Nexus Authentication Server

Product Brief

Version: 1.2

Introduction

Protecting your digital resources and services using only username and a static password as authentication method is not secure enough. Why? Passwords must be long and complex, to be less unsecure. Passwords must be changed frequently. Users often reuse the same password for different services. If a password for one service gets into the wrong hands, unauthorized people can not only get access to that service but also to a range of other services. Passwords can be easily stolen through social engineering. There is an endless range of methods, for example, convincing emails or spoofed websites where people are asked to share their username and password. And, a surprisingly large percentage of people do share their login information when asked to.

Using multi-factor authentication from Nexus dramatically mitigates the risk of unauthorized people getting access to services and information. As part of Nexus Hybrid Access Gateway, the Authentication Server provides a unique solution for enabling trusted authentication, without the complexity of distributing and maintaining hardware security tokens. Using Nexus solution, organizations can empower their users with authentication technology that is easy to use, easy to manage, cost effective and secure, to enforce strong multi-factor authentication.

Enable strong user authentication throughout the organization and customer base without the complexity of distributing hardware security tokens.

What is multi-factor Authentication?

The security and trust level of an authentication solution depends on the number of factors required for successful identification. An authentication solution capable of withstanding any type of identity fraud should consist of a combination of these factors:

- What you know:
  A static username and password
- What you have:
  A unique possession, such as a hardware token, a mobile, or smartcard
- What you are:
  A unique biological characteristic, such as a fingerprint or iris pattern

Strong multi-factor authentication protects against phishing, password cracking, key logging and many other types of identity theft.

Enabling trusted identities

Nexus Hybrid Access Gateway Authentication Server

Nexus Hybrid Access Gateway Authentication Server is a software based solution that provides strong multi-factor authentication to applications and services. Nexus solution is unique as it does not require the organization to purchase, distribute or maintain expensive hardware tokens for each user. The Authentication Server can utilize hardware that the end user already has, such as a mobile phone, smartphone or a tablet, to deliver strong one-time passwords.

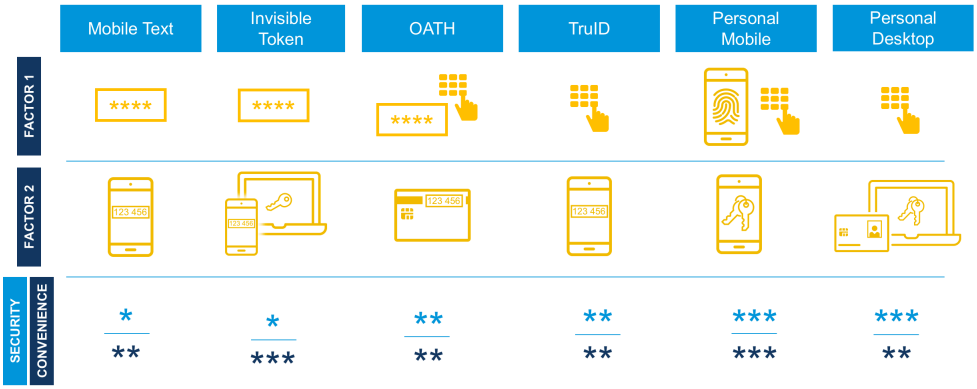
Nexus Hybrid Access Gateway is based on leading industry standards to guarantee operability with existing applications and security infrastructures. Any application, router, firewall or gateway that supports RADIUS can utilize strong multi-factor authentication from Nexus. The solution supports SAML 2.0 as well as OAuth 2.0. For applications that do not support any of these standards, integration with Web Services interface is offered.

Nexus offers several different authentication methods of different strengths in one flexible and integrated, versatile authentication solution,. Nexus Hybrid Access Gateway includes the following multi-factor authentication mechanisms:

- Nexus Personal Mobile
- Nexus Personal
- Nexus TruID
- Nexus Mobile Text
- Nexus Invisible Token
- Nexus OATH, HOTP, TOTP and OCRA

Versatile and risk appropriate authentication

The benefit of using a platform supporting versatile authentication is that you can select to apply the most appropriate authentication method for each application. Practically, you can use simple password-based authentication to provide access to less sensitive applications, and more complex authentication to secure access to highly sensitive data. When an already authenticated user requests access to a more sensitive application, you can apply step-up authentication, which requires the user to authenticate again with an additional credential. This is what the industry refers to as risk-appropriate authentication.



