IDENTIV SOLUTIONS BRIEF

Multi-Factor Authentication Solutions

Working with Identiv, organizations remain trusted and deliver outstanding employee and customer experiences without worrying about cybersecurity issues.

What Is Multi-Factor Authentication?

Multi-factor authentication (MFA) necessitates the user to provide two or more verification factors to gain access to a resource such as an application, an online account, or a virtual private network (VPN). It is a core component of a strong identity and access management policy.

Why Do You Need Multi-Factor Authentication?

Instead of simply asking for a username and password, MFA requires additional verification factors, reducing the probability of a cyberattack.

Additional benefits include:

Protecting Against Data Breaches

The biggest reason you need MFA is to keep your critical business information safe from potential data breaches.

According to the Verizon 2020 Data Breach Investigations Report (DBIR), around 45% of data breaches featured hacking, 70% of which were perpetrated by external actors.

If you only use a password to authenticate a user, it leaves an insecure vector for attack. If the password is weak or was exposed elsewhere, how do you know if it is actually the user signing in with the credentials and not an attacker?

By requiring a second form of authentication, you increase security; the additional factor is not easy for an attacker to obtain or duplicate.

Securing Your Digital Assets

MFA is one of the most cost-effective mechanisms enterprises can deploy to protect digital assets. In a world where credential harvesting attacks are on the rise, better authentication is moving from a nice-to-have to an absolutely essential technology.

Although a strong password is vital for cybersecurity, it is just one piece of the puzzle. By turning on multi-factor authentication for all accounts, you can ensure your password always has backup to keep you secure.

Avoiding Stolen Credentials

Passwords are perhaps the most common way to authenticate your online identity, but they provide very little protection. Once a password is stolen, hackers can use your credentials to log in to applications and business systems, bypass other access controls, and wreak serious havoc.

Deploying an MFA tool blunts the effect of excessive password reuse by requiring users to have something more than passwords to authenticate their identities. Multi-factor authentication methods, including FIDO security keys and smart cards/tokens, tighten security and keep out potential threats.

Giving Peace of Mind

Online accounts and services are, in many ways, inevitable offshoots of living in the modern world. They add convenience, enabling us to connect with friends on social media or shop at our favorite stores. The downside of having these accounts is giving cybercriminals more opportunities to steal your information.

To make things worse, if one of your accounts is compromised, the others are also vulnerable to attacks. For example, if a hacker accesses your social media, they can steal information that can be used to attack other accounts.

Multi-factor authentication gives you peace of mind; even if you become the victim of an attack, there is an added layer of security to protect you.

Staying Ahead of Changing Cyber Threats

Cyber threats are becoming more sophisticated. Cybercriminals now use sophisticated phishing and smishing techniques that fool even the most cyber-savvy person. To stay cyber-secure, you need every line of defense you can get.

By enabling multi-factor authentication, you ensure you stay one step ahead of these changing threats. Suppose you become the victim of a sophisticated phishing attack, and your password for a key account is stolen.

MFA protects you by requiring the cybercriminal who stole your password to have access to another device, such as your cell phone, or provide another piece of information to log in.

By adding multi-factor authentication to your arsenal, you have another means of defending yourself from cybercriminals who are becoming more adept at stealing information.

Multi-Factor Authentication Use Cases

Multi-factor authentication is one of the most effective ways for businesses to protect their systems and their customers' online accounts from hacking, spamming, data theft, and more.

Here are some common multi-factor authentication use cases in high-risk industries benefiting from incorporating MFA into their security protocols:

Finance

Financial institutions like banks are a top target for cyberattacks. Banks need to provide as much security as possible to protect customer data.

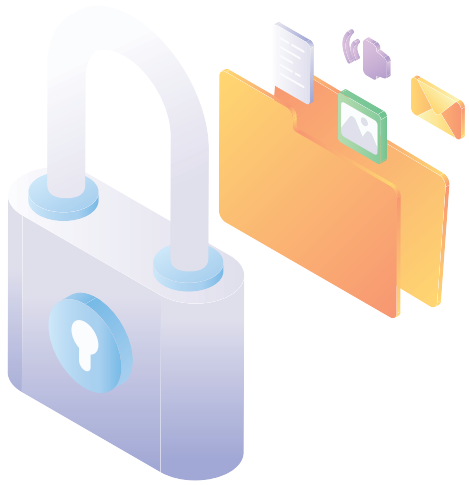
If a hacker gains access to someone's bank account, they can get a lot more than just money. They also have access to credit card information and social security numbers, leading to identity theft cases that can take years to resolve.

