Hardware-based user authentication made simple

Intel® and Intercede® collaborate to enable passwords to be replaced with hardware-protected digital identities, increasing security and convenience.

All enterprises need to ensure that only trusted users can access their systems and networks. To achieve this they want a modern authentication mechanism that is highly secure, easy to use and simple to deploy.

Intercede's MyID®, together with Intel® Authenticate, is a credential management solution that makes the issuance and management of Intel® Authenticate hardware-protected digital identities simple and scalable.

It eliminates the continuing reliance on insecure passwords that do not provide adequate security and are inconvenient for end users and system administrators. It also removes the need for high-cost physical tokens, such as smart cards, that enhance security but have an adverse operational and cost impact on the business.

MyID works with Intel® Authenticate to enable passwords to be replaced with a simple PIN and a hardware protected digital identity. It increases security and provides more convenience for the user.

Hardware-protected identity **Simple to deploy** **Easy to use**

What's the problem to be solved?

Data breaches have dominated headlines recently. Whether it's nation-state spies intent on stealing information, cyber pranksters and hacktivists looking for attention, or cybercriminals out to make a buck, there are plenty of adversaries intent on breaking into networks and databases and carrying away whatever pieces of information they can grab.

The hacking of weak and stolen credentials (e.g. passwords) remains the single biggest cause of attacks. For years experts have warned about the risks of relying on weak credentials to restrict who has access to the data, and this is still a big problem. Passwords are insecure: they get reused, leaked, guessed, and are subject to attacks such as key loggers, phishing and dictionary-based brute-force. They are also inconvenient, as they are forgotten, need resetting and need changing, which wastes users' time and cost businesses money.

How to step-up cybersecurity without getting in the way of day-to-day business has become a key business priority, and reaches all the way to the Boardroom. The challenge is to replace passwords with something that is more secure, more convenient and available at a reasonable cost.

How it works

Intel® and Intercede provide an innovative solution to the challenges of user authentication. We work together to provide your organization with the highest levels of security, while providing your users with the simplest way of connecting to your information and systems.

Intel® Authenticate is a hardware-enhanced, multifactor authentication solution that strengthens identity protection on the PC, making it less vulnerable to identity and security credential attacks. It is a feature of 6th Generation Intel® Core vProTM which uses a FIPS 140-2 Validated Cryptographic Module[1] to perform cryptographic functions inside the hardware-based Converge Security and Manageability Engine (CSME) outside of the operating system.

Intel® Authenticate verifies identities by using a combination of up to three hardened factors at the same time: "something you know," such as a personal identification number; "something you have," including a mobile phone; and "something you are," like a fingerprint. IT can choose from multiple hardened factors of authentication that are based on company policies, and no longer has to rely solely on employees remembering complicated passwords.

By combining 'something I have' (a unique hardware protected digital identity) with 'something I know' (a simple PIN) organizations can step-up to two-factor authentication. This significantly increases the level of security and effectively protects against many of the most common threats such as password reuse and phishing.

An additional benefit of Intel® Authenticate is the availability of a Protected Transaction Display (PTD), which provides a secure entry screen for the user's PIN. As it is isolated from the main operating system at a hardware level, the PTD effectively protects against malware attempting to gain knowledge of a user's PIN (e.g. from key loggers).

For hardware protected digital identities to be useful to a business they must meet the primary use case, which is Windows logon.

Intercede provides two components that are embedded into Intel® Authenticate:

- The MyID Minidriver for Intel® Authenticate, which makes chip-protected digital identities accessible to applications via a standard interface
- The MyID Virtual Reader for Intel® Authenticate, which (via the Minidriver) makes chip-protected digital identities available for Windows logon

Digital identities can only be trusted if you can be sure of the system that issued them. Hardware-protected digital identities are no exception. Simply using a hardware chip to protect an identity does not increase security if an organization cannot be sure it was issued to the right person. This is where MyID comes in.

MyID is a secure and scalable credential management system that provides organizations with the ability to issue and manage Intel® Authenticate credentials across the enterprise.

- **Increase security**
  Step up your security by replacing insecure passwords with highly secure hardware-protected digital identities.
- **Make it easier**
  Provide easy to use interfaces for system administrators and operators. Make it more convenient for users by replacing complex, changing passwords with a simple PIN.
- **Manage the credential lifecycle**
  Clear workflows ensure the credential lifecycle is managed; from being issued, updated, replaced, renewed to eventually being revoked.
- **Avoid disruption**
  Integrate seamlessly with your existing in-house systems and business processes. Use with your current directories, certificate services, identity management solutions and existing infrastructure.
- **Quickly deploy at scale**
  MyID makes Intel® Authenticate deployable at scale across all of your enterprise. It's already used by many of the World's largest and most security conscious organizations.
- **Save money**
  Reduce costs by using the hardware you already have built into your machines (No need for a separate smart card!). Reduce operational overhead by providing a self-service model for updating, replacing or renewing credentials, using simple guided processes.

[1] For FIPS 140-2 Compliance, 6th Generation Core vProTM systems require a chipset firmware greater than 11.6.x.x.