POINTSHARP

Net iD Software Suite

Net iD Portal
Net iD Access
Net iD Enterprise

pointsharp.com

Net iD Enterprise

The client software Net iD Enterprise is the most commonly used middleware on the market for establishing strong Multi-factor Authentication based on certificates and PKI. Net iD Enterprise integrates smartcards and other certificate carriers with all types of applications and IT environments. The solution makes it simple to establish the highest possible level of security, without users finding the process difficult and complicated.

Simply decide which work environment you want to protect, and we will swiftly deliver an optimal solution for the operating system of your choice: Windows, macOS, Linux or Chrome OS. The solution provides the best protection for logging into computers, domains, applications, identity providers (iDP), online services, and servers. It also protects login to Office 365 and all other cloud services. And together with the Citrix platform, the solution supplies ultra-swift, secure Single Sign-On and smartcard roaming.

You can also take out a support agreement to access professional support for all the Net iD products you use.

How it works

Net iD Enterprise makes it simple to log in securely. With a certificate on an ID carrier of their choice, users can log into applications and web-based services that require electronic identification and signature based on PKI. The same ID carrier can also function as visual identification for entry into the workplace and for secure follow-me printing.

In large organizations comprising numerous users with different needs, we supply customized Net iD packages and associated components to match specific requirements and target environments. This assures maximum use benefit and significantly simplifies the roll-out of the software. Customer-specific solutions include, for example, customized configurations, own PIN dialogue (logo), and MSI package with built-in license key.

In most projects, our customers use Net iD Portal for life cycle management of Certificates. This is the added value that underpins the entire setup through the administration of digital identities in the entire organization.

Benefits with Net iD Enterprise

- Built on standard components, functions in all usual system environments,
- Platform-independent. Windows, macOS, Linux, Chrome OS,
- Support for all common smartcards and YubiKey,
- Flexibility in the choice of integration interface for applications,
- Configuration of customized flows through group policy object (GPO),
- Unique function supplement provides Citrix users with swift Single Sign-On and smartcard roaming,
- Accessible in thin clients from Dell, Igel, Fujitsu, 10ZIG, etc.

Product specification

Net iD Enterprise integrates the use of certificates on smartcards or YubiKey in existing IT platforms. The software opens up great opportunities to simplify the following for users:

Single Sign-On (SSO)
By inserting the smartcard into the card reader and entering their PIN code once, users have access to all systems, applications, and websites they are authorized to use. This means that users no longer have to keep track of different passwords for each system and can use a single PIN code rather than ten passwords.

For Single Sign-On with a certificate to function appropriately, the target system must support certificate-based login. Single Sign-On can also be introduced for older applications that only support username and password combination through supplementation with an SSO platform, for example, Imprivata.

Card Insert and Remove actions
Card Watch is a function that automatically initiates the desired action when users insert or remove their cards from the card reader. For example, correct shutdown, or launch of an underlying program. When the card is removed from the card reader, a dialog window can be displayed on the screen, asking what the user wants to do. For example log out, shut down or lock the computer.

Fast User Switching
Users who share computers that run on Windows can use their smartcards to switch users quickly and simply while maintaining the desired level of security on local workstations.

Workstation Lockdown
When workstations are located in public settings, Workstation Lockdown makes sure that non-authorized users cannot access the computer environment. After shutdown, the computer is completely locked, and keyboard commands are totally ignored until an authorized card is inserted into the card reader and the user enters the PIN code.

Credential Provider
Users often have multiple certificates on their smartcards. Net iD Enterprise contains functions that make it simple to select the right certificate. Credential Provider, Certificate Provider, and PIN Provider are examples of functions that, with visual and automated resources, make it easy for users to select the right certificate on the basis of the application.

Central configuration through group policy
Central management of configurations via Group Policy is enabled by the system allowing configurations of Net iD Enterprise to be entered in the registry (Windows registry). This makes it easy to create bespoke configurations and to change these for user groups with different needs. For example, different groups may need Single Sign-On functionality, or different responses when they insert or remove their cards from the card reader.