Any organization that processes and stores card payment data, including banks, must comply with Payment Card Industry Data Security Standard (PCI DSS). This industry standard strongly encourages at least two separate forms of authentication before a user can access their account.

Although multi-factor authentication is not yet required for PCI DSS compliance, finance organizations will benefit from following this industry-recognized best practice as early as possible.

Implementing MFA is the next step in building customer trust and loyalty, which banks need to maintain long-term relationships. It offers a high level of security without causing too much inconvenience to clients who have high expectations for data privacy from their financial institutions.

- **Use a FIDO key as a secure authentication factor and gain access to your cryptocurrency account via FIDO supported application**
- **Gain access to the building facility with a smart card and contactless reader**
- **Get secure access to the bank with a smart card identification badge**
- **Leverage smart card technology to get secure network access to financial information and private customer data**



Healthcare

With greater data access, the healthcare industry finds itself at an increased risk for data breaches. Healthcare portals are now a common way to send electronic records, creating more opportunities for hackers to infiltrate both patient and provider accounts. Medical records contain sensitive data that cannot be frozen or shut down like a stolen credit card number, making health providers a major target for hackers.

The Health Insurance Portability and Accountability Act (HIPAA) was originally created to protect individuals' health records. With the prevalence of technology in the healthcare industry, HIPAA compliance now requires strong authentication procedures. Health providers usually rely on login passwords alone to access healthcare systems, but with data breaches on the rise, it is no longer enough.

Data breaches often target healthcare employees' user credentials to gain access to a system, so internal multi-factor authentication should be a high priority for health providers. MFA is also an effective way to meet the HIPAA requirement for authorized access to electronically protected health information (ePHI).

- **Access PHI quickly and securely with a contactless smart card and contactless reader**
- **Use MFA to securely access a medical device after an x-ray or procedure where PHI is gathered on a device and reviewed/transferred for storage**

E-Commerce

While e-commerce sales continue to grow, fraud is growing nearly twice as quickly. Account takeover is the fastest-growing fraud threat for e-commerce companies, causing $5.1 billion in losses in 2017.

Although many online merchants are hesitant to implement multi-factor authentication for fear of deterring customers, the risk of being defrauded is becoming a greater threat for businesses.

Hackers do not need to be physically present to commit online fraud and e-commerce websites can be attacked on a large

scale. Online sales fraud, such as fake charges, is very costly for companies. It is the retailers who ultimately pay the price when they must issue refunds to scammed customers.

E-commerce fraud can be easily prevented by adding MFA to online accounts. Not only does this reassure customers their data is protected, it also deters hackers who prefer to target weaker websites. By decreasing the risk of fraud with multi-factor authentication, e-commerce companies can increase their bottom lines and build a reputation for protecting customer data.

- **Use FIDO security keys to secure Google Express or eBay shopping transactions to prevent account takeovers**

Government

Government employees are prime targets for cyberattacks because they have access to sensitive data, such as financial, economic, and military records. Hackers typically target government employees using phishing scams, posing as trusted sources to access login credentials.

One renowned MFA use case in government is the extensive requirement of two-factor authentication on many government websites to combat the threat of hackers.

The consequences of a cyberattack go beyond a compromised network. In just the past decade, we have seen high-profile data breaches that disrupted government services and affected millions of people whose private information was leaked. Multi-factor authentication guarantees only approved users can access government data, decreasing hackers' possibility of infiltrating a system.

- **Pair Common Access Card (CAC)/Personal Identity Verification (PIV) access with smart card readers, where the CAC/PIV card is the authenticator and the smart card reader is used in the authentication process**
- **Secure your Login.gov account with a FIDO security key to prevent phishing attacks from hijacking your account and compromising credentials**

Web Services

Multi-factor authentication deployment can also be used as the identity provider for a web service like Google Docs or Salesforce cloud apps. In this scenario, a login request uses the Security Assertion Markup Language (SAML) and trusted certificates between the app and the multi-factor server for the additional authentication step.

This is the method used by Google and Apple to add second-factor features to users' Google accounts and Apple IDs, respectively. Using multi-factor authentication is a powerful way to protect your online accounts against cybercriminals.

Use two or more authentication factors to verify your identity, including:

- **Something you know: password, passphrase, or personal identification number (PIN)**
- **Something you have: security key or smart card**
- **Something you are: biometric like a fingerprint**

Multi-Factor Authentication via Smart Cards

Smart cards are cards or cryptographic USB tokens used for several authentication purposes, including physical access (buildings, rooms), computer and network access, and some secure remote access solutions (virtual private networks, portals).

