



Net iD with Intel® Authenticate

Strong authentication of clients and users



Identity theft is a globally growing problem and today a daily issue for individuals and businesses. Secure, easy-to-use solutions are necessary to prevent hackers from gaining access to usernames and passwords.

Strong individual-based authentication is crucial to prevent hackers from accessing usernames and passwords. Intel® Authenticate solution based on Intel® identity protection technology deepens the security of the client.

With Net iD and certificates you can also identify the user behind the client. Easy managed through the Net iD Portal lifecycle management consol. Through the collaboration, the user gets a simple everyday life, better security and increased productivity.

SecMaker's Net iD is expanding to hardware protection features and multifactor authentication capabilities with Intel® Authenticate Solution

Benefits

- Hardware-enhanced security features help protect certificates, using Intel® Authenticate Solution.
- Enables logon using combinations of PIN, fingerprint, facial recognition, logical location or Bluetooth phone proximity.
- Net iD Portal issues certificates to the processor to be used by any of the logon methods.
- Desktop and laptop clients available now from a large number of vendors supporting Intel® Authenticate Solution.

The importance in today's connected world of having a robust authentication solution to access IT systems and business applications continues to grow.

The traditional method for authentication has typically been to apply a username and password. However, passwords have proven to be a weak method of authentication. The starting point for many security breaches is a compromised logon credential that allows hackers to gain access.

As IT systems have become harder themselves to penetrate, the hackers have sought out softer targets such as human fallibility and the use of passwords.

Adopting bad habits such as not changing passwords, or making them complex enough, re-using or even sharing them with others, creates vulnerabilities that can be exploited.

Authentication solutions that make it possible to apply secure and reliable login technologies that store, control and manage credentials, have become critically important.

User credentials and devices are less susceptible to tampering when hardware, software, and firmware form an integrated security solution. By combining Intel® Authenticate Solution with Net iD from SecMaker, you get a comprehensive multifactor authentication solution that is user-friendly and customizable.

Authentication factors are “hardened” and better protected in the hardware of the Intel® vPro™ platform. This protection makes it more difficult for malware and attackers to access or tamper with sensitive authentication data. Users can be better secured with smart card or with Intel® Authenticate Technology acting as a virtual smart card. Users, certificates, and authentication methods can then all easily be managed with Net iD Portal.

A flexible combination

Intel® Authenticate Solution in combination with Net iD makes multifactor authentication easier to deploy and manage by making it possible for IT departments to customize login factors in several ways, now including:

- **Something you know** (such as a PIN)
- **Something you have** (such as a mobile phone)
- **Something you are** (such as a fingerprint)
- **Someplace you are** (location-based identification)

Virtual smart cards can be used as an add-on to the existing smart card solution, or in environments where the use of physical smart cards is not recommended.

Virtual smart cards and additional factors from OEMs and hardware partners give you even more choice to protect the latest Intel® Core™ vPro™ processor-based computers.

Solution overview

SecMaker’s Net iD Portal is an application that simplifies the lifecycle management of smart cards, devices, certificates, and an organization’s end users. The management portal interconnects the certificate service, catalogue and data-base services in an organization’s IT infrastructure.

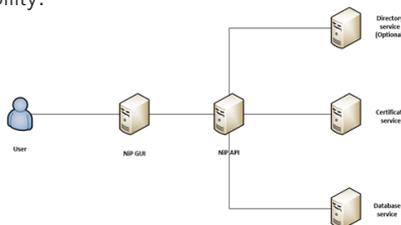
It’s easy using the Net iD Portal to create lifecycle workflows for enrollment, revocation, and the renewal of certificates. It is possible to enroll a smart card or a virtual smart card protected by the Intel® vPro platform hardware, and adopt any of the authentication factor combinations available with the Intel® Authenticate Solution.

“Give users access to advanced and high security without making it more difficult for the user.”

The Net iD Portal has a web GUI that permits users to access different features that they are authorized to use. As an example, the Net iD Portal GUI can permit a user to manage end user tokens and certificates for authentication towards hardware, active directory, VDI applications, web pages, Office 365 and other cloud based system platforms. It can also be used for digital signing and encryption of e-mail and documents.

The architecture of Net iD Portal consists of an API and GUI. The Net iD Portal GUI interacts with the Net iD Portal API and becomes a web portal that can be used with a web browser.

Below is a reference design for installing the Net iD Portal in your environment. Net iD Portal can be installed in different server architectures depending on the demands for high availability.



Net iD by SecMaker

The Net iD product family is based on the Net iD Enterprise client software and Net iD web portal for lifecycle administration, with additional security products for mobility, integration and certificate handling.

Net iD products are based on open standards making our solutions simple to launch and administer regardless of system environment.

Net iD is appreciated by security and IT managers alike for features that provide high security, flexibility, and cost-effectiveness. End users of Net iD solutions appreciate it because it supports mobile operations, is easy to use and offers simple and more secure workflows.

Where to get more information

Learn more at:

netid.secmaker.com and www.intel.com



Disclaimers & Legal Notices

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure.

Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Intel, the

Intel logo, Intel vPro, and Intel Core are trademarks of Intel Corporation in the U.S. and/or other countries.

© Intel Corporation

About SecMaker

As a trusted leader in IT security, SecMaker strive to preserve our independent role and collaborate with many of the leading system platforms, hardware and smart card providers. In this way, we ensure that integration with your IT environment works well.

SecMaker has chosen to take an active role in international standardization work around IT security based on certificates and PKI. In this way, we have become a driving force in the future of PKI and certificate-based security solutions.

SecMaker has established a partner program for technology, cloud and integration partners. As knowledge leaders, we gladly share our expertise and experience with our business partners and customers.

