nexus
IN GROUPE

Enabling trusted identities

About **IN Groupe**

As a European specialist in identities, secure transactions and digital services, IN Groupe is a trusted partner in the management and protection of sensitive data.

By mastering the entire value chain of the identity, IN Groupe deploys its expertise from sovereign identity to solutions and services for professional identities and identity of things (IoT). IN Groupe is a key player aimed at upholding the right to preserve one's own identity in the digital space.

With more than 2 000 employees worldwide, IN Groupe has a €623m turnover. The Group is a trusted partner to governments and private sector customers in more than 130 countries.

IN Groupe relies on a foundation of strong values to ensure the evolution of its recognized expertise and to develop core businesses that require Ethics, Compliance, and Security. Since 2007, IN Groupe has based its Sustainable Development approach on its integrated QSE-SSI (Quality-Security-Environment and Information Security) management system, which has earned several certifications, labels and charters.

Read more about IN Groupe here:

A selection of IN Groupes certifications: ISO9001, ISO14001, ISO 27001, ISO 14298, ISO 37001, ISO 45001.

IN Groupe relies on the excellence of its brands

Nexus – Enabling trusted identities for Workforce and IoT
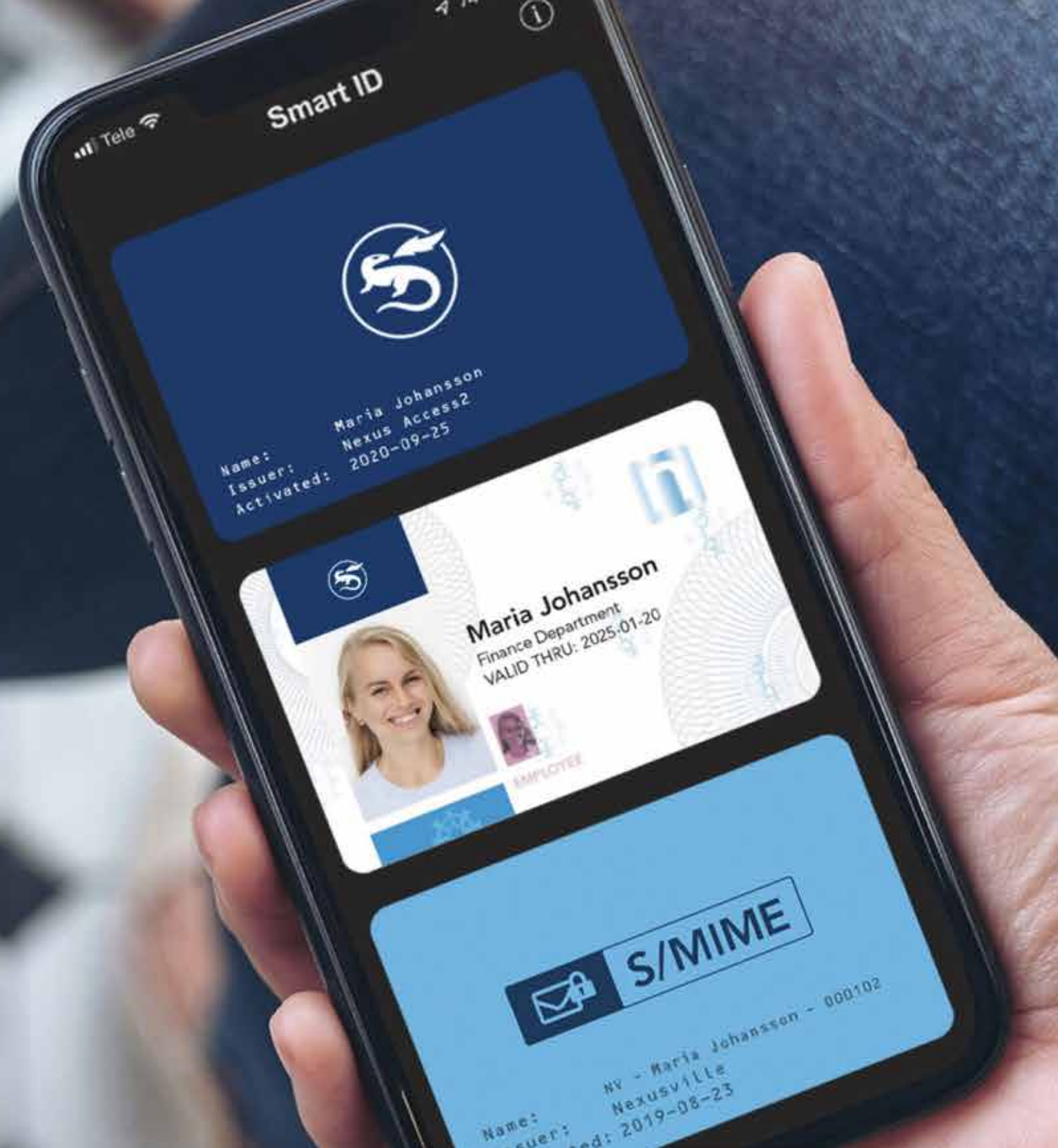
Nexus is a part of the Digital Services division within IN Groupe and are specializing in innovative and trusted identity management solutions, both in the physical and digital world.