Nexus solution is easy to integrate with existing infrastructures. It uses standard authentication protocols and is extendible through a plug-in API, which facilitates the use of new or custom authentication methods. Open standards such as X.509, Open Authentication, RADIUS, LDAP, SAML 2.0 and OAuth 2.0 are supported.

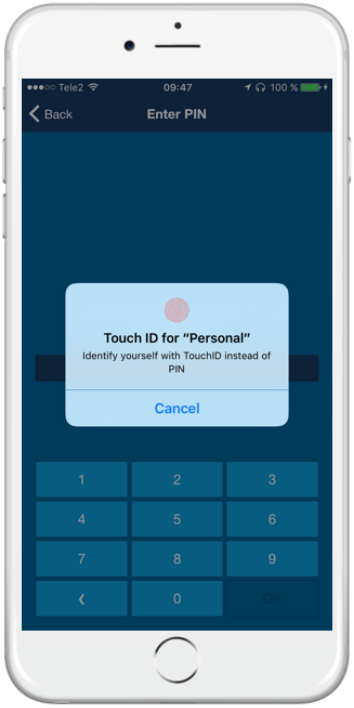
Enabling trusted identities

Nexus Personal Mobile

Nexus Personal Mobile is a mobile app that makes two-factor authentication (2FA) and digital signing easier and more cost efficient. It is used together with Nexus Hybrid Access Gateway, which provides user authentication and access to applications, portals and cloud services. Hybrid Access Gateway supports a wide range of authentication methods, and Personal Mobile is the newest one.

Personal Mobile is very easy to use and supports push notifications. The iOS and Android platforms are supported, and for iOS devices Touch ID is supported. To authenticate with Personal Mobile, the user then only has to press the smartphone's fingerprint reader.

Onboarding of new users is easy and the personalization of the Personal Mobile app can be securely done online. The enrolment process is very user friendly. Once users are invited, they can download Personal Mobile from Apple's App Store or Google's Play Store. The user gets a one-time activation code distributed as a clickable link or as a QR code that is scanned by the mobile app. The activation process can be invoked either by an administrator, the help desk or by the user itself through the self-service function.



Personal Mobile consists of multiple layers of security. Private and public keys are used. During authentication, the user must verify a random image in the mobile app and the target application to prevent against session hijacking. The user's digital identity is protected with multiple encryption layers and device-binding. The mobile app is highly secured and protected against reverse engineering, jail-breaking, debuggers, and rootkits.

Personal Mobile is also available as a software development kit (SDK), allowing for close integration with other mobile apps.

Key features

- Intuitive and user-friendly two-factor authentication (2FA)
- No need for additional hardware tokens, which reduces the total cost of ownership and enhances usability
- Takes advantage of the fact that most users already have a mobile phone
- Easy enrollment process for the end user via QR code
- Support for multiple users/user profiles
- Push notifications in the mobile phone for immediate communication with the user
- Support for iOS and Android
- Support for Touch ID
- Ready-to-use app available for download from Apple's App Store and Google Play Store
- Software development kit (SDK) available for embedding in your own app
- Strong protection of the private keys by multiple encryption layers and device-binding
- Integrity protected app with embedded obfuscation, which means that the code is protected against reverse engineering and malware

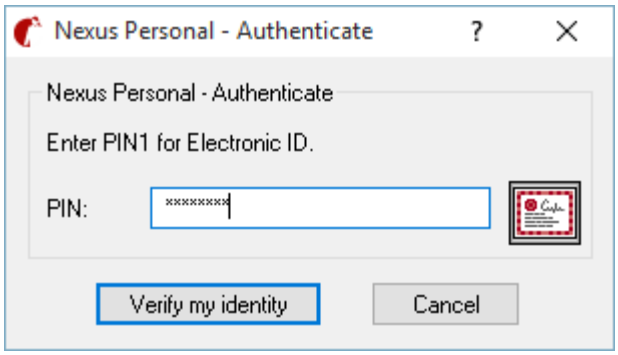
Nexus Personal Desktop

Nexus Personal Desktop is a client software that provides your users with intuitive two-factor authentication (2FA) and digital signing straight from their desktops, with or without a smart card. The client is well-suited for cloud, Windows, Mac and Linux applications .