Flexible support for smartcards
Net iD Enterprise supports the most usual smartcards on the market. In partnership with card suppliers, we add support for new types of cards on an ongoing basis. The flexible architecture of Net iD Enterprise makes it easy to add support for new smartcards.

Virtual smartcards
Net iD Enterprise can also be used for login with virtual smartcards stored in Microsoft TPM or Intel Authenticate.

Net iD Customized Packaging
A customized configuration of Net iD Enterprise accommodates specific wishes and requirements, based on the organization and target environment. User interface, graphic design, texts, and information flows are examples of variables that can be adjusted to match your wishes and requirements exactly. This will simplify the roll-out and administration of the software and eliminate support-intensive processes. For customers with support agreements, we also take responsibility for configuration choices over time, in other words for updating parameters that may have been changed in new versions of Net iD Enterprise.

General Minidriver versus Net iD Minidriver/ CSP
Generic smartcards are normally delivered directly from the card supplier with a Minidriver, which, in combination with Microsoft Base CSP, provides basic functionality for smartcard login. Net iD Enterprise contains an advanced CSP (Certificate Service Provider) and an expanded Minidriver which supports most smartcards on the market, over and above the basic functionality. In addition, it supports more functions and more advanced functions, such as Single Sign-On, hot seating, fast user switching, and advanced options for bespoke configuration. As such, Net iD Enterprise provides more support and increased flexibility for IT staff and users.

Additional options

The client software Net iD Enterprise is the most commonly used PKI middleware on the market for establishing strong Multifactor Authentication (MFA) based on certificates and PKI. Net iD Enterprise integrates smartcards and other certificate carriers with all types of applications and IT environments. In most cases, the standard packages of the software can be used without any adjustments. With our large toolbox of configurable parameters, you can optimally streamline the user experience for both users and IT administrators. Being able to adjust even small details is crucial, for example, when logging in to applications with unorthodox PKI implementations.

For technicians involved in the configuration, packaging, installation, and support of software in the IT infrastructure, see Net iD Enterprise Technical Description.

Examples of additional options with Net iD Enterprise

- Central handling of PIN policy makes it possible to apply requirements to PIN code content and to replace PIN codes,
- Unlock Card. Unlocking locked cards before login,
- MIFARE info. Reading and writing information to MIFARE (wireless technology),
- Simple adaptation of texts and links in the interface. For instance, this is for support and help pages,
- Web admin. Built-in browser for communication with Net iD Portal. Sidesteps issues with plug-in support and makes the solution browser-independent,
- Tracker. Central logging of incidents with regard to successful or failed logins,
- Reset Card. Resetting smartcards,
- Signature and encryption of files and emails with certificates,
- Trace service. Flexible activation and tracking as assistance in troubleshooting.

Net iD Enterprise Developers Guide

Provides additional insight into all the opportunities that exist for streamlining the user experience.

Net iD Portal

Net iD Portal is the new generation web portal for fully governed life cycle management of digital identities. The portal handles everything you need to introduce strong authentication (Multifactor Authentication, MFA) in your organization. It handles smartcards, virtual smartcards, YubiKey, mobile apps, and different function certificates such as web server certificates.

How it works

Net iD Portal links together the organizations' underlying infrastructure. This implies certificate service, catalog service and database of certificates issued in a web-based, platform-independent interface. On the basis of a central person entry, Net iD Portal is able to process and maintain an overview of all employee's digital identities. Smartcard, YubiKey, file-based certificate, certificate allocated to the Net iD Access app, and machine certificates of various types.

You can integrate the standard version yourself, or order a bespoke solution for your organization. We carry out the work in the form of a project involving one of our integration partners. This is normally the system partner you already use for your IT operation.

Signing a support agreement ensures access to professional support that covers all the Net iD products you use.

Benefits of Net iD Portal

- Complete life cycle management of smartcards, certificates, and users via a web portal,
- Interface for administrators, operators, and users,
- Self-service for certificate users,
- Activation, unlocking, renewal, and blocking of certificates,
- Adaptable dissemination flow using XML configuration,
- API for integration with third-party systems,
- Expanded tracking and logging function,
- Simple and straightforward user interface.

