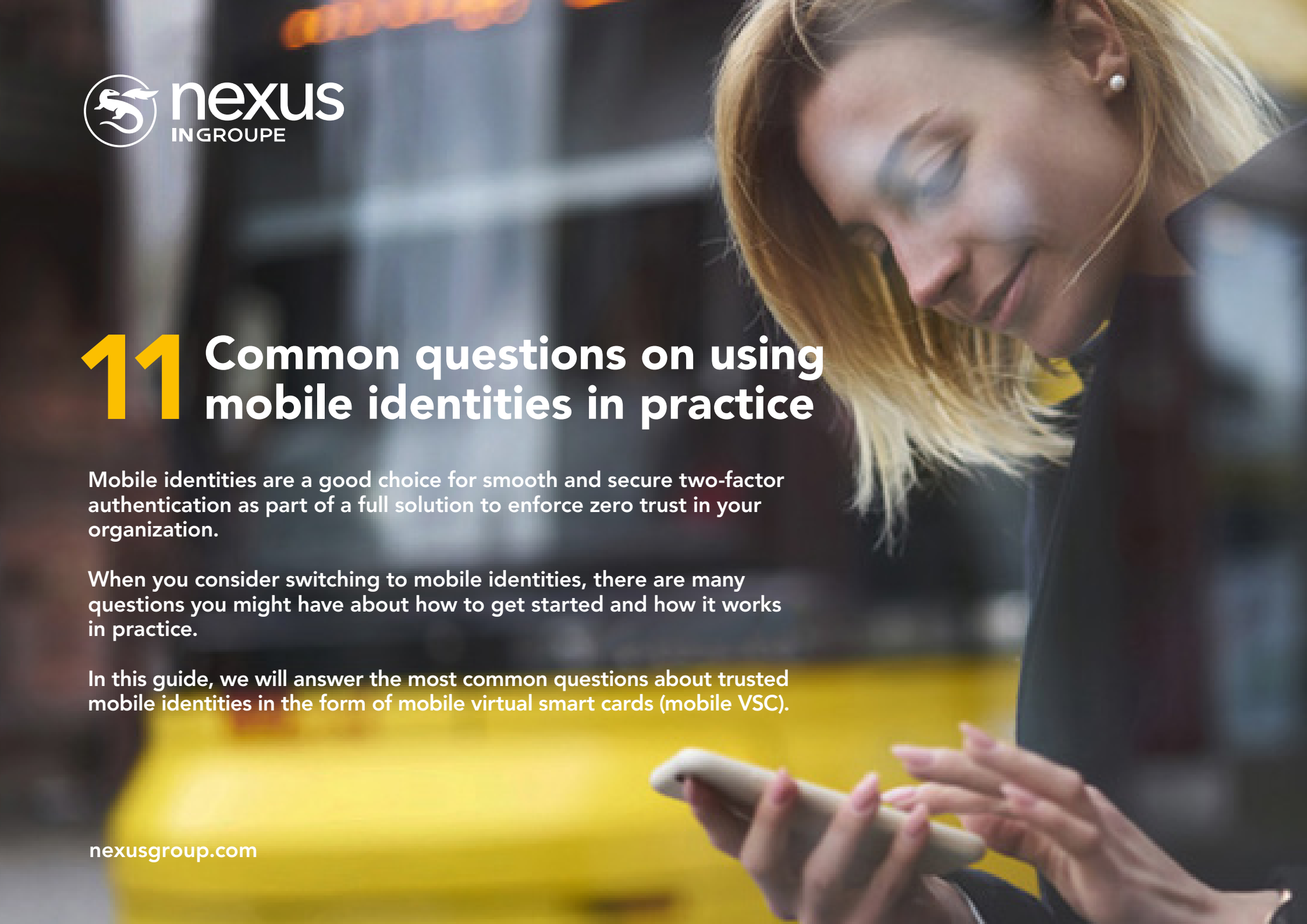


nexus
IN GROUPE

11 Common questions on using mobile identities in practice

Mobile identities are a good choice for smooth and secure two-factor authentication as part of a full solution to enforce zero trust in your organization.

When you consider switching to mobile identities, there are many questions you might have about how to get started and how it works in practice.

