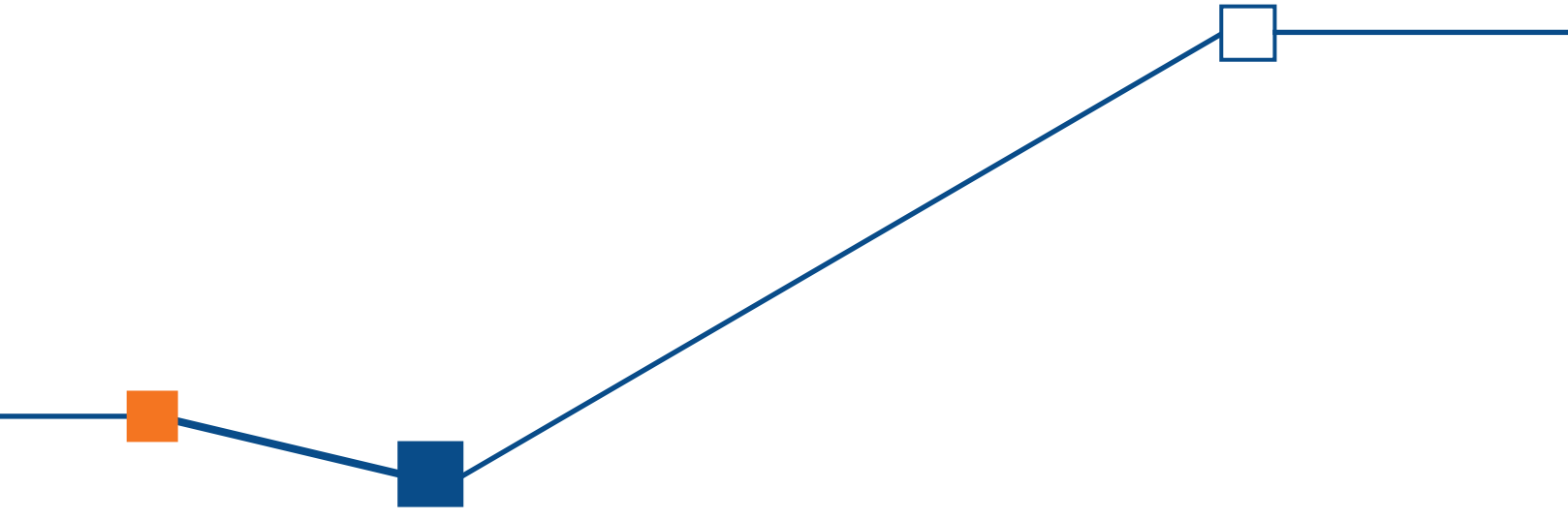
Digital Certificates



SECARDEO

Distributing Certificates and Keys

SECARDEO GmbH

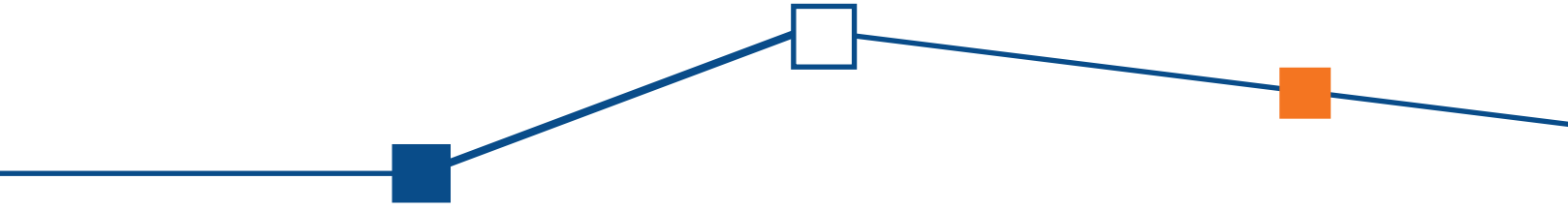
SECARDEO GmbH is a provider of corporate solutions using digital certificates. Since 2001 SECARDEO offers competent consulting, innovative products and integrated solutions. Our customers are global players and medium to large enterprises.