Nexus enables organizations of all sizes and industries worldwide to issue, manage, and utilize PKI-based trusted identities for their Workforce, Workplace devices, and Internet of Things (IoT) devices. The comprehensive and trusted identity solutions help organizations achieve an identity-first Zero Trust security approach based on open standards, is future-compatible, and complies with European and global regulations.

Read more about Nexus here:

Some specific certifications relating to Nexus

Common Criteria

SP CERTIFIED ISO 27001 Information security management systems RISE

TISAX

Workforce

Workplace devices

IoT

Full identity management
Automation and compliance

Enabling trusted identities for the workforce

Secure digital transformation based on the principles of Zero Trust requires issuance and management of trusted identities to mitigate risks, ensure compliance with regulations, and restrict access based on business needs.

Trusted identities can be used to securely access facilities and digital resources, sign documents, encrypt e-mail, and more.

– **Ensure compliance with regulations**
– **Simplify on- and offboarding**
– **Integrate with standard systems**
– **Deploy as it suits you**
– **Improve usability**

Manage all **workforce identities**

Manage trusted workforce identities for employees, contractors, and visitors in one central system.

The platform can be easily integrated into existing corporate directories and other systems to enable smooth and secure on- and offboarding of employees and contractors. Automation and self-service further improve management and usability while offering complete audit traceability.

ONBOARD

USE

MAINTAIN

OFFBOARD

Smart ID for the workforce

– The platform with many choices

– Strong authentication
– Encryption and privacy
– Integrity
– Smart cards
– Mobile identities
– Virtual smart cards

– Visual identification
– Physical access
– Digital signing
– Email encryption
– Remote access

NATIONAL
SECURITY
SERVICE

Dan Brown
Valid thru: 2028-01-01

NATIONAL
SECURITY
SERVICE

Dan Brown
Valid thru: 2028-01-01

DIGITAL ID

What is a connected Workplace device?

– **Mobile devices**
– **Laptops**
– **Network equipment**
– **Printers**
– **Conference devices**
– **Servers**

Protect your connected
Workplace devices

With Smart ID, you can automate enterprise certificate provisioning for both domain endpoints, such as machines and servers, and non-domain endpoints, such as dev ops servers, mobile devices, and networking devices.

– Ensure that there are no unauthorized devices in their network
– Be compliant and ensure privacy
– Reduce the risk of service interruptions due to expired certificates
– Use automation rather than manual processes to prevent certificate expiry

Enable trust for the
Internet of Things

With billions of things connecting to the Internet, the challenge is how to address security, privacy and safety, and where to get started. Most industries need a security technology that is easy to implement, seamless in use, economical, flexible for various use cases, and scalable for future scenarios.

Everything is connected!
– Simple as well as advanced devices

Whether looking at society in general or individual business segments, including telecom, automotive, healthcare, energy, and others, digitization is at its peak, with more and more things becoming connected. The diversity of these connected devices is vast. From simple, constrained sensor equipment to advanced, self-driving cars and everything in between.