Benefits of Smart Card Authentication

Secure Credential

Due to advanced cryptographic capabilities, smart card authentication is more secure than using passwords, radio frequency identification (RFID), or magnetic stripe cards. By using a PIN with the smart card, you get an added layer of security. Even if a smart card is stolen, a prospective thief needs to know the PIN to use it.

Smart cards are also tamper-resistant and difficult to hack, clone, or counterfeit. They are manufactured with built-in security features, including metal layers, sensors that detect thermal and UV light attacks, and software and hardware circuitry to thwart differential power analysis security countermeasures.

In addition, smart cards contain cryptographic elements protecting the information stored on the card and require secure methods to retrieve the stored information.

Multi-Purpose

Smart cards are convenient because a single card can serve

multiple purposes, eliminating the need for the user to carry multiple credentials. For example, one smart card could be used for physical building access, secure computer and network access, and as a user ID (employee, patient, visitor, government, etc.).

Data Storage

The chips embedded in smart cards make it possible to add, store, and update information on the card, including patients' PHI, even after the card is issued.

Easy to Use

Smart cards are lightweight, easy to carry, and offer streamlined access. As smart cards are already widely used for several purposes, like credit cards, most people are already familiar with them and how they work.

Are Smart Cards Right for Your Organization?

Smart cards are a multi-purpose option for organizations looking to couple physical and digital access. They also offer stronger security than many other types of credentials. However, there are higher costs and greater effort associated with purchasing, customizing, and deploying smart card authentication, so there may be more affordable and secure alternatives that meet your organization's needs.

If smart cards align with your organization's priorities, finding a solution with the right capabilities is crucial to minimizing the associated time, effort, and costs. We recommend going with a fully integrated smart card management solution that:

- **Manages the creation and lifecycle management of smart card devices and PKI certificates out of the box**
- **Provides broad support for contact and contactless smart card technology in card and token forms**
- **Delivers all the necessary components to successfully deploy, manage, and use smart card technology with Public Key Infrastructure (PKI), including smart cards, smart card readers, smart card management, PKI certificate management, and professional services**

Identiv's MFA Solutions

uTrust FIDO2 NFC Security Keys

Identiv's uTrust FIDO2 NFC Security Keys allow individuals, businesses, government agencies, and contractors to replace passwords with a secure, fast, scalable, cost-effective login solution. They support both contact (USB A/C) and contactless (NFC) use cases, provide multi-protocol FIDO U2F, FIDO2, smart card, and OTP support, are compatible with Windows, Linux, macOS, Android, and iOS, and are assembled in the U.S.A.

uTrust SmartID Secure Access Credentials

Identiv's uTrust SmartID Secure Access Credentials are a multi-application family of credentials for converged access, securing data integrity and authenticity. They protect multiple credential holder's identities from the door (physical access control) to data (logical access control). Based on digital certificates, our portfolio provides trusted authentication, digital signatures, secure remote access, desktop login, and data encryption.

uTrust Token Family

The uTrust Token Family offers users secure mobility for mobile desktop applications in PC-connected mode and a contactless smart card token in autonomous mode for a host of contactless applications. All uTrust Tokens enable strong two-factor authentication, combining something users have (the token) with something they know (their PIN code).

SCR3310 v2.0 USB Contact Smart Card Reader

CAC and PIV-approved SCR3310v2.0 is a small, robust PC-linked ISO/IEC 7816 contact USB smart card reader with backside mounting holes. It is the ideal PC-linked USB contact smart card reader for a wide variety of secure applications. Providing full compliance with all major industry standards, including ISO/IEC 7816, USB CCID, PC/SC, and Microsoft WHQL, the SCR3310v2 works seamlessly with virtually all contact smart cards and PC operating systems.

uTrust SmartFold SCR3500 Family

uTrust SmartFold SCR3500 Family are CAC and PIV-approved PC-linked USB contact smart card readers providing ISO/IEC 7816, CCID, PC/SC, EMV 2011, and GSA FIPS 201 compliance. You can use the readers for electronic ID, social security and loyalty programs, e-couponing, secure network logon, e-banking, online shopping, and gaming.

uTrust 3720 F Smart Card Reader/Writer Family

Our uTrust 3720 F Smart Card Reader/Writer Family integrates multi-technology and multi-ISO contactless interface options to support a wide variety of identification applications, including electronic identification and e-passport, e-banking, and e-commerce.

Identiv's MFA solutions keep your employees' and customers' data safe and protected.

Ready to secure your business? Speak to an expert today at sales@identiv.com or +1 888-809-8880.