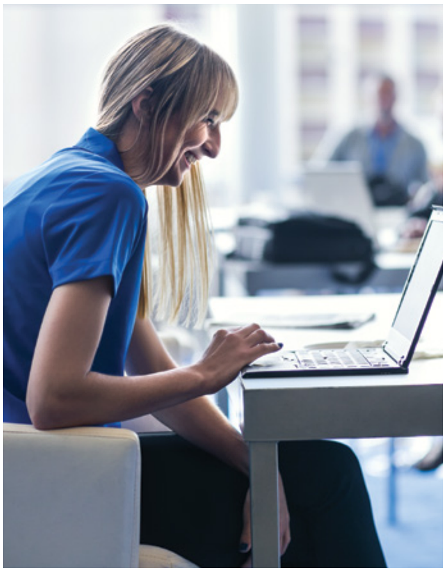
SOLUTION BRIEF

Business Client
Client Security & Manageability

Enable more secure business growth with multi-factor authentication

Help protect user identities from cyberattack while streamlining operations and reducing costs



Author
Emily Ryan

Enterprise Solution Architect,
Influencer Sales Group,
Intel Corporation

Executive Summary

Today's cybercriminals are a wily and determined breed. Their modes of attack are complex and their opportunities are increasing as the volume of data and number of devices accessing this data in a typical organization grow.

Traditional software-only methods of protecting identities – such as username and password – are too easily overcome by these cybercriminals. IT teams are challenged to introduce additional layers of identity protection to a business user community that often sees security as a barrier to innovation and productivity.

Intel® Authenticate Technology provides enterprises with a convenient and efficient way to manage policy-driven, hardware-based multi-factor authentication (MFA) for identity and access management. It moves multi-factor authentication data into the hardware and so helps reduce software-only vulnerabilities. It is designed to help IT turn security into a business enabler while combatting the risk posed by cybercrime.

Cyber threats and big data growth put pressure on IT security

According to a 2015 Verizon* Report, over half[1] of data breaches are due to lost credentials, and identity-based attacks are now a significant threat across industries. In addition to the data loss itself and its legal, reputational and commercial implications, the costs associated with these breaches can be huge.

Not only has the incidence of such serious breaches been increasing[2], but the attacks themselves are also becoming more sophisticated, with techniques including phishing, password cracking and screen scraping. The proliferation of devices and online or cloud-based tools and applications also means that users are required to manage more and more identities. This drives them to reuse passwords across multiple platforms and applications, not only in their enterprise environment, but across their personal lives as well. All this creates more potential attack surfaces, while behind the scenes the ongoing growth of big data means the pool of information vulnerable to attack is also steadily getting bigger.

While everyone recognizes that protecting valuable corporate data, intellectual property, and customer and employee details is crucial, many enterprises still rely on a software-only username-and-password approach that is no longer sufficient. Business users struggle to remember and properly use multiple passwords and tend to view security as a hurdle to be overcome in order to carry out their work. Some tools designed to address this issue – such as tokens and smart cards – can end up adding to the complexity for both users and IT as they can be easily lost or stolen and difficult to maintain. For a workforce that is focused on driving agility and innovation in today's digital economy, the burden of security can significantly impact productivity, efficiency and employee satisfaction.

Some business stakeholders fear that the administrative headache traditionally associated with IT security will be made worse by initiatives that create more data. This can make them wary of implementing the digital transformation projects that will empower their company to succeed in today's economy. This tension between the desire to transform and the distaste for incurring additional security burdens means business-enabling cloud and big data projects may slip down the enterprise's to-do list, leaving it fighting to keep up with more innovative competitors.

However, security does not need to be a business inhibitor. With the right tools in place – such as hardened multi-factor authentication – it can help employees work more effectively and become an enabler to keep the organization moving rapidly, safely and conveniently.

Addressing user experience and manageability with hardened multi-factor authentication

Once a threat, such as a virus or Trojan attack, has infiltrated an environment or device, it can take up permanent residence in the memory and layers of the operating system. The speed at which these threats are developed and evolve is often faster than most businesses can keep up with, especially those with older device fleets or traditional security software alone. With identity theft one of the core elements of the hacker's toolkit, IT is challenged to find a way to ensure cost-effective authentication at the endpoint device while still keeping workers mobile and productive from wherever they are.

Intel Authenticate Technology on the 6th generation Intel® Core™ vPro™ processor is a multi-factor authentication solution that strengthens identity protection for the enterprise. It hardens factors in the firmware. By moving the multi-factor authentication data and functions into the hardware below the operating system, the solution reduces software-only vulnerabilities. This hardening inhibits corporate or workforce identity credential exposure, theft and misuse, as well as safeguarding authentication processes and policies from interception, override and replay attacks. It consolidates authentication, implementation, management and enforcement under one umbrella and lets the IT team move security beyond usernames and passwords with multiple hardened factors to verify identities. These include:

- Something the user knows, such as a personal identification number (PIN)
- Something the user has, such as a mobile phone
- Something the user is, such as a fingerprint

The more factors used, the better the assurance of identity, especially when those factors are specific to the user. The information collected is encrypted at the hardware level, meaning it remains resistant to theft and misuse by unknown or unauthorized individuals. If the user's password is stolen, the requirement for a fingerprint and/or PIN mean a malicious actor is much less likely to succeed in gaining access.