In this guide, we will answer the most common questions about trusted mobile identities in the form of mobile virtual smart cards (mobile VSC).

nexusgroup.com

1. Why use mobile identities?

Trusted identities on the mobile device is a highly convenient and secure method for two-factor authentication and other use cases, such as Windows logon, digital signing and email encryption. As opposed to smart cards, mobile identities mean no hassle or cost with extra hardware costs when people already have smart phones. They are easy to use, and end users prefer them over other alternatives.

2. What is a mobile virtual smart card? (mobile VSC)

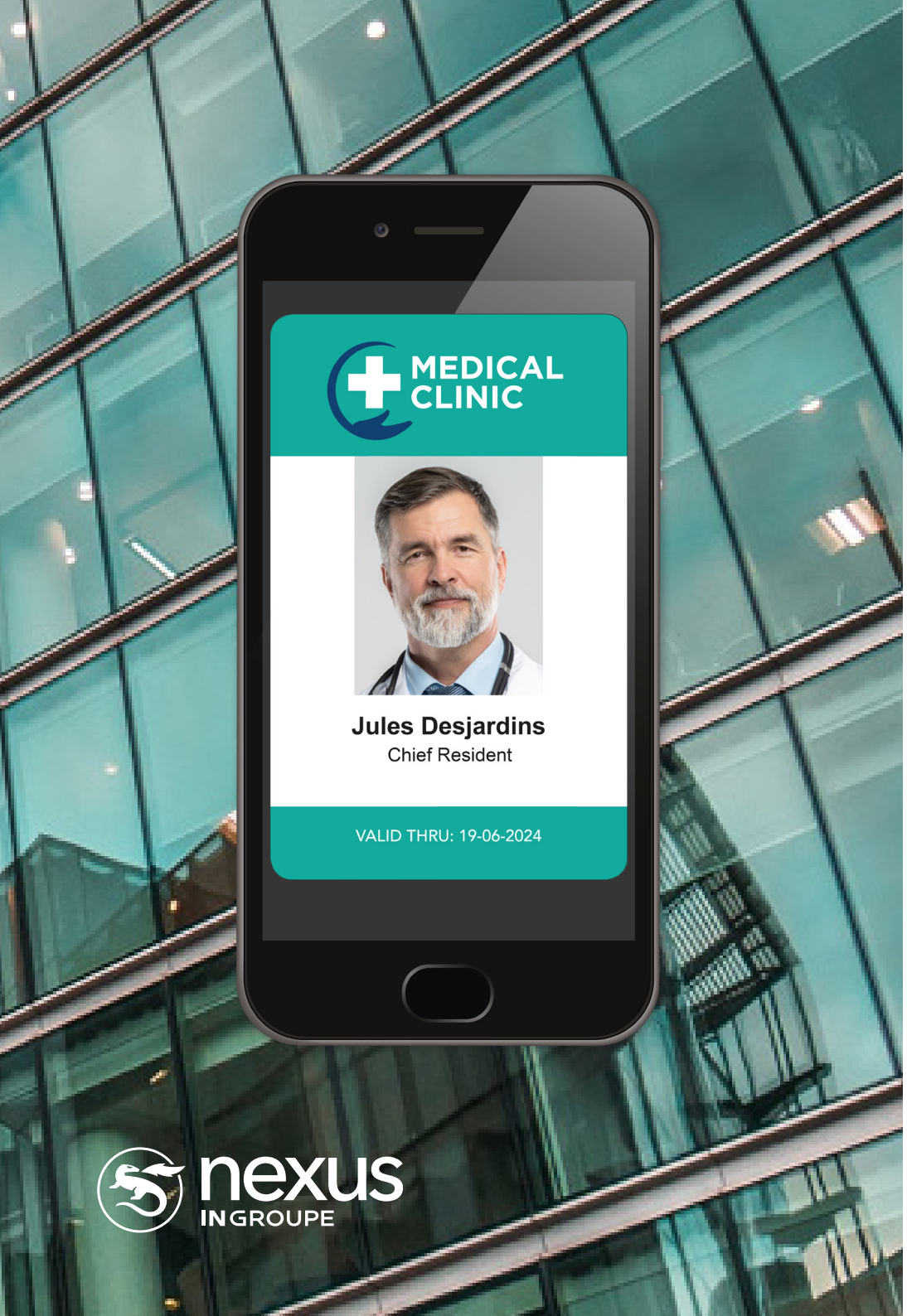
A mobile virtual smart card has the functionality of a smart card represented on a mobile device. The mobile VSC can have different features, such as a visual ID that can be branded with a company logo and individualized with personal data and photo.