Public Key Infrastructures

A Public Key Infrastructure (PKI) provides mechanisms for using asymmetric cryptosystems and digital certificates. This allows for an encryption of data, strong authentication and the use of digital signatures. PKI provides the basis for a high security level.

PKI - Inhouse or Managed

A PKI can be used internally or outsourced as a Managed PKI Solution. In many instances a Microsoft Certification Authority (CA) is available, which supplies Windows clients with certificates without extra costs. SECARDEO posesses an expertise, proficiency and a long list of successfully executed consulting and implementation projects.



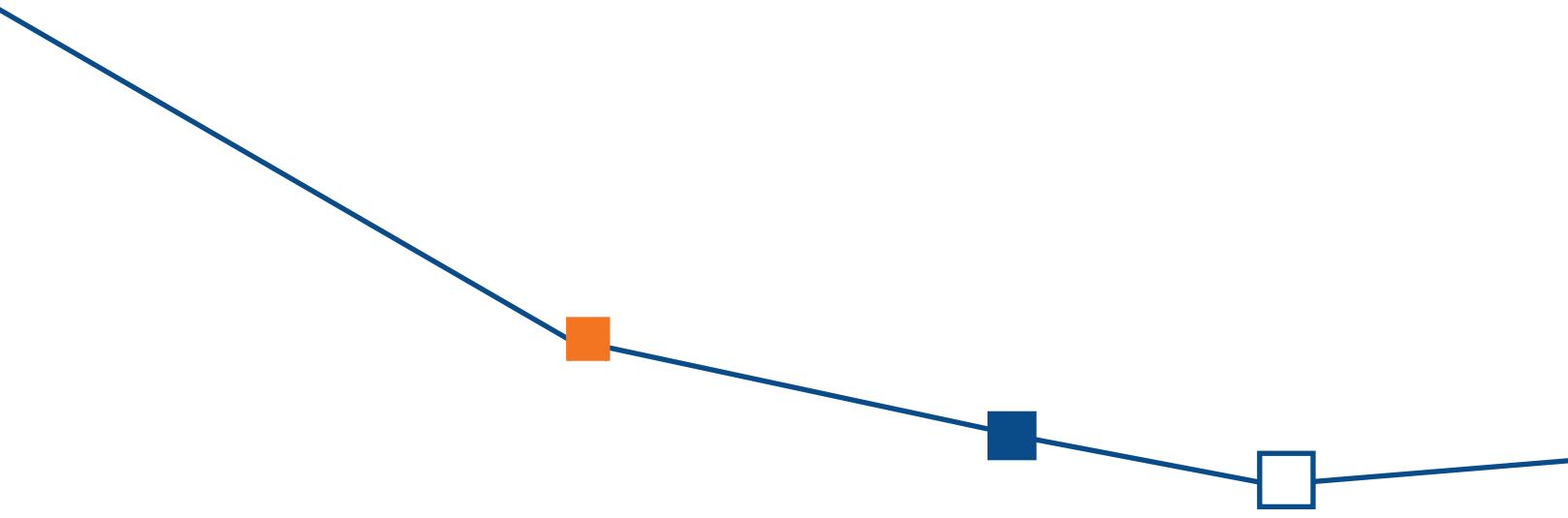
„All users, devices and computer services in the world will communicate securely with each other in a completely transparent way by using digital certificates.“

“SECARDEO distributes the necessary keys and certificates - securely, automatic und trustworthy.”

Dr. Gunnar Jacobson, CEO

Distribution of Keys and Certificates

The distribution of certificates and private keys to all devices in the company in a secure and trustworthy manner is one of the main tasks of a PKI. With the TOPKI (Trusted Open PKI) platform SECARDEO offers a fully-automatic, reliable solution for Windows, network- and mobile devices. This enables the use of common CA products or public CA services for autoenrollment. Moreover, transparent encryption with external partners will be possible. The costs for the PKI operation will be drastically reduced with TOPKI and IT security greatly maximized.