Personal Desktop uses the public key infrastructure (PKI) security method. The PKI-based eID needed for authentication and digital signing is stored either as a software token on the user's computer, or on a smart card or some other hardware token. If a smart card is used, a card reader is connected to the user's computer. To authenticate or sign, the user types a PIN into the user interface, which pops up automatically.

Use cases include enabling user-friendly 2FA for desktop applications, domain login, and remote desktop and VPN access. The solution is also well-suited for secure and cost-effective identification of users of online banks, e-commerce sites or e-services in the public sector. The signing functionality can be used for transactions such as online shopping, loan applications, contract signing and tax declarations.

The client software is installed on the users' computers, and their eIDs and PINs are managed by the administrator through a web portal. It is easy to configure Hybrid Access Gateway out-of-the-box to require Personal Desktop for 2FA. If Personal Desktop is to be used with your online services, you integrate the included message server in your online service solution. The client software works with all web browsers, and does not require plug-ins.



Personal Desktop can be used together with the access solution Nexus Hybrid Access Gateway, which enables users to authenticate themselves and get remote access to digital resources. Since Hybrid Access Gateway supports identity federation and single sign-on (SSO), the user only has to log on once with Personal Desktop to reach all exposed resources. Personal Desktop is also very well suited for secure mobile eID activation in the Nexus Personal Mobile app.

Key features

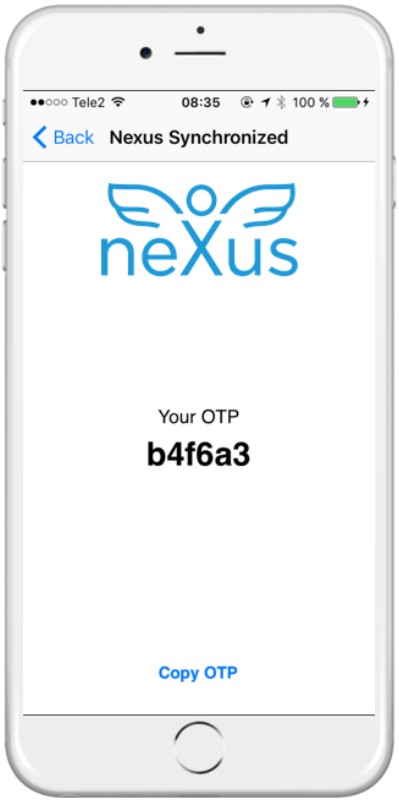
- Provide your users with intuitive two-factor authentication (2FA) and digital signing, straight from their desktops
- Support for smartcards and file based certificates
- Support for Windows, Linux and Mac
- Use a method for identity control that supports single sign-on (SSO)
- Support for all web browsers, and does not use plug-ins

Enabling trusted identities

Nexus TruID

Nexus TruID is a mobile two-factor (2FA) software token that is installed on a hardware device that the user already has, such as a smart phone, PC (Linux/Windows) or a Mac. The user enters a pin code into the soft token to generate a one-time password, OTP. This OTP is used to logon to the application or service.

The TruID token generates a unique OTP for each user and for every authentication attempt. The user simply starts the app and enters their PIN to get the OTP. To generate the OTP a unique seed is used in combination with a PIN and a random challenge or a user specific counter. To personalize each users TruID client, it must carry a unique seed that is generated by the Hybrid Access Gateway Authentication Server.



To ease distribution of Nexus TruID the solution includes the Distribution Service that enables automated token distribution, installation and set-up. The Distribution Service ensures that this process is fully automated for smooth and easy end-user deployment. All the end-user has to do is follow an URL link sent by the server in an SMS and within seconds the user is equipped with TruID mobile two-factor authentication.