Product specification

In its standard version, Net iD Portal can provide many organizations with a complete solution for the administration of certificates for smartcards, smartphones, YubiKey, and different function certificates such as web server certificates.

For users
Activation of own cards and allocation of user certificates

Replacement of security codes for cards

Unlocking security codes for cards

Use of temporary authorization to administrate colleagues' cards

Activation and issuing of mobile certificate for Net iD Access.

For operators
Issuing, blocking, and renewal of certificates for various carriers such as smartcards, YubiKey, smartphones and function certificates.

Standard version or company-specific workflows

Administration and overview through log function and reports

Remote unlocking of users' cards thorough challenge-response

Regeneration of users' cards

For administrators
Configuration of Net iD Portal

Processing of certificate templates

Processing of policy for security codes (PIN)

Processing of administrator groups

Uploading lists from card suppliers containing information about cards supplied

Interface for audit logs and reports concerning, for example, card users, operators, smartcards and certificates allocated or blocked.

Appreciable flexibility to manage and restrict authorizations for operators. Opportunity to delegate temporary authorization to stand-in operators according to a schedule.

General
Support for smartcards and card profiles from the most common card suppliers

Encryption of sensitive information in the application database

Logging of all incidents that result in changes

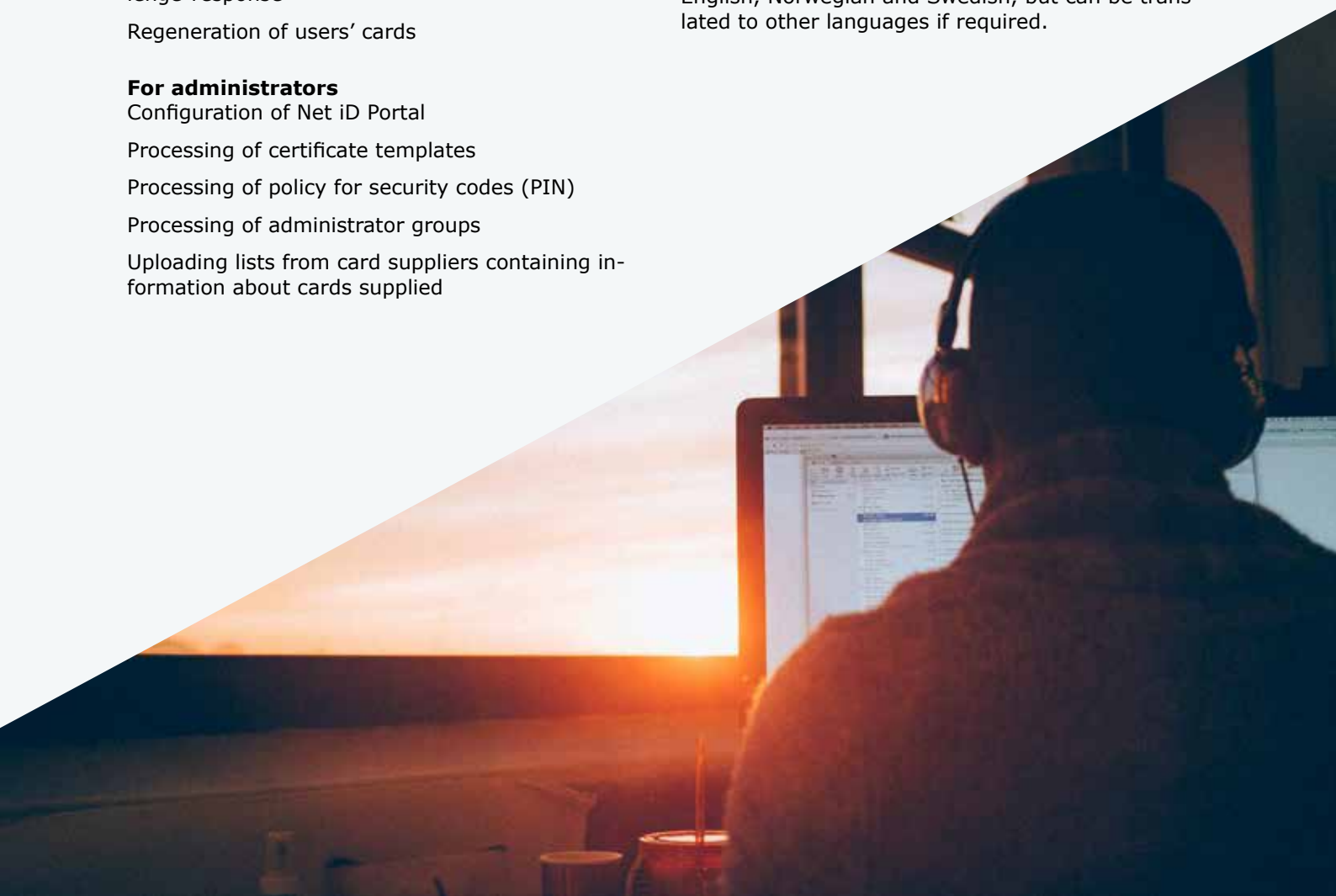
Built-in intelligence that senses which work assignment an operator wishes to perform

