5.11 - Authentication methods

This article describes authentication methods available in 5.11 - Nexus Hybrid Access Gateway. Authentication methods are used as requirements in access rules for authentication. Different authentication methods provide various levels of security.

How does authentication work?

When a user uses a web browser to access a resource, the request flows through a web of specialized services: the access point, the policy service, the authentication service, and back again. But for the user, the single point of contact is the web browser. The access point verifies the identity of the user by forwarding the user credentials via the policy service to the authentication service, which in turn compares the information with credentials stored in the user storage. When the control is completed, a request accept is sent to the access point which allows the user to enter.

What authentication methods are supported?

There are many authentication methods supported by Hybrid Access Gateway, for example, the Hybrid Access Gateway methods: Personal Mobile, Personal Desktop, Password, TruID, OATH, Invisible Token, and Mobile Text. They are all based on the RADIUS protocol. Other authentication methods are, for example, Swedish Mobile BankID, SecureID and LDAP.

To choose the authentication method, you need to consider your users' needs: mobility, device flexibility, and level of security. A number of authentication methods can be set for each resource and it is also possible to specify multiple authentication methods for a specific resource.

Description of commonly used authentication methods

See also 5.11 - Set up Personal Mobile authentication.

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. 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 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.

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 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.

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. See [Set up Nexus TruID and Nexus Mobile Text as 2FA](#).

For more information, see [5.11 - Brand TruID client](#).

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.

Nexus Mobile Text uses the mobile phone and a mobile text-distribution service such as SMS 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. See [Set up Nexus TruID and Nexus Mobile Text as 2FA](#).

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 or email. 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. If Mobile Text is integrated with Microsoft Active Directory the password policies in Active Directory will apply when a user changes or resets a password.

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.

For more information, see [5.11 - Invisible token](#).

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 non-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.

With Nexus Hybrid Access Gateway Authentication Server, any OATH (Open Authentication) 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.

The Initiative for 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.

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.

Nexus Hybrid Access Gateway support authentication using the Swedish national eID BankID. With Hybrid Access Gateway you can let your users authenticate with BankID on smartcard, file or by using a smartphone with Mobile BankID. There are multiple ways to connect Hybrid Access Gateway to the service for validation of BankID and Mobile BankID. By using a national eID such as BankID you can easily and securely enable your services for a large number of customers without the burden of managing their credentials and authentication methods.

BankID is an electronic identification solution that allows companies, banks, organizations and governments agencies to authenticate and conclude agreements with individuals over the Internet. BankID is an electronic identity document comparable to passports, drivers licenses and other physical identity documents. Since Swedish banks are the issuers of the BankID credentials, the users obtain their BankID from their bank. Normally using their Internet bank and a self service to obtain the BankID or Mobile BankID. In this way you will not carry the burden of providing, or managing the lifecycle of your end users eIDs. This also means that you will get instant access to one or several secure ways to authenticate a large number of your end users.

Nexus Hybrid Access Gateway is a flexible solution for enabling strong authentication using national eIDs like BankID and Mobile BankID. When using Hybrid Access Gateway for authentication with BankID or Mobile BankID all you need to do is configure Hybrid Access Gateway to connect to an API. There is no need to develop specific support for the National eID within your own organization. Currently three different APIs and standards are supported.

When using Nexus GO for BankID authentication you connect the cloud service Nexus GO provided by Nexus. Nexus GO provides a self service portal where you easily can register and subscribe to the Nexus GO service for BankID and Mobile BankID authentication. All information about how to connect Hybrid Access Gateway to Nexus GO is provided in the portal and you can start using BankID for authentication in minutes. Nexus GO will manage all contacts with the re-sellers of BankID and will also act as the relying party to the BankID service.

For more information, see Nexus GO Services and 5.11 - Set up Nexus GO as an authentication method.
Nexus Managed Services offers authentication with BankID and Mobile BankID using the SAML 2.0 standard. Hybrid Access Gateway supports the SAML 2.0 standard and can connect to any service, providing BankID authentication using the SAML 2.0 standard. Nexus Managed Services will manage all contacts with the re-sellers of BankID and will also act as the relying party to the BankID service. The SAML 2.0 support is also used to connect Hybrid Access Gateway to eIDAS and the Swedish eID system for national eIDs.

For more information, see 5.11 - SAML 2.0 federation.

When using a direct integration to the web service API for relying parties from BankID, Hybrid Access Gateway is configured to connect directly to the BankID services. You will need to subscribe for the BankID service from one of the banks that are reselling the BankID service.