easily: a temporary card can be issued in a minute.

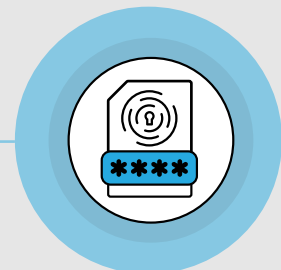


### VISIBILITY

A synchronized inventory of internal and external certificates provides visibility on the certificates users and devices have together with their origins. Reports enable analysis and statistics.

### KEY MANAGEMENT

Encryption keys and certificates can be securely archived and restored on need. Remote and operator renewal are available.

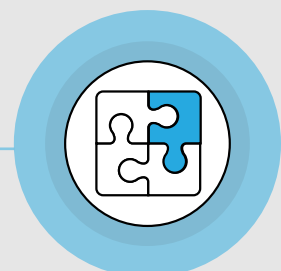


### SECURITY

Key and sensitive data are protected by a cryptographic module. Additionally, an agent-based implementation enables the separation of the critical elements of the PKI environment from zones with user access. Supports access based on the four eyes principle.

### INTEGRATION

Built-in and custom integration modules are supported, enabling integration to any environment beyond common standard solutions. Custom solutions include enterprise directories, custom IDM interfaces or certificates from external authorities.





**AN EXPERT** in information security technologies and services



**20+** years of PKI and **10+** years of certificate management  
**EXPERIENCE**



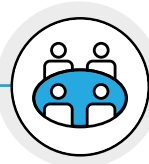
**IN-HOUSE PKI SOLUTIONS** and digital signature products



participation in the implementation and **CONTINUOUS SUPPORT** of trust service providers and corporate PKI systems



**ACTIVE MEMBER** of information security and international PKI professional communities



**CLIENTS** that include leading financial, telecommunications, industrial and trading companies, and public administration.



1118 Budapest, Rétköz u. 5.



+361 438 6380



LinkedIn