Adaptations
Adaptation of graphic profile such as logo, background, text, etc.

XML-configuration. Add or remove functions you do not want to be available to users

Integration with third-party systems. Integration with Net iD Portal API. For example, automate creation of user-profiles and authorization sets, programmatically via Microsoft Identity Manager

Language adaptation. Available as standard in English, Norwegian and Swedish, but can be translated to other languages if required.



One card for everything

Just as important as improving information security with strong two-factor authentication (Multifactor Authentication) is the capacity to coordinate the processing of cards with other types of functionality. For example, there are many benefits to combining electronic entry and ID cards with secure login in one and the same card. In particular, it improves security because the card becomes extremely valuable to the user, reducing the risk of him/her forgetting to remove it from the computer card reader. Adding follow-me print functionality to the card increases security and flexibility with regard to printing on shared printers. In addition, the solution saves costs through having to issue fewer cards, and by ensuring more efficient processing of the cards.

Smooth introduction of the multi-factor authentication

Pointsharp has long and broad experience in helping large organisations introduce security procedures based on smartcards and Multi-factor Authentication (MFA). We are skilled at composing holistic solutions for:

- How to use the same card for logging in and entering buildings – and even as a physical ID card
- How to apply a carefully considered policy regarding cards and security
- How to add in new services subsequently – we cover all needs for secure login, including those based on smartphones and YubiKey
- How to establish a carefully considered administration and allocation process
- How to introduce effective support routines and reduce support-intensive factors
- Adapting smartcards to match the organisation's graphic identity
- And much more besides

Net iD Access

Net iD Access provides full PKI-based Multi-factor Authentication for mission-critical information and applications on all types of clients. As it supports iOS and Android, the user can be sure of maintaining security levels on smartphones and tablets as well. Provide security for the users by issuing file certificates or a smartcard used in an external card reader. Net iD Access functions just as well with web applications as with mobile apps.

Benefits of Net iD Access

This is a versatile solution that enables a user to use modern communication tools that facilitate the work and open the door to a mobile way of working. In addition, to support for authentication with smartcard- or file-based e-identities, the solution also includes signature functions. A range of predefined integrations ensures that Net iD Access does the job in precisely the IT environment used.

A user can also use YubiKey Lightning with the built-in Net iD Access App for swift and secure access to the services via your iPhone or Android device. YubiKey Lightning expands user benefit because it supports a variety of protocols and services over and above PKI.

More benefits with Net iD Access

- Access to mission-critical information wherever the user may be,
- Integrates with existing PKI infrastructure
- Handles client apps' requirements for integration with card readers, cards, keys, and certificates,
- Free download for iOS, Android,
- Also available for Windows, macOS, Linux, and Chrome OS,
- Permits ID exchange,
- Multiple predefined integrations with IdP, journal systems, Office 365, etc,
- Unique support for secure Citrix login.

Product specification

Smartcard, YubiKey or file-based certificate
Net iD Access supports all common smartcards on the market, as well as YubiKey. If the user does want to use smartcards, Net iD Portal makes it simple to set up an allocation flow adapted to meet the organization's needs, based on YubiKeys, and or even together with file-based certificates.

