



Nexus Credo Credential Manager

EASY LIFECYCLE MANAGEMENT OF VARIOUS CREDENTIALS OVER THE WEB

- Manages multiple credentials types, incl. passwords, smart cards and tokens
- Covers lifecycle from issue through renewal and replacement to withdrawal
- Supports all routines and emergency situations
- Integrates with corporate CA, directory, HR database and IDM system
- Extreme ease of use enable delegation of operator tasks to non-IT staff
- Self-services reduce helpdesk costs and raise productivity
- Card Office add-on provides high quality surface prints and RFID function
- Support for multiple organisations with secure data separation
- Secure: strong authentication, role-based, fine-grain authorisation, audit
- Flexible, scalable, independent of platform and token vendor

In a typical corporate IT environment, users own a number of credentials, like passwords, company cards, VPN software certificates and so on, which are issued and withdrawn by the IT department. IT will again be involved in emergency cases, such as when a password or card PIN is forgotten, a card is lost or left at home, a card is blocked or a certificate expires. Such events are a considerable and stressful burden for the IT department, and cause loss of working time for the credential owner. Security measures will ultimately suffer from low acceptance and will be bypassed if possible.

Nexus Credo Credential Manager provides one central tool for the lifecycle management of users' various credentials. Credo's situation-oriented, comprehensible and multilingual web interface enables non-IT staff and the credential owners themselves to conduct common tasks and deal with emergencies.

Manages multiple credential types

Credo supports several types of credentials, including passwords, smart cards, cryptographic USB tokens, software PKI tokens, certificates, PINs, PUKs and one-time passwords (OTPs). Any PKI token and smart card with standard middleware can be managed by Credo. Many token types and profiles can be managed on one single system.

Covers entire credential lifecycle

Credo supports all routines encountered during the

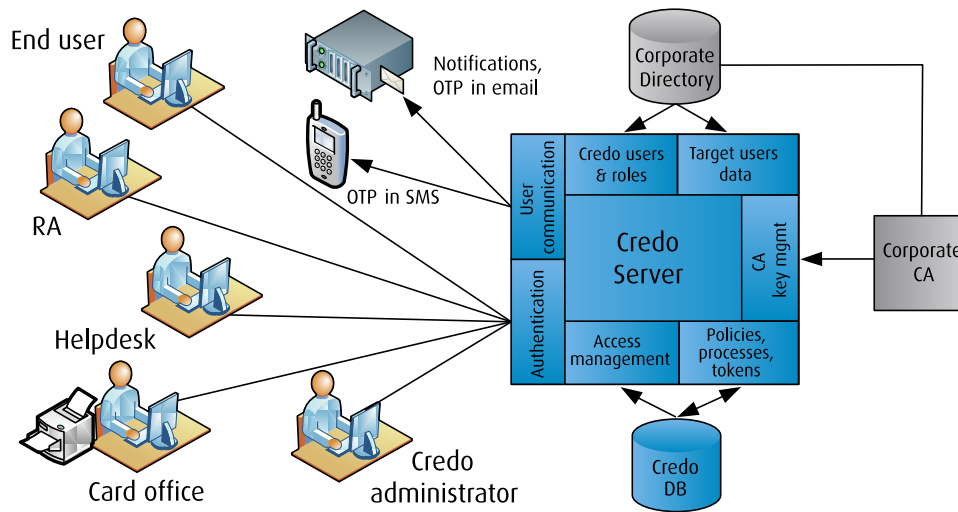
lifecycles of passwords and PKI-based credentials, and covers all real-life emergency situations. Besides the creation, renewal and revocation of PKI tokens, they can be replaced quickly when lost, broken or left at home. Forgotten passwords and PINs can be reset; blocked smart cards can be unblocked. Passwords and PINs can be changed, recovered or reset and are controlled by policies.

Integrates with corporate CA and directory

In larger organisations, user accounts and user roles are typically defined in Active Directory, an LDAP server, an HR database or an Identity Management System. Credo hooks in to any source of user data instead of multiplying user management. Credo also integrates with the organisation's Certificate Authority (CA). Credo comes with out-of-the-box support for Active Directory, LDAP servers and Nexus CA.

Simplicity enables use by non-IT staff

Credo puts an emphasis on simplicity and user-friendliness: the situation-oriented and intuitive user interface hides the complexity of PKI, directories or other systems and concentrates on the simplest and quickest possible completion of tasks. This enables the delegation of credential management tasks to non-IT staff, who can handle situations at the right place in a short time without special training. The result is lower operational costs and rapid emergency resolution.



System overview

Self-services reduce helpdesk costs

Statistics show that the average IT user runs into trouble four times a year due to forgetting or losing credentials, with each case demanding considerable time from both the user and the IT department. Credo provides credential owners a uniform, user-friendly web application to maintain their credentials on their own. This saves helpdesk costs and increases user productivity and acceptance.

Advanced surface prints and RFID functions

The Card Office add-on in Credo enables the batch production of cards. The integrated Card Management System (CAMS) features advanced multi-layer card surface printing with holograms and UV readable images for safe "optical" authentication. RFID chips from major vendors are encoded during the same procedure as surface printing and PKI personalisation. The result is a fully fledged corporate badge that combines best-of-breed physical and logical security functions.

Support for multiple organisations

Credo has been designed for the needs of large, distributed organisations and service providers. Accordingly, data from several organisations or clients can be maintained on the same system, while virtually being completely separated.

Authentication, role-based authorisation, audit

Credo is a highly secure platform: users are authenticated with the necessary level of assurance by one of several possible methods. Emergency cases allow the use of secondary credentials, such as the user's domain password or an OTP. Users' permissions to perform certain tasks and to work on specific user groups are controlled on the basis of their role. Users' roles are linked to external user

management, e.g. groups or roles in the directory. Credo comes with a well-designed set of typical roles and corresponding access profiles, which can be changed or extended at any time. All logins and actions are logged in a revision-safe searchable audit log.

Flexible, scalable, platform-independent

Credo is open and flexible in many respects. The GUI can be customised to a familiar corporate design. Customers can implement individual roles, processes and token profiles. Credo integrates in principle with any user database, CA and access management system. Credo server runs on Windows and Linux and requires no web application server. The clients require only a browser and are thus nearly administration-free and always up-to-date.

About Nexus

Nexus Technology works internationally with e-communication, information and security solutions. Our clients are companies and organisations for which IT and the Internet are essential to the management of sensitive information and knowledge. Nexus' business concept is to offer solutions, products and services that make the right information available to the right people, at the right time, wherever they need it in the world. We help our clients to not only protect their information, communication and knowledge, but also to create opportunities to make more effective use of them. Nexus is an international company headquartered in Sweden and with offices in several European countries and partners all over the world.

