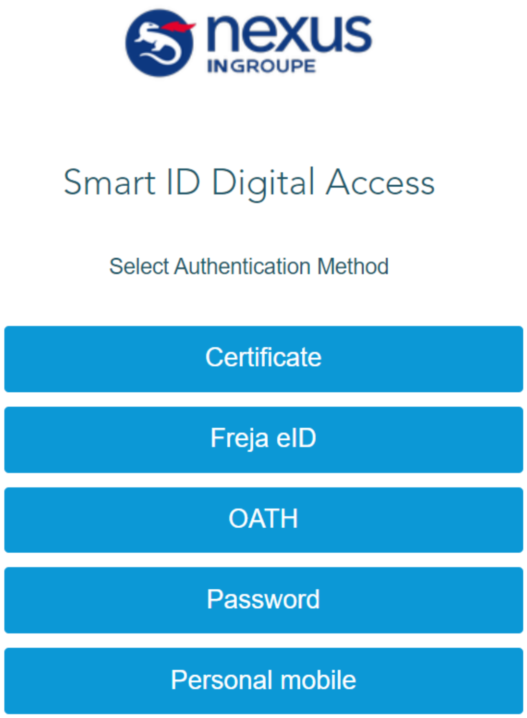
Digital Access component overview



The **Smart ID Digital Access component** helps to enable the right users - employees, customers or citizens - get secure access to the right digital resources, no matter where users or resources are located. Digital Access helps prevent unauthorized access and go passwordless by supporting many user-friendly two-factor authentication (2FA) methods and provides single sign-on and identity federation, enabling users to log on just once to reach all managed resources.

Protect your digital resources with strong authentication

Multifactor authentication, meaning a user must present two or more separate pieces of evidence to prove their identity, is recommended for high security. And high security does not mean inconvenience for the user, rather the other way around - smooth usage is critical.

Smart ID Digital Access supports a wide range of smooth and secure multifactor Authentication methods in Digital Access. Complete functionality is included to issue own identities, using the Nexus Smart ID apps for virtual smart cards on desktop or mobile, or you can choose to use existing third-party identities, such as public eIDs, corporate identities from an Active Directory via LDAP, one-time passwords (OTP) via SMS, smartcards, hardware tokens or email. In total, around 30 different methods are supported by Smart ID Digital Access, allowing you to choose the right ones for your use cases and needs.

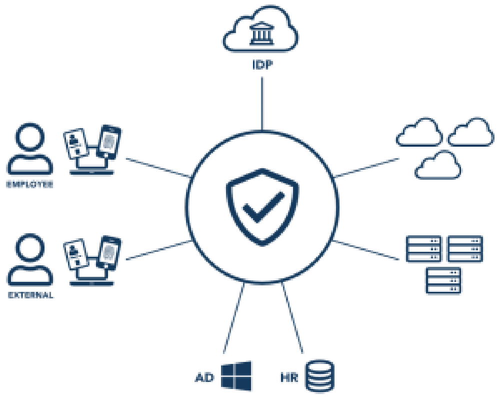
Manage access to local and cloud resources

Smart ID Digital Access helps you to manage secure access to all kinds of digital resources, that are installed on-premises or available in the cloud. Authentication of online services is supported as well as acess to re mote workforce networks.

Existing online services can easily plug in the solution to start using strong authentication methods to securely identify online users, by use of SAML, OpenID Connect or API.

Digital Access component is clientless and compatible with a variety of user clients. An access portal is provided where the user can find all available resources. For non-web applications, an access client is available to create secure tunnels between user devices and client-server applications.

Identity orchestration is supported, that is, a user account can be created dynamically when a user accesses a web resource.



Ensure smooth administration by setting up access rules

To ensure compliance with rules and regulations and minimize manual administration, authorization of users can be based on Access rules in Digital Access. Access rules is a way to formalize and enforce the company policies, by specifying detailed requirements for users to access resources and single sign-on domains, based on for example:

- authentication method
- group membership
- client device
- geographical location and network
- date and time

Allow for single sign-on or identity federation

Smart ID Digital Access helps end users to simply access all their local or remote resources with just one login, by using single sign-on and identity federation.

Single sign-on in Digital Access (SSO) permits users to enter their credentials once, which then gives them access to several resources without the need to re-authenticate later on. Smart ID Digital Access supports several SSO mechanisms, including web-based applications, cloud applications or through an access client.

Identity federation is an agreement that can be made between multiple service providers to let users get access to all services with the same identification data. Smart ID Digital Access supports federation technologies such as SAML 2.0, OpenID Connect federation in Digital Access component and OAuth 2.0. Digital Access can act as an identity provider or connect to other identity providers, depending on the use case.

Make administration easy with self-service

Any administration or configuration changes for example of users, resources, authentication methods and access rules in Digital Access, is done via the web-based administration interface.

Users can also use the built-in self-service portal to change or reset passwords or provision their own mobile identities with the Smart ID Mobile App. In combination with the Smart ID Digital ID solution, more self-service functionality is provided.

Combine with other Smart ID solutions

Nexus' Digital access is a set of processes for how to grant and manage secure access to different users into the right digital resources. It can be combined with other Smart ID Workforce modules for a complete security solution, including acting as an identity provider against Nexus' services or external services.

More information

- Hardening of Digital Access component appliance
- Digital Access interfaces
- Digital Access component architecture overview

- Supports identity federation via the protocols SAML, OpenID Connect and OAuth2
- Supports OATH one-time passwords
- Supports RADIUS clients and servers

- Connects with public eIDs, such as Swedish BankID, Freja eID and Norwegian BankID
- Offers a webservice API for authentication and user management, as well as for configuration

For more information, see Digital Access component requirements and interoperability.