The visual ID can also include a QR code for linking to digital documents or similar. One mobile VSC can have multiple certificates and they can share PIN code or be protected through the smartphone biometric. One device can host multiple mobile virtual smart cards for different purposes, including one-time password (OTP).

3. Who can use mobile virtual smart cards

Mobile virtual smart cards in the Smart ID mobile app are suitable for all types of end users, for example employees, customers or citizens. The app authentication can be based on optional unique identifiers, such as username or email from the organization's corporate directory.

This gives more flexibility compared to other solutions, such as BankID (in Sweden), that rely on the personal identity number. With the Smart ID mobile app, company employees and authority officials do not need to use their personal identity, but rather their trusted work identity.



4. What can a mobile VSC be used for?

As the name suggests, virtual smart cards have the functionality of physical smart cards. Mobile virtual smart cards in the Smart ID mobile app are mostly used for strong 2FA with certificate or one-time password (OTP) but can also be used for email encryption, digital signatures, and Windows logon.

5. How can I use mobile identities for Windows logon?

The Smart ID mobile app can be used for Windows logon with mobile devices and operating systems that support communication over Bluetooth low energy (BLE). With this support, the mobile virtual smart card can be used for logging on to Windows in the same manner as a smart card, and with the same use cases.

6. Can I use mobile identities for other Windows use cases?

Yes, when a mobile device with the Smart ID Mobile App is connected to a Windows 10 computer over Bluetooth, the mobile identities can be used for native Windows smartcard use cases like email signing, encryption and decryption, PDF signing, TLS client authentication and more. The mobile identities are simply recognized by Windows as traditional smartcards.

7. How can I use shared devices?

Nexus has recognized a big demand in the market where many organizations need to combine mobility with strong PKI-based online authentication. Scenarios are often when mobile devices are shared between many employees, who are often out in the field. The shared mobile device typically carries an App tied to the organization, for the employee to carry out his or her work duties, and here the authentication with the App becomes a problem since:

1. Using username and password is both cumbersome and leaves security compromised.
2. Mobile identities are not the answer to the problem as the identity of each employee must be replicated to every mobile device the employee will use.

Nexus' response to the problem laid out above is to combine the mobility of Nexus Smart ID App shared between many resources, with a personal physical contactless external smartcard holding the security information of each employee.

In essence, whenever the employee needs to perform an authentication, Smart ID Mobile App is triggered and lets the user enter their personal smartcard PIN code before finally tapping the contactless smartcard to the mobile device to execute the authentication.

8. Can I combine OTP and certificate authentication in the Smart ID mobile app?

Yes, the Smart ID Mobile App can simultaneously contain multiple mobile virtual smart cards on one device for either one-time password (OTP) generation or online authentication. Typically, the different types can be used for different applications, depending on the security requirements.

9. Does the Smart ID mobile app require a specific PKI platform? – Can we use ADCS?

Nexus' Smart ID solution can be connected to multiple PKI platforms, such as Nexus Certificate Manager or ADCS. The Smart ID mobile app can also be used in a simpler version with raw keys, without connection to a PKI platform.

10. How do we as an organization enroll users for mobile identities?

End users can easily be enrolled for mobile identities. A user downloads the Smart ID mobile app and enrolls with the online self-service functionality in Smart ID. To activate, the user scans a QR code with the app, and secure private keys are generated on the device.

11. How do we as an organization manage mobile identities for our users?

With the Smart ID solution from Nexus, you get full life-cycle management with self-service and automated processes for common use cases, such as to issue, renew and lock mobile identities for users. The solution includes an Identity Manager which gives a good overview of current users and mobile identities.

Do you want to know more? Contact us!

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

nexusgroup.com