Nexus TruID is available in two modes; Challenge and Synchronized. TruID Challenge requires a challenge response. Users enter their PIN and a server initiated challenge when generating OTPs. TruID Synchronized instead utilizes a user specific counter. Users simply enter their PIN to generate an OTP. This usually is simpler for the user, since there is no challenge to read and enter into the TruID token. The Synchronized mode includes support to re-synchronize the counter if the offset has been exceeded and time differential is too large.

Key features

- Mobile two-factor authentication
- Support for Android and iOS
- Support for Windows, Linux and Mac
- Works offline
- Secure online seed distribution
- Challenge-Response and Synchronized modes

Nexus Mobile Text

Nexus Mobile Text utilizes the mobile phone and a mobile text-distribution service such as SMS (Short Message Service) to distribute the One-Time Password. By using SMS, any mobile phone can be used for this two-factor authentication(2FA) method, and smart phones are not required.

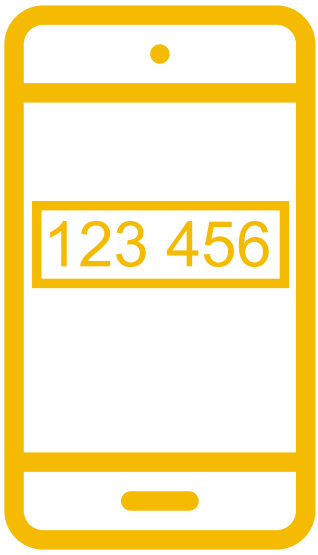
Nexus Mobile Text is a two-factor authentication solution that combines a static password with the possession of a physical device, a mobile phone. The user authenticates by entering username and password. If the credentials are correct, an OTP is generated and sent to the user's device. The user enters the received OTP in next step to authenticate. Mobile Text relies on a message delivery infrastructure, such as SMS (Short Message Service) or e-mail. The solution can use a wide range of distribution channels to deliver OTPs.

The Mobile Text authentication method integrates with Microsoft Active Directory and can reuse the username, passwords and mobile phone numbers residing in an Active Directory. With Mobile Text, comes self-service functionality to manage the passwords. Passwords that will expire or have expired can be updated. Forgotten passwords can be reset and the user account can be recovered through the self-service functionality.

You can define your own password policy and set requirements for password length, complexity, disallowed characters, password change and password history. The solution can integrate with Microsoft Active Directory and reuse the passwords from Active Directory. Then the password policies in Active Directory will apply when a user changes or resets a password.

Key features

- Easy to use
- Easy to roll out
- Works with any mobile phone
- Reuse Microsoft Active Directory Passwords
- Support for password reset/recovery
- Support for password change
- Self-service function to manage passwords



Nexus Invisible Token

The Nexus Invisible Token is a unique on-demand solution that combines the strength of passwords and tokens for two-factor authentication (2FA). It is secure, convenient, easy to deploy, and most importantly easy to use. Invisible Token is based on HTML5 and transforms your browser into an OTP-token that is independent of the platform you are using.

Your browser is enrolled when used for the first time with a technology that seamlessly configures your browser and integrates an OTP-token into it. The standard activation flow is using a one-time activation code to activate the current browser. The activation code is sent to the user as SMS or email. Roles or persons in the organization with a clear connection to the user can be used to support the user in activating the Invisible Token. It could for instance be a team member, manager or help-desk staff that is selected to receive the activation code as a fallback or emergency operation. The deployment process can reuse existing passwords and other information available in directory services. Through simplified provisioning an administrator or help-desk can allow a browser to be activated at next logon, without using activation code. The user will be able to activate one browser using only username and password.

Once enrolled, the usage of Invisible Token is transparent to the users; they continue using password based authentication and existing passwords in directories such as LDAP or by using Active Directory. The end user never needs to interact with Invisible Token – all they need to do is enter their username and password on a trusted device using a trusted web browser.

The OTP algorithm is based on the standard from Open Authentication, OATH HOTP. The seed used to calculate the OTPs is stored using the WebCrypto API in the browser. The use of a not-exportable flag protects it from theft based on e.g. user tampering or XSS (Cross Site Scripting) attacks. The OTP-token in the browser has a configurable lifetime. If the end user loses their password, in e.g. a phishing attack, the attacker will still be unable to log on using the stolen password, as they don't have access to an activated browser.