While digitization has immense benefits, it also imposes extensive requirements on the device security management platforms. These platforms must handle a broad range of devices and the large load created by the number of connected devices.
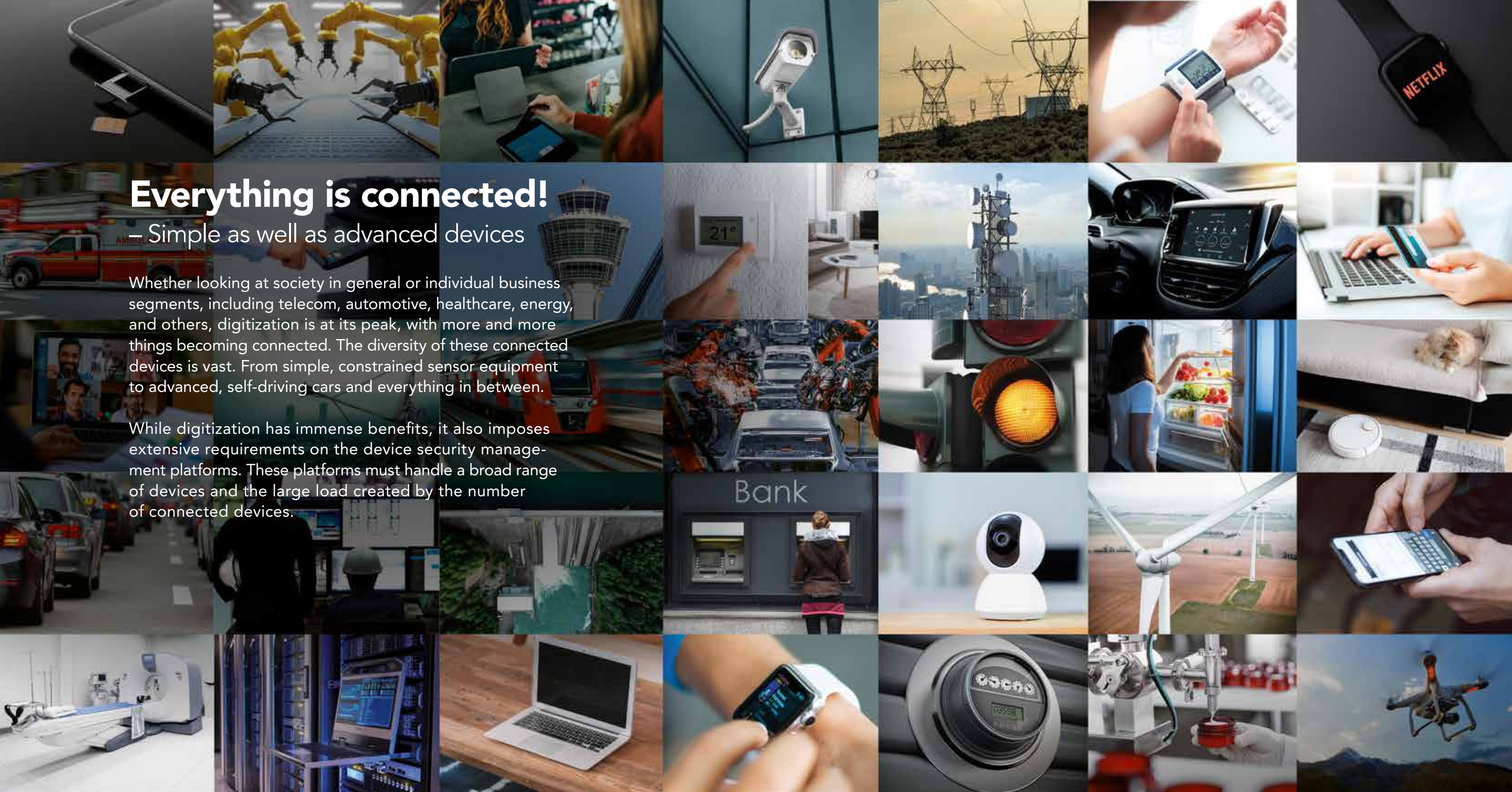
Enable trust for IoT with Smart ID
– Address a wide range of IoT devices and applications by leveraging PKI

Using a public-key infrastructure (PKI) to issue certificate-based identities enables true end-to-end security and prevents cyber-attacks against IoT applications. These trusted identities secure the IoT applications with strong authentication of devices, people, and servers to ensure encrypted communication and data integrity.

Common Criteria EAL 4+ certified Smart ID supports a broad range of certificate management protocols used by different types of connected devices. It can scale to manage smaller IoT applications as well as the bigger ones with hundreds of millions of devices.

Ready-to-use services for smooth deployment

– Adopt Identities as a Service with Nexus GO

The number of "as a service" deployments is growing due to the convenience of implementing a scalable solution, which makes it easier than ever to enable digital transformation.

Let Nexus GO manage trusted identities for you so that you can focus on your core business. Enable smooth and easy use and issuance of digital identities for all corporate users, IT devices, and IoT devices and applications.

