SOLUTION BRIEF

Passwordless secure access

Secure. Seamless. Scalable.





1.
Flexible authentication for diverse needs

Nexus Smart ID enables secure, certificate-based multi-factor authentication (MFA) to protect access to applications, data, and digital services

In addition to standard credential-based authentication, Smart ID supports a wide range of authentication methods to meet the versatile needs for secure access, from employees and partners to customers and citizens.

MOBILE APP

Mobile-based certificate authentication, secured with biometric or PIN.

OATH-BASED OTP

One-time passwords generated via mobile apps or hardware tokens.

FIDO2

Hardware-backed, passwordless authentication with phishing-resistant security keys.

VIRTUAL SMART CARDS (VSCS)

Certificate-based authentication through advanced middleware.

SMART CARDS

Certificate-based authentication through advanced middleware.

INVISIBLE TOKEN

Browser-based OTP authentication that works without extra hardware or mobile apps.

MOBILE TEXT

One-time password delivery via SMS for strong yet simple mobile authentication.

FEDERATED AUTHENTICATION

Integrate with external identity providers using SAML 2.0, OpenID Connect, or OAuth 2.

THIRD-PARTY EIDS

Support for BankID SE, Freja eID, and other national or commercial digital identity services.

Reduce risk, meet compliance goals, and deliver a seamless user experience, whether users are onsite or remote.

2.
Designed for interoperability

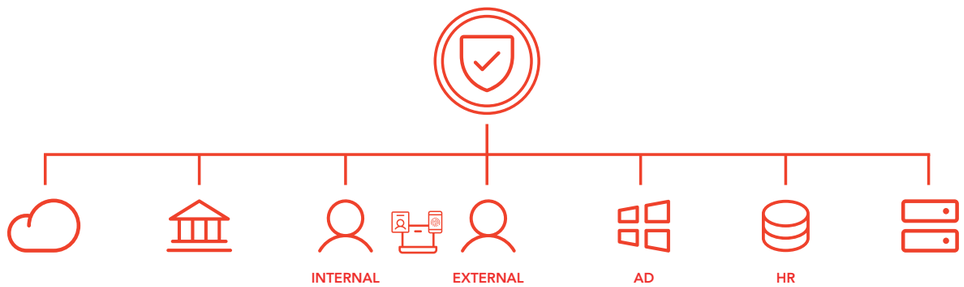
Connect effortlessly with your business-critical platforms, applications, and infrastructure

3.
Enable trust with Smart ID

Smart ID protects your organization from unauthorized access, phishing, and credential theft, while making it easier for users to access the tools they need securely

Smart ID protects your organization from unauthorized access, phishing, and credential theft, while making it easier for users to access the tools they need securely.

- **Versatile authentication options:** Support for smart cards, mobile devices, FIDO2 keys, and biometrics.
- **Seamless user access:** Enable single sign-on (SSO) to minimize login friction across cloud and on-prem apps.
- **Policy-driven access control:** Define authentication requirements based on user roles, devices, and context.
- **User self-service portal:** Empower users to manage credentials, reset PINs, and enroll new methods.
- **Federation and identity brokering:** Integrate external identity providers using standard protocols (SAML, OIDC, OAuth2).
- **Audit and logging capabilities:** Monitor authentication events for better oversight and compliance readiness.
- **Simplified administration:** A web-based interface enables centralized configuration and easy day-to-day management.
- **Flexible deployment options:** Choose cloud-based or on-premises installation, or run in hybrid environments.
- **Scalable and future-ready:** Designed to support growing organizations and evolving access needs.



Thank you

All rights reserved. Specifications and information subject to change without notice. The products described in this document are subject to continuous development and improvement. All trademarks and service marks referred to herein, whether registered or not in specific countries, are the property of their respective owners.

ingroupe.com

IN GROUPE