You define your own password policy and set requirements for password length, complexity, disallowed characters, password change and password history. The solution can integrate with Microsoft Active Directory and reuse the passwords from Active Directory. Then the password policies in Active Directory will apply when a user changes or resets a password.

Key features

- Easy to use
- Easy to roll out
- Based on HTML5
- Activation codes distributed in SMS or email
- Can reuse Microsoft Active Directory Passwords
- Support for password reset/recovery
- Support for password change
- Self-service functions to manage passwords and register trusted devices
- Uses open algorithms from Open Authentication
- Uses secure key storage in browser (Web Crypto)

Nexus OATH

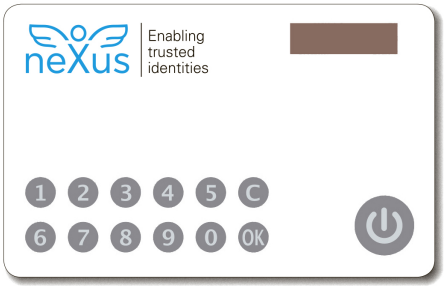
With Nexus Hybrid Access Gateway Authentication Server, any OATH compliant software or hardware security token may be used to provide user authentication. OATH provides an open architecture enabling customers to replace disparate and proprietary security solutions to increase flexibility and to lower TCO.

The Initiative for Open Authentication (OATH) addresses the challenges with implementing solutions for strong authentication based on OTPs by defining standards and open technology that is available to all. OATH is taking an all-encompassing approach, delivering solutions that allow for strong authentication of all users on all devices, across all networks.

Nexus solution supports OATH HOTP, TOTP and OCRA from Open Authentication. You can use one button tokens or tokens with PIN protection. The platform is fully compliant with the OATH reference architecture and endorses the development and adoption of interoperable solutions enhancing ease of use for end users.

Key features

- Open standards
- Multiple vendors of hardware tokens
- Key fobs
- Display Cards
- Multi-functional display cards
- Cost efficient compared to proprietary tokens



Nexus Password

Nexus Password is the most basic offered authentication method.

You can define your own password policy and set requirements for password length, complexity, disallowed characters, password change and password history. The solution can integrate with Microsoft Active Directory and reuse the passwords from Active Directory. Then the password policies in Active Directory will apply when a user changes or resets a password.

This method is most suitable for environments with lower security demands.

User management and self service

User management is done using the web based administration console which supports delegated management so that the helpdesk staff can only manage the right user account. It is also possible to integrate and automize user administration using the web services API, XPI:WS. Personal Mobile and TruID are securely activated online. Provisioning through LDAP and Active Directory is supported to fully automate the enrollment process without requiring any manual user administration.

A forgotten password helpdesk case costs businesses significant amount of money. Especially after the holiday season, the requests to reset forgotten passwords pile up. Through the web portal, Nexus solution offers a secure and efficient tool that allows your users to manage their passwords autonomously. When a password is about to expire, the user will be notified and asked to update the password. If a user has forgotten his password or locked his account due to too many failed attempts to log on, the function for password and account recovery is activated. The user requests a recovery code via the login page. The code is sent to the user as a text message or email and is valid only once and for a limited time. New passwords are automatically checked for compliance to password policies. Hybrid Access Gateway also checks the password history to make sure that passwords cannot be reused. The solution can integrate with Microsoft Active Directory and can therefore also manage the accounts and passwords within Active Directory.

Summary

It is time to say goodbye to passwords and implement two-factor authentication (2FA) instead. Organizations cannot afford to risk the immense damages that leaked passwords could entail. Passwords are a hassle for both internal and external users, and there are now better login methods available. End-users demand more convenient authentication methods than passwords since 2FA methods have become user friendly. 2FA methods have become easy to implement, even for the mobile workforce. Using Nexus solutions, organizations can empower their users with authentication technology that is easy to use, easy to manage, cost effective and secure, to enforce strong multifactor authentication.

How to contact us

To provide feedback, please send an email to products@nexusgroup.com. If you have questions about the product or this description, do not hesitate to contact us.

General information is available at: www.nexusgroup.com.