ID-exchange (derived credentials)
Net iD Access combined with Net iD Portal makes it possible to switch ID from existing smartcards to YubiKey, or to a protected area for keys and certificates within the actual Net iD Access app on mobile devices with iOS or Android operating systems.

Ready-to-use integrations
A variety of identity providers (IdP) including PhenixID, Swedish e-identity, Mobilityguard, and Curity already support Net iD Access in their products. The support can be used for login or signature in both apps and web applications such as Treserva, Cosmic Nova, SwipeCare and Phoniro Care. With an MFA adapter for Net iD Access, the user can also set up a login to a range of ADFS-integrated (Active Directory Federation Services) applications. Contact us for additional information.

Secure Citrix login
Fast and secure authentication with a PIN code for Citrix ADC (formerly NetScaler) and StoreFront for connection to both Citrix XenApp and XenDesktop.

Net iD Access Server
Our server component handles all communication with the calling identity providers and/or applications, as well as the validation information of the underlying PKI infrastructure (via Windows' built-in functions for OSCP and CRL), if desired. This is where systems define which services Net iD Access is to be used for, and which certificate issuers are approved for access to the services. Net iD Access Server is installed as a web service under Microsoft Internet Information Server, IIS. The configuration is handled through a standard XML file.

Interface between Net iD Access and the connected service
In order to guarantee the integrity of the exchange of information between the Net iD Access apps and the Net iD Access Server, communication is run via TLS supplemented with an additional layer of encryption. For traffic between the IdP- or application server and Net iD Access Server, two-way TLS can be activated if desired.

Net iD Access Client
Apps and applications for iOS, Android, Microsoft Windows 7/8/10, macOS, and Linux.

Net iD Access Server
Microsoft Windows Server 2012 R2, 2016 and 2019.Microsoft SQL Server 2012, 2014, 2016, and 2017.

Interface
Web service for calls from the service supplier's server (IdP). Calls for app exchange via URL form.

Internal web service for communication with the Net iD Access applications.

Hardware support via PC/SC (card reader and smartcard)

Standards
TLS for all communication, digital signatures in accordance with PKSC#7 and RAW.

Card readers
iOS, Identos Tactivo for iPhone and iPad.

Android, Identos Tactivo.

Windows, macOS, Linux. Reader compatible with the PC/SC standard.

Support for other card readers for mobile devices is assessed and added on an ongoing basis.

Smartcards
Support for cards formatted according to the PIV, PKCS#15 1.1 and ISO7816-15 standards. In addition, support for the PKI section in YubiKey. Flexible architecture makes it possible to add support for new smartcards as required.

Browser
Browser-independent functions with all browsers.

Languages
English, Finnish, Norwegian, and Swedish

Licensing
Licensing of Net iD Access is dealt with in Net iD Access Server, based on the number of unique users. Standard versions of the client applications for different platforms are included in the price of the license.

How it works

Net iD Access offers a holistic solution for mobile security, featuring a server component and a cost-free application for the client side. The solution provides full Multifactor Authentication (MFA) for the apps, without the need for advanced PKI development. The user decides for himself whether wishing to deal with validation and access authorization in the Net iD Access server, or on the server-side in your services. When users want to log into a service, they simply enter their user ID in the service application, which forwards it to the services server-side. The server then sends a login request for the user to the Net iD Access Server using a simple web service call. At the same time, the user is switched over to the application.

The actual login with the card, YubiKey or the file-based e-identity is run against the Net iD Access Server. The Net iD Access Server verifies the user and reports "all clear" to the server-side of the service.The user is automatically switched back to the service application and can then access the desired service. Net iD Access separates the information channel from the "security channel". This is also known as "out-of-band authentication".

It allows a variety of different use cases, and the one to be used is defined through configuration for each service. For example, login can be initiated in an application on one device, while authentication takes place on a completely different one. In another scenario, access to critical services can be limited so that they are only accessible from the unit where the card is inserted.

For the function for switching between Net iD Access and the browser or service app to operate, a specific call must be implemented in the web pages or service app.

For more detailed information or to order an evaluation licence

sales@pointsharp.com

POINTSHARP