– **We develop, install, and operate - You use**
– **Quickly deploy a scalable service with fast onboarding**
– **Benefit from using the most up-to-date software based on standard services**
– **Avoid system and application downtime due to expired certificates**
– **You pay as you grow**
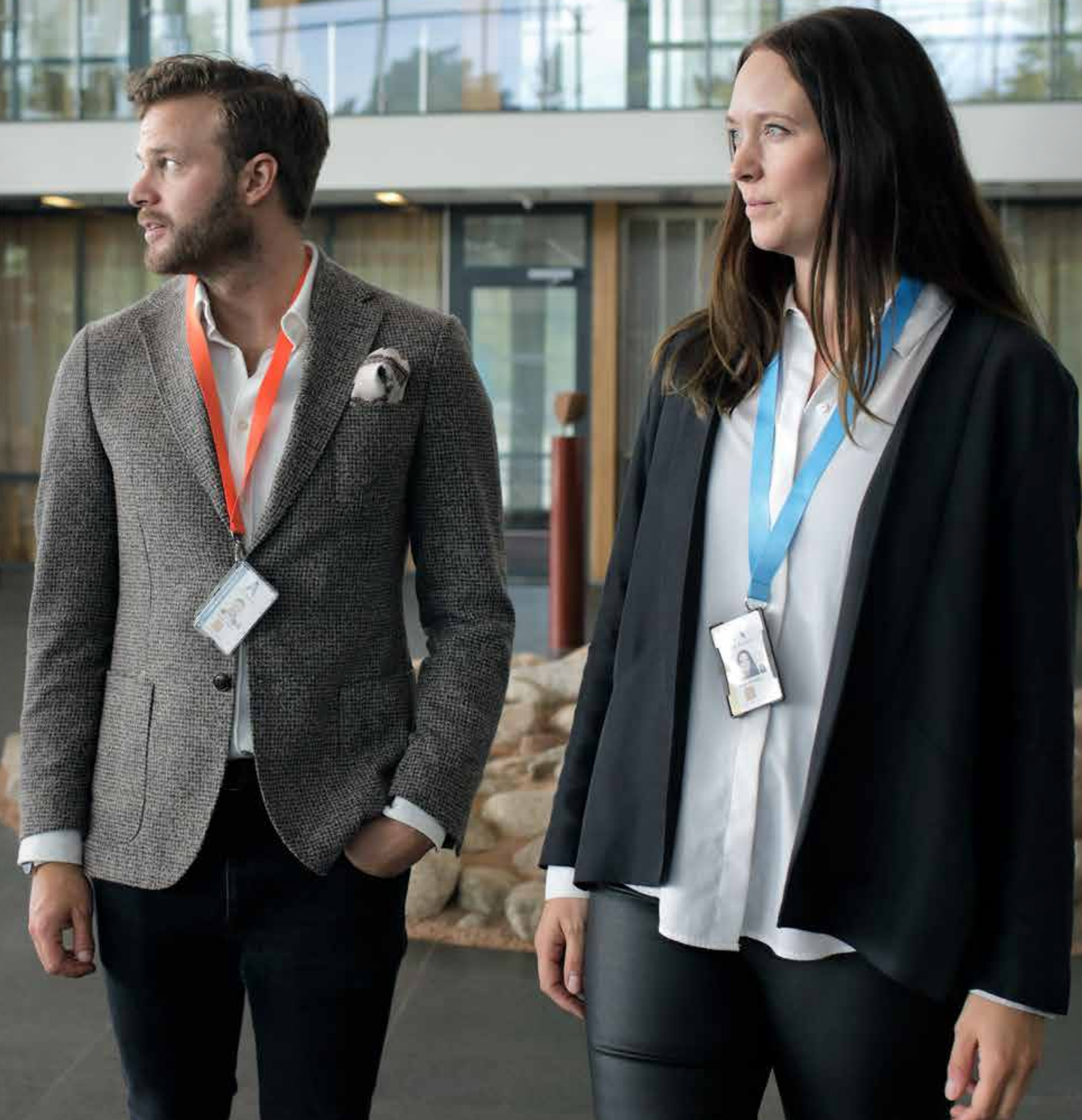
Leading organizations
trust Nexus Smart ID

The Nexus Smart ID platform is a high-performing, standards-compliant proven solution. Whether your organization needs to issue and manage PKI-based certificates to secure your workforce, workplace devices, IoT, or all the above, Nexus Smart ID is a flexible, easy-to-use, and secure platform to meet all your needs.

