SOLUTION BRIEF

How to make use of your workforce identities

nexusgroup.com

nexus INGROUPE

Use trusted employee identities for many purposes

Username and password are not secure enough to meet today's requirements for secure login. Instead, trusted employee identities can be issued in the form of corporate ID cards or virtual smartcards on phones and laptops.

Select the identities that suit your organization best, considering your needed use cases and level of security.

With trusted employee IDs, you can log on to Windows, sign documents digitally, sign and encrypt emails, identify visually, access buildings, and log in once with multifactor authentication to all digital resources. This means that the organization and employees don't have to deal with multiple passwords, cards or tokens.

Manage your trusted identities with Smart ID

With Nexus Smart ID for the workforce, trusted identities for employees, contractors and visitors are managed in one central system, which can easily be integrated into existing corporate directories and other systems. This enables smooth and secure on- and offboarding of employees and contractors and makes it easy to trace actions and audit the solution.

Ensure compliance to regulations
Using one central management system for identities helps to control compliance to regulations. Reporting functions and object history enable monitoring and auditing. With standard processes and automation, policies are automatically enforced.

Simplify on- and offboarding
On- and offboarding and lifecycle management are made easy with standard processes for common use cases. Automation and self-service tasks help simplify administration.

Integrate with standard systems
Integration with standard systems such as Active Directory (AD), HR systems, IT service management (ITSM) systems and physical access control systems (PACS) ensure alignment of identities across systems.

Deploy as it suits you
Flexible deployment options enable adapting to your security needs and use cases. Decide if you want to deploy your identity management solution in the cloud, on-premises or with a hybrid solution.

Improve usability
Let your users log in once to many resources with single sign-on instead of having to remember many complex passwords for different services. Select the identity carriers that suit your users' needs, for example mobile virtual smart cards if all employees have smart phones. Self-service tasks help users stay in control.

Log on to Windows with multifactor authentication

Using passwords for Windows logon is both a security and a usability issue. Users might have passwords that are far too easy to guess, or they must remember long and complex passwords that need to be changed a few times annually.

Using multifactor authentication (MFA) increases both security and usability. Instead of relying on a password as the single factor, the security relies on at least two factors. And users do not need to remember a long and complex password but can easily authenticate with biometrics or a PIN as one factor. MFA options include virtual smart cards that are stored on the trusted platform module (TPM) on the laptop, physical smart cards with a card reader, or mobile app with Bluetooth connection.

Company policies typically state that employees must lock the screen when they leave their computer. By locking the screen automatically when the mobile phone is moved away from the computer or at smart card removal, the policy is automatically enforced.

nexus
IN GROUPE

Sign and encrypt emails

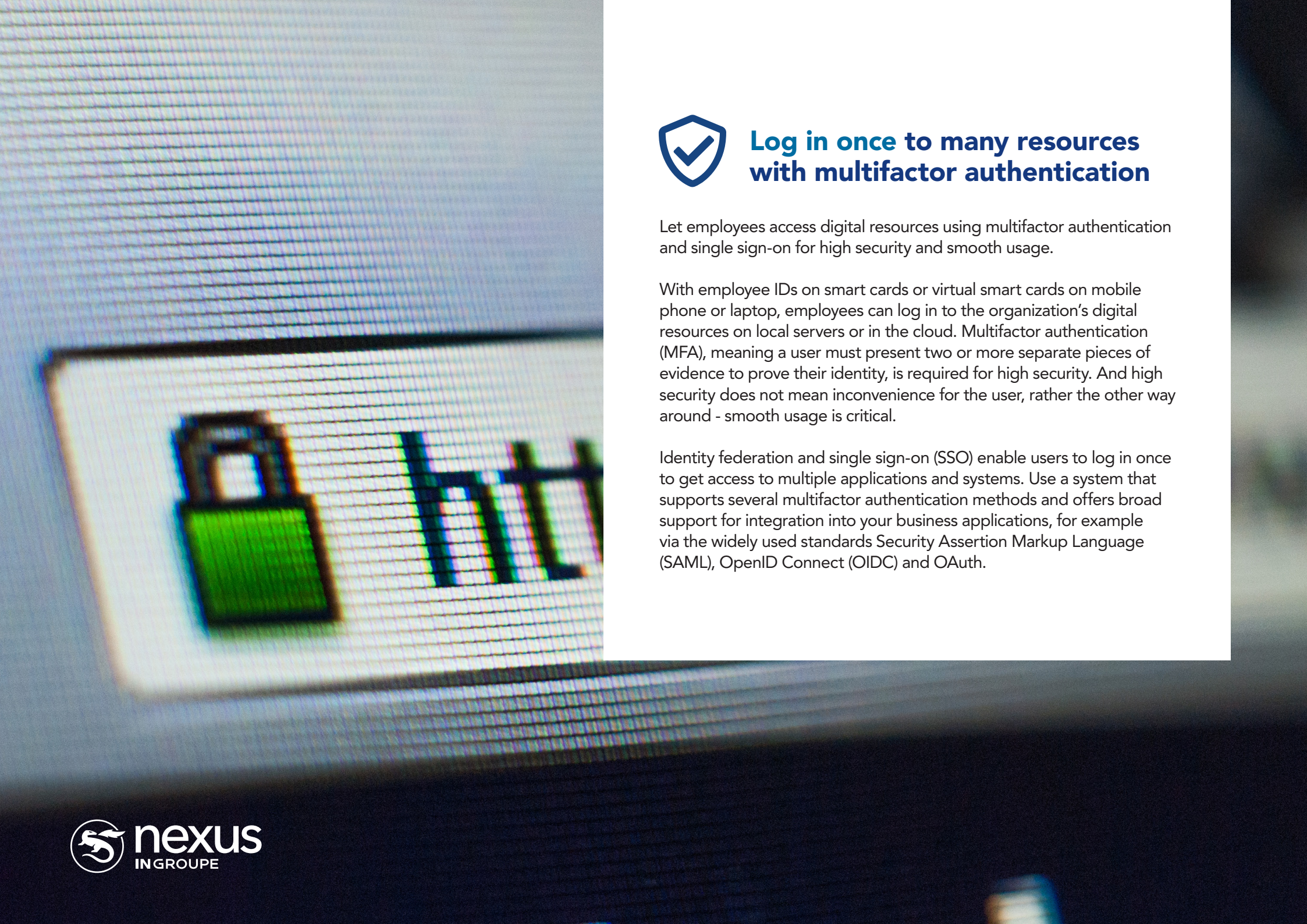
Employee emails are often an easy target for cybercriminals. Organizations need to safeguard against threats like phishing attacks, malware infections and confidential data breaches.

