Smooth management of certificates from trusted root

The joint offering of certificates from the German Trust Service Provider D-TRUST, a 100% subsidiary of the Bundesdruckerei, and Nexus Smart ID, allows the use of certificates on various devices with respective lifecycle management processes, and without the need to manually set up trust for each sender.

Use trusted certificates on multiple devices

This collaboration between Nexus and the German Trust Service Provider D-TRUST, which is a 100% subsidiary of the Bundesdruckerei, allows the use of PKI certificates for signing and encryption on various hardware devices, such as smart cards, mobile phones and laptops, with automated management processes.

Secure exchange of data using certificates from trusted root

PKI certificates are ideal for secure emails and data transfer. Organizations need to use certificates for signing and encryption in internal and external communication, without forcing the receiver or their IT department to manually set up trust to each sender. Servers need to be secured by using SSL/TLS certificates. To ensure secure processes throughout the business, a fast and efficient way to request and manage certificates is necessary.

For the receivers that use signed or encrypted information, it is tedious manual work to set up trust to various certificate authorities, if certificates do not come from a trust service provider.

Manage certificate lifecycle

Certificates can be distributed in various formats and on different hardware devices such as smart phones, laptops, smart cards or tokens. The certificates and connected devices must be managed throughout the lifecycle.

For efficiency reasons, automated processes are preferred for many cases, such as expiry of certificates or lost credentials. For example, if a user loses a phone with a mobile ID or a laptop with a softtoken, the certificates must be recovered to still have access to the encrypted information.

Solution: Smooth management of certificates from Trust Service Provider

With the solution from Nexus and D-TRUST, you can use PKI certificates from a public trusted root for signing and encryption of data and for server authentication and encrypted communication. These certificates as well as the various credentials are managed easily and efficiently in one central system.

Certificates on the right security level for your need, for example qualified or advanced, from a qualified German Trust Service Provider D-TRUST, let all receivers have immediate trust in your emails or data, without having to set it up manually.

Centralized identity and credential management with automated processes and self-service makes it easy to be in control and avoid manual work.

The solution allows a flexible use of certificates, thanks to support for multiple smart cards, keyfobs, mobile identities, softtokens and virtual smart cards.

Key archiving and recovery (KAR) is available, to recover keys for reading encrypted emails, and so on.

Key benefits

Quick and easy to request certificates

Apply for certificates for multiple purposes from an easy-to-use web interface from D-TRUST.

Trusted certificates for smooth use

Combining certificates from D-TRUST with the credentials of choice allows flexible use and guarantees high security standards.

Manage certificates and credentials in one system

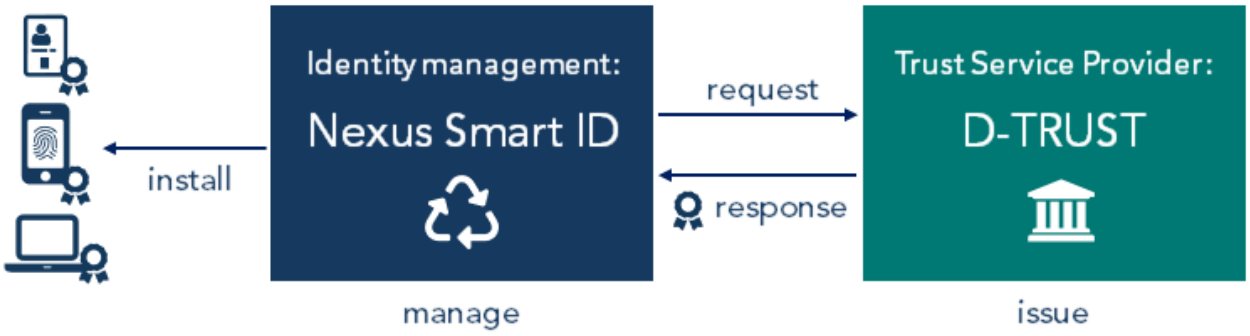
One central system with automated processes enables efficient management of D-TRUST's certificates and credentials.

Recover lost keys

If a credential is lost, key archiving and recovery (KAR) ensures access to encrypted data.

More information

- Smart ID Identity Manager
- D-Trust at Bundesdruckerei



Issue and manage certificates on multiple devices with the joint solution from identity company Nexus and qualified Trust Service Provider D-TRUST.

Nexus Smart ID Identity Manager

Nexus Smart ID Identity Manager is a solution for centralized management of identities and credentials for physical and digital access.

With Smart ID you can manage multi-functional ID cards and tokens that can be used for both physical access to buildings and authentication to computers and server applications. Smart ID integrates with various data sources, for example Active Directory, and physical access control systems (PACS).

To help manage identities and credentials throughout the lifecycle, Smart ID includes best-practice processes and workflows for production and lifecycle management. The identity and card history facilitates audits and can be used to generate reports and statistics.

Smart ID has the following benefits:

- Centralization – Manages all identities and credentials for both physical and digital access in one central system
- Control – Gives you transparency, traceability and compliance across units and locations
- Outsource – User can request and manage their certificates via self-service

D-TRUST Certificate Service Manager

D-TRUST Certificate Service Manager (CSM) is a web-based certificate management platform used to process certificate requests and to manage verification data and certificates in a one stop shop.

Using the CSM, all request and verification data for all certificates required in the future can already be sent before the actual request is made. The required verification and the purchase process take place in advance. This means direct access is available to many different types of certificates, for example SSL/TLS certificates securing data transmissions, S/MIME certificates for digital signing and encryption of e-mails and machine certificates for securing communication between machines or objects with organizational affiliation.

CSM advantages at a glance:

- Fast – Certificates made available in a matter of seconds
- Central – Certificate stock managed at the company
- Flexible – Assignment of finely graded user authorizations
- Automated – Seamless integration into existing workflows thanks to an API interface

Nexus, a part of IN Groupe, is an innovative identity management company. It secures society by enabling trusted identities for people and things. Nexus has 300 committed employees, as well as a global partner network. The headquarter are in Stockholm, Sweden. Nexus is certified in information security according to ISO 27001 and TISAX.

For more information, please visit www.nexusgroup.com or write us at contact@nexusgroup.com.

Berlin-based D-TRUST GmbH is a subsidary of the Bundesdruckerei GmbH. Regarded as a pioneer in the field of secure digital identities, D-TRUST has already been listed with Germany's Federal Network Agency since 2016 as a qualified trust service provider in accordance with the eIDAS regulation.

For more information, please visit www.bundesdruckerei.de or write us at info@d-trust.net.