Don't take our word for it. See what organizations like yours have to say about it. Visit nexusgroup.com/customer-cases.
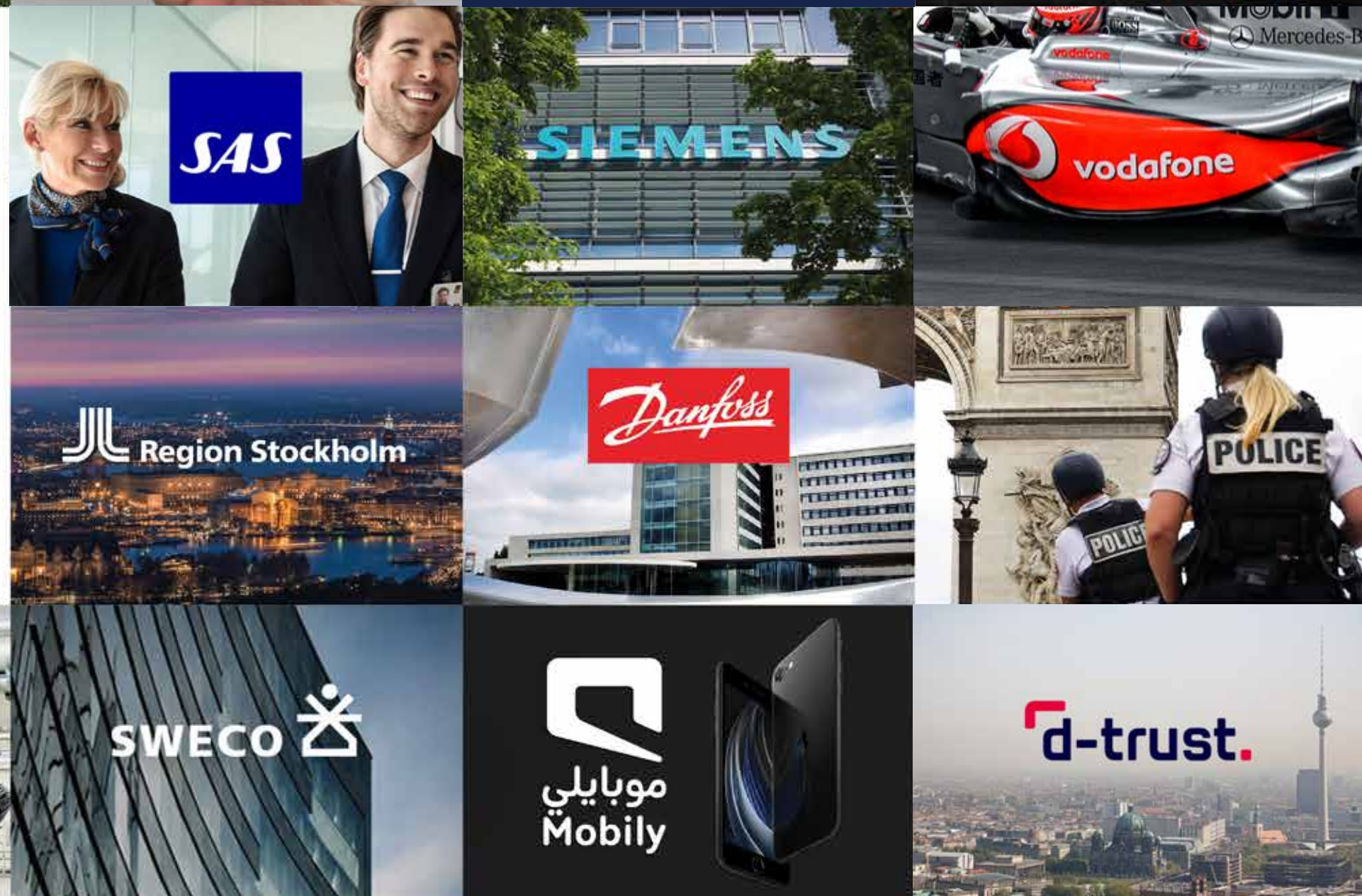
Smart ID modules and building blocks...

Creating smooth and secure identity solutions!

Nexus Smart ID provides solutions for physical and digital identities for the modern workforce as well as PKI-based identities for IoT devices.

Smart ID is a complete identity management platform that covers all needs related to the Workforce, Workplace, and IoT. It goes beyond managing identities for people and things separately and encompasses all potential combinations and interactions within these areas.

While digitization and compliance are often the main drivers for adopting a centralized identity-first security strategy, a flexible and future-proof platform is vital to ensuring success.

Let's discuss trusted identities!

nexus
IN GROUPE