With S/MIME certificates, emails can be signed to prove the identity of the sender and encrypted to ensure that the content is only read by the intended receiver. These certificates can come from any CA, including trust service providers such as QuoVadis and D-Trust, and be hosted on virtual smart cards on the laptop or mobile phone or on physical smart cards.

S/MIME certificates enable the following applications to protect your email communication:

- **Digital signatures** – The content is digitally signed with an individual's private key and is verified by the individual's public key.
- **Encryption** – The content is encrypted using an individual's public key and can only be decrypted with the individual's private key.

nexus
IN GROUPE



Log in once to many resources with multifactor authentication

Let employees access digital resources using multifactor authentication and single sign-on for high security and smooth usage.

With employee IDs on smart cards or virtual smart cards on mobile phone or laptop, employees can log in to the organization's digital resources on local servers or in the cloud. Multifactor authentication (MFA), meaning a user must present two or more separate pieces of evidence to prove their identity, is required for high security. And high security does not mean inconvenience for the user, rather the other way around - smooth usage is critical.

Identity federation and single sign-on (SSO) enable users to log in once to get access to multiple applications and systems. Use a system that supports several multifactor authentication methods and offers broad support for integration into your business applications, for example via the widely used standards Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and OAuth.

nexus
IN GROUPE

Sign documents digitally

To sign paper documents with handwritten signatures can be both time-consuming and insecure, especially when signers are on different locations and paper documents are sent by mail. And when the document is signed, there is no easy way to verify that the signature and content are authentic.

Digital signatures shorten the lead times for a mobile way of working. Multiple customers, citizens or employees can sign a document at any time and place by authenticating online with existing trusted identities, such as national eIDs or employee identities. The signatures can be validated at any time and the document content cannot be manipulated without being detected.

Identify visually

Part of the physical security of an organization is to make sure that only authorized persons are present in the workplace. In a time when more employees work from home, it is more likely that you have not seen all new colleagues and consultants in real life, even if you have worked for the same company for years.

To easily identify persons on-premises, many organizations require that employees, as well as contractors and visitors, carry proof of their identity clearly visible. Employees and contractors can have a visual identity in the form of a smart card with photo and company logo or similar features in a mobile app. Temporary guests can carry a card that is clearly marked with a different color to show their visitor status. ID cards can include various visual security elements, such as a micro text or UV print. On a visual ID on the mobile phone, additional images can be added, such as a QR code linked to a certification.

Access buildings and sites

Secure physical access means the rights of employees, contractors or visitors to enter an organization's premises, while keeping unauthorized persons out, which is essential for both information security and physical security. Radio-frequency identification (RFID) technology, for example on a smart card, is the most common means to opening locked doors in offices and on sites. Other use cases for RFID include follow-me printing, payments in cafeterias or parking fees.

The individual's access rights usually depend on the rights of the user group. For example, visitors have limited access to common areas, while the IT staff needs access to all server rooms, and so on. Multi-site organizations often rely on proprietary physical access control systems (PACS) from several vendors. To align identities and access rights, it is strongly recommended to manage them in one central system that can be integrated to multiple PACS as well as the corporate directory.

Choose from various IDs to suit your needs

Organizations often provide their employees and contractors with trusted identities in multiple forms, to support various use cases with the right level of assurance. Normally, a smart card is issued to function as a trust anchor, and then the employees can use self-service to smoothly and securely derive virtual smart cards to mobile phone and laptop.

Nexus Smart ID lets you select the types of trusted identities that suits your needs, and helps you to easily issue, manage and use them throughout their lifecycle.

nexus
IN GROUPE

Do you want to know more? Contact us!

https://www.nexusgroup.com/contact/

nexusgroup.com