„Properly implemented strong crypto systems are one of the few things that you can rely on.“

Edward Snowden, Whistleblower

End-to-End Encryption

For a continuous "end-to-end encryption" the private key of a user has to be installed on every user's device. Also his partner's certificates must be provided there and his own certificate has to be provided to them. For external e-mail encryption globally accepted certificates should be used from a public CA.

The connection with the CAs and the distribution of all certificates and private keys will be processed automatically by TOPKI without client software having to be installed. A user may then encrypt, decrypt and sign his e-mails on Windows using Outlook or with the mail app on his managed or unmanaged mobile devices.

SECARDEO has performed a lot of consulting and implementation projects and addresses customers in the upper midsize market, financial institutions and public authorities as well as international groups.

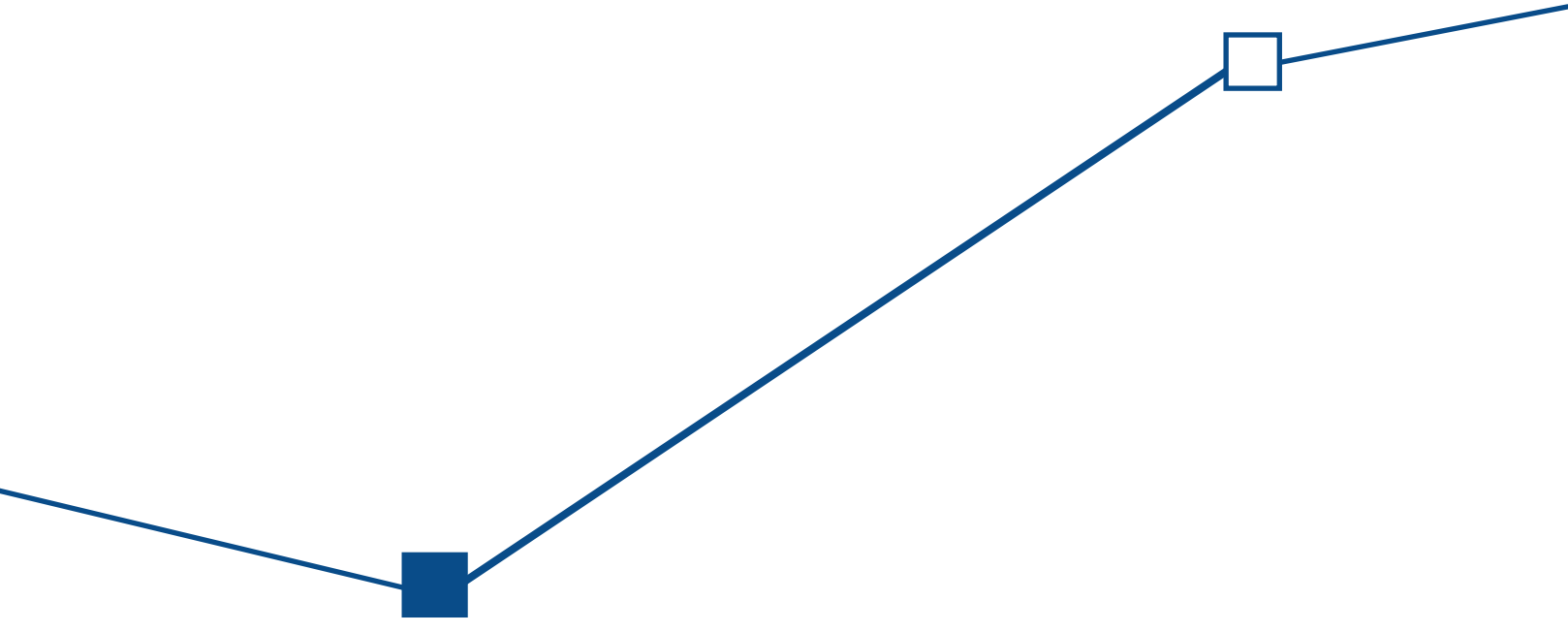
Device Authentication and Secure Communication