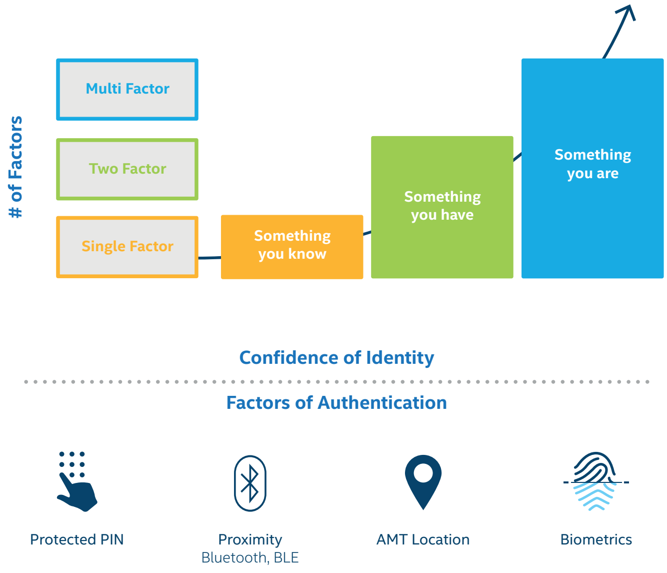


Figure 1. The elements of multi-factor authentication

Transforming the user experience

The solution supports three key use cases for enterprise identity management:

- **Access to Device:** Policy-defined access to the device, operating system and local data
- **Access to Network:** Policy-defined access to the domain, virtual private network (VPN), servers, cloud applications and other network assets
- **User Presence Detection:** Matching user to approved system, locking the system if the user walks away, requiring additional factor(s) to unlock the system; providing continuous user presence verification for inactivity monitoring

From a user's perspective, the multi-factor approach of the Intel Authenticate Solution creates a smoother and less disruptive experience, with intuitive and flexible sign-on. By combining factors such as protected PIN, proximity, location and biometrics, the login process no longer acts as a barrier to productivity, instead giving the employee an uninterrupted workflow that supports productivity. Without having to stop and enter a different username and password each time they move to a new application or tool, the employee can stay focused on the job and no longer needs to worry about remembering a complex password that meets strict password restrictions.

Improving control and manageability

Meanwhile, the enterprise needs to keep down costs for managing identities and factors. The Intel Authenticate solution is part of the 6th generation Intel Core i5 and i7 processors and Intel Core vPro processor. This means it enables remote device management while also integrating with existing management consoles within the organization. In this way it provides a standard method of setting and managing identity policies across all devices and user identities. Managing multiple authentication factors can be done easily and from familiar policy management console tools, by setting policies for different scenarios and user types, specifying the appropriate access, people and materials for each.

Reducing risk while driving business performance

Intel Authenticate Technology enables flexible policy configuration and enforcement using familiar PC management features and centralized tools. Policy administration, application distribution, and related fleet management can all operate in line with your usual business processes.

The solution's MFA model allows greater business agility, free of passwords and security barriers. It provides more robust protection for identity and access management than software-only approaches, while enabling a more efficient and seamless user experience. It provides line of business users with strong security that helps protects them and the organization against risk without slowing them down, enabling the business to move with velocity and preparing it to take full advantage of the potential of digital transformation and innovation.

In addition to offering value to business users, Intel Authenticate Technology can help IT to streamline processes, achieve greater confidence in the organization's identity protection and assurance measures, and reduce costs. For example, one of the main drivers of IT helpdesk costs is dealing with forgotten passwords. By implementing additional authentication layers (such as a PIN, smart phone or fingerprint), you can eliminate the need for passwords, helping the helpdesk team focus their valuable resource on more complex or business-critical issues.

The solution's features are designed to deliver tangible value to both the business and IT:

- Hardened authentication factors rooted in firmware and hardware address the current vulnerabilities of software-only authentication methods
- Flexible and secure IT policy administration create a robust solution that is easy on IT
- A hardened MFA decision point delivers trusted authentication
- Embedded credentials mean there are no external tokens to buy or lose, helping drive cost savings
- Security-enabled device pairing creates a 'ready when you are' security model for employees, whether they are accessing the system, network, applications or websites
- An extensible architecture means the solution easily integrates with existing tools and consoles, and helps ensure that it can be easily deployed and scaled
- Designed as a horizontal capability, the Intel Authenticate Solution is available to ISVs and OEMs, enabling the creation of customizable solutions

Solution architecture: Multi-factor authentication

Intel Authenticate Technology captures, encrypts, matches and stores PINs, biometrics, keys, tokens and associated certificates in the hardware, out of sight and reach from typical attack methods. The flexible and hardened multi-factor solution enables IT to help protect employees' identities and prevent loss of sensitive data while providing an enhanced user experience. The solution provides the capability to harden the factors, policies and decision points in the hardware, which removes the vulnerability normally found in operating system-based solutions.

