Nexus Smart ID

The Nexus Smart ID solution provides easy-to-use modules for managing physical and digital access, physical access entitlement, two-factor authentication and single sign-on to digital resources, as well as certificates for enterprise use and for IoT devices.

Smart ID modules

For a quick overview of the modules and included functionality, see here:

- Read the list of features: Smart ID module overview

- Watch the video: Nexus Smart ID in 5 minutes

Here are all the modules in Nexus Smart ID:

- **Physical ID**: Visual ID and RFID card management, including basic PACS integration.
- **Digital ID**: PKI token management, including Mobile ID and Physical ID.
- **Physical access**: Physical access entitlement including Physical ID and full entitlement PACS integration.
- **Digital access**: Two-factor authentication (2FA), single sign-on (SSO), and federation.
- **Digital signing**: Remote signing services for PDF documents and XML data.
- **Corporate PKI**: Certificate management for enterprise use, to be used stand-alone or as an add-on to Digital ID to replace Microsoft ADCS or any other CA or PKI platform.
- **IoT PKI**: Trusted identities by issuing certificates to devices, in internet of things (IoT) applications.

Additional services and hardware can be added to the Smart ID modules for a complete solution. For more information, see Smart ID add-ons.

Benefits of Smart ID

Smooth and secure solution

The Smart ID solution provides easier management of your organization's security solutions in Nexus systems that are integrated with existing infrastructure such as active directory (AD) and physical access control systems (PACS).

With its standard use cases and easy system setup, the solution suits all small and medium organizations, municipalities, etc, that want to ensure security, traceability, compliance to local and global regulations, and minimal administrative work to manage identities, cards, certificates, and access to digital resources. In the Smart ID solution, Nexus has implemented best-practice use cases, based on previous world-wide experiences.

Cover most common use cases

The Smart ID solution includes most common use cases, with automated workflows for example for lost cards, temporary cards, new mobile devices, and change of PIN. These workflows include approval steps and email notifications to ensure that the identities and cards are managed in a secure way throughout the lifecycle.

Integrate in existing infrastructure

The Smart ID solution integrates to your existing infrastructure. Identities are managed by synchronization with your existing Active Directory or Human Resources system. The solution also

Video

To watch the video in full screen mode, start the video and then click the Youtube link.

Related information

- Smart ID module overview

connects to your existing physical access control system (PACS) and certificate authority (CA).