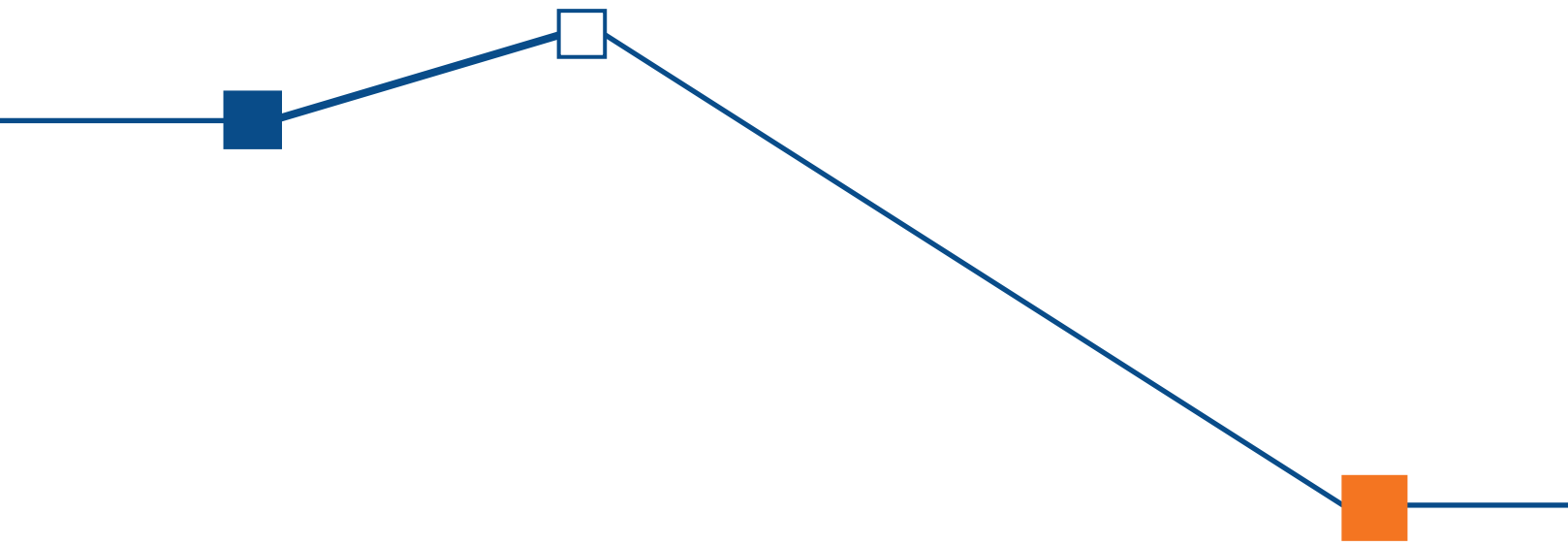
For authorizing devices for network access, authentication of domain controllers or using secure communication protocols, all devices have to be equipped with digital certificates. TOPKI allows for using protected Open Source CAs or CA software-as-a-service in the cloud.

Consulting

With digital certificates you can improve IT security in your enterprise. There are many solution alternatives, be it an inhouse solution based on a Windows PKI or a managed PKI with certificates from an accepted CA. We support you with competent consultancy by experienced experts for:

- PKI conception
- PKI analysis
- Project support
- PKI seminars
- Inhouse workshops





SECARDEO

Secardeo GmbH
Hohenadlstrasse 4
D-85737 Ismaning
Germany

Tel. +49 (0) 89-1893589-0
Fax +49 (0) 89-1893589-9

E-Mail: info@secardeo.com
www.secardeo.com