The solution consists of the components to allow IT to tailor policies with appropriate combinations of hardened identity factors, based on what works best for your business. To implement it within your environment, you will need:

- The 6th generation Intel Core vPro platform or other Intel Core processor-powered platform, which includes additional security and scalability capabilities for the best Intel Authenticate Solution implementation
- Intel Authenticate client-side software for enrollment and configuration
- A management console with a console server plug-in to set authentication and factor policies, such as:
  - o Microsoft Active Directory and Group Policy*
  - o Microsoft System Center Configuration Manager*
  - o McAfee® ePolicy Orchestrator
- An iOS* or Android* phone with proximity device software for proximity use cases (available from Apple Store* and Google Play*)

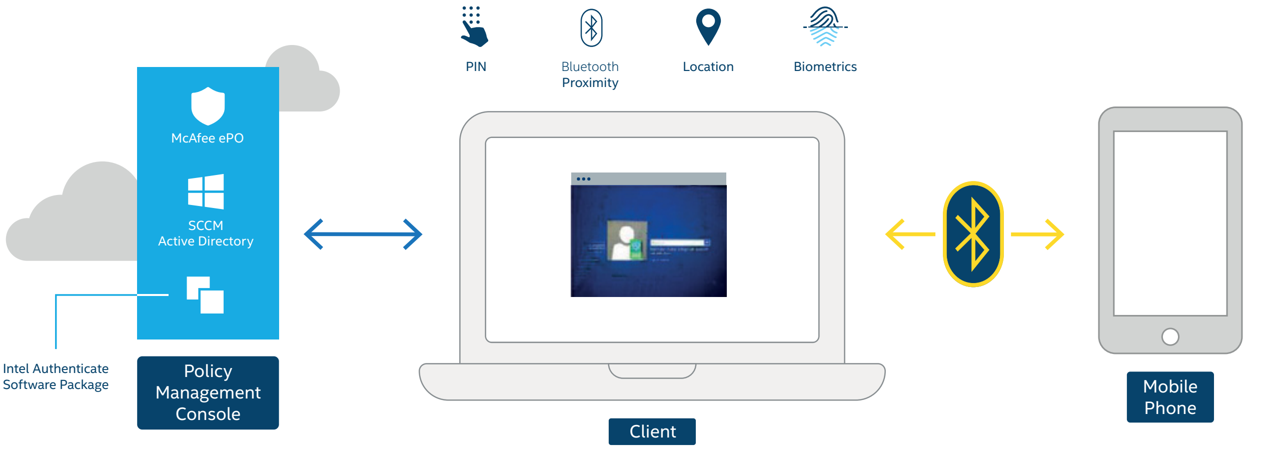


Figure 2. The Intel® Authenticate Solution Architecture

Multi-factor Authentication – Business and IT Value

The Intel® Authenticate Solution Architecture delivers:

- Hardware- and firmware-based authentication methods that resolve vulnerabilities associated with current software-based approaches
- Flexible and more secure IT policy administration
- A hardened MFA decision point that ensures trusted authentication
- Embedded credentials that eliminate the need for external tokens to buy or lose, driving cost savings
- Security-enabled device pairing that creates a 'ready when you are' security model for employees
- An extensible architecture that allows smooth integration with existing tools and consoles

Conclusion

Securing employee identities should be a priority for all organizations, but traditional methods are no longer robust enough to stand up to the sophisticated techniques of today's cyber criminals. Those that wish to flourish in today's fast-changing world of digital transformation and constant innovation need a solution that will enable, not inhibit, the business.

By implementing Intel Authenticate Technology, you will empower your IT team with hardware-enhanced protection of identity information and processing, and policy-driven, enterprise-level identity validation. This will in turn help reduce costs, improve the user experience and reduce your threat surfaces.

Solutions Tested by Your Peers

This document provides a starting point for the development of a multi-factor authentication solution. Solution architects and technology experts for this reference architecture are listed on the first page.

Find the solution that's right for your organization. Contact your Intel representative, register at Intel IT Center, or visit http://www.intel.com/authenticate

[1] 2015 Data Breach Investigations Report, Verizon. http://www.verizonenterprise.com/DBIR/2015/

[2] ITRC Breach Statistics 2005 – 2015, http://www.idtheftcenter.org/images/breach/2005to2015multiyear.pdf

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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. Check with your system manufacturer or retailer, or learn more at <most relevant URL to the product>.

2016/0716/JNW/CAT/PDF 334651-001