Workplace PKI

With Nexus' solution Smart ID Workplace, you can automate enterprise certificate provisioning for IT systems and devices: personal computers, mobile devices, servers, web applications, services, network devices, network printers, conference systems etc. It supports enterprise IT to manage and automate the entire life cycle of their internal and external PKI-based certificates.

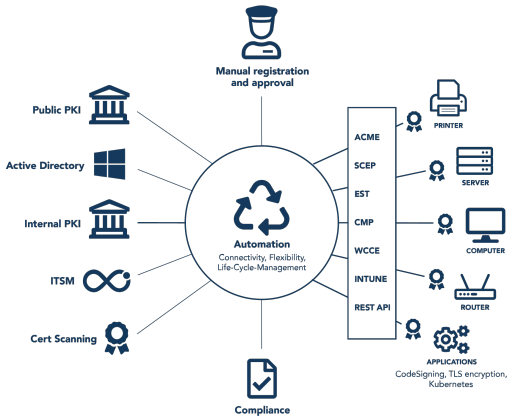
Do you want to know more?

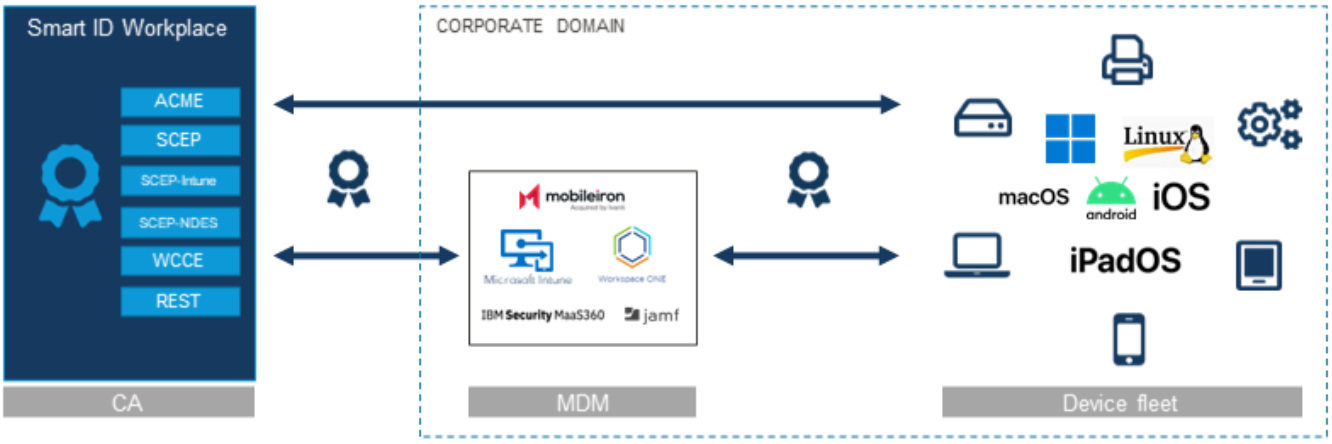
Contact us

The certificates are used for controlling access to the corporate network, and to corporate applications either in the corporate network or in the cloud, as well as for encrypted and authenticated communication among those devices and services.

The certificates are held by:

- Operating systems on the desktop devices, such as Windows, Linux and macOS
- Operating systems on the mobile devices, such as Android and iOS
- Operating systems on servers: Windows, Linux
- Container of servers or services: Docker
- Web servers, applications and services, which need TLS server certificates
- Network components (hardware and software), WLAN access points
- Other network-connected devices, such as printers and conference systems





Use cases

Secure communication among IT systems and devices

Authentication of the communicating client and server components, as well as session authentication, sessi on integrity protection and session encryption. These security mechanisms are typically implemented in a corporate network by means of the standard protocols TLS and IPSec. As part of these, session encryption keys are deduced by an embedded key agreement protocol from the authentication PKI keys of the communication parties. Also, session authentication and integrity protection are provided by built-in mechani sms of the protocols and need no additional cryptographic keys. At the end, the communicating parties need only an authentication key pair and respective certificates.

Digital signing of software

Many corporations develop their own software, such as mobile apps or server applications for various platfor ms. Digitally signing the software enables the executing platform to verify the origin and the integrity of the software. A code signing service enables a development platform to let digitally sign software, which origins from a secure development process.

Certificate management aligned with the life cycle of IT systems and devices

IT systems and devices ('assets') are usually managed in an identity or asset management system, such as Active Directory, Azure Active Directory, in an MDM system or in a process-oriented IT Service Management (ITSM) management system (for example, ServiceNow). With Smart ID Workforce, certificates are provisioned when the device is commissioned and revoked when the device is decommissio ned. Certificates are updated (renewed) automatically as long as the certificate-holder asset is active. Changes in the identity data of an asset leads to replacing the certificate on the asset.

Automated certificate management

The certificates can be provisioned directly to the target asset in an automated process via the API of the W orkplace PKI, such as in the WCCE (Windows Client Certificate Enrollment), SCEP, or ACME protocols. MD M systems (Intune, MobileIron, etc.) “mediate” in the certificate provisioning process, that is, they request the certificate from the PKI on behalf of the asset and provision it to the asset using the asset’s general purpose management mechanism. A virtual hosting and orchestration environment (hypervisor, Kubernetes) and a DevOps environment can create and destroy virtual resource instances in an automated and dynamic way. Especially in such an environment, only automated management of the certificates is fea sible. The respective platform typically acts in a similar way as intermediary between the asset and the PKI.

Asset management

Nexus Smart ID Workplace solution provides an advanced asset management system, enabling control of the complete IT equipment device fleet. It offers a web GUI, providing an inventory of all devices and ready-made workflows for manual asset registration and management with associated owner notifications and approvals.

Integration with public CAs

Web servers accessed via the browser need a server certificate from a publicly trusted Certificate Authority (CA). Smart ID Workplace can connect to such a trusted CA and enable the seamless management (that is, issuing) of the web server certificate via Smart ID Identity Manager. Currently, the following publicly trusted CAs are supported:

- D-Trust, part of Bundesdruckerei, Germany
- QuoVadis, Switzerland; part of Digicert, U.S.

Nexus' solution

Nexus' Smart ID Workplace solution is based on Smart ID Identity Manager and Smart ID Certificate Manager.

For more information, see the following links:

- Identity Manager overview
- Identity Manager requirements and interoperability
- Certificate Manager overview
- Certificate Manager requirements and interoperability