# Modernizing multi-factor authentication with NFC Technology

## Increased deployment of FIDO tokens improve convenience, credentialing, and equipment security through several verticals

If there is one thing the past couple years has taught organizations, it is that business continuity requires ubiquitous connectivity. Digital transformation and modernization are reshaping societies and industries, and the security industry is no different. And with these changes challenges also arise.

As many economies transition into the era of intelligence—driven by next-generation technologies such as artificial intelligence and machine-learning—security threats increasingly become more sophisticated. From phishing attacks to password breaches and COVID-19 themed email scams, organizations have had to tighten up their cybersecurity strategies.

One of the outcomes of this is the increased deployments of FIDO (Fast IDentity Online) authentication in an effort to enable a passwordless future. Developed by the FIDO Alliance, an open association with representatives from several global organizations including Google, Microsoft, MasterCard HID Global and Yubico, FIDO standards provide a framework for stronger passwordless and multi-factor authentication. FIDO authentication provides convenience, seamless credentialing, equipment safety/security, while enabling quick transactions.

Essentially, FIDO works like a lock and key. First, a user registers a device and chooses any authentication method provided locally by this device (either biometric—like a fingerprint, or password ). During this registration, a public/private key pair is created. The private key stays on the user's device (a smartphone, smart card or key, for example) and is used to authenticate the device to the service/application. Access to this key is protected by the authentication method chosen. For stronger security, it is possible to register additional authentication methods (for example, a FIDO token + fingerprint + password).

When the user needs to access the service, they confirm their identity on their device with their authenticator, and the device acts as a translator between the authenticator's security and the service's security. This combination of layered protocols provides extremely robust access control.

### AN INTEGRATED AND CONVENIENT APPROACH TO AUTHENTICATION

With leading global organizations taking huge strides in reducing the world's over-reliance on passwords, the authentication market is flourishing with many customers deploying an integrated solution that includes near-field communication (NFC) authentication tokens embedded with FIDO2 protocols and encryptions, through NFC readers.

NFC readers are ideal in retail, health care and pharmaceutical, financial services, and other organizations seeking higher security and access management while providing greater convenience and increasing speed at which users authenticate to perform their tasks. Use of NFC readers also eliminates the need to install drivers, and can be used with standard PCs and workstations, as well as with thin and zero clients. Most importantly, NFC readers support security and regulatory compliance requirements, which mandate two-factor user authentication for accessing workstations and applications.

**HID**

Advanced NFC reader technology allows organizations from several markets to benefit from strong authentication, as well as meet security and regulatory compliance requirements that mandate two-factor user authentication for accessing workstations and applications.

Additionally, leading reader technologies in the market should be interoperable with different smart card technologies, tags, and NFC-enabled smart devices, and be compliant with identification standards such as ISO14443 A/B and ISO 15693. Other key features to keep in mind are:

- **Contactless performance –** Reliable, secure authentication no longer require physical contact
- **Integration with existing employee badge –** Expand the usage of existing physical access cards to computer logon, as well as network and cloud access.
- **Increased security and better user experience –** Read and retrieve highly secure one-time passwords (OTP)
- **Easy installation –** Eliminates the need to install drivers; uses native supported CCID drivers within the operating system.
- **Compact Form factor –** Enables two-factor authentication in space-restricted work environments such as healthcare and point-of-sale
- **Regulatory compliance –** Certifications to all relevant industry standards including PC/SC, WHQL, USB CCID, EMV 2000, and Common Criteria ensure security, worldwide compliance and easy integration in any system.
- **Long reading range –** Allows for convenient and contactless authentication

### AUTHENTICATION DEVICES: BALANCING ZERO TRUST SECURITY AND END-USER CONVENIENCE

Users need access to a variety of IT resources conveniently and efficiently. Particularly in hybrid environments, the need to maintain strong security— from physical entry to IT systems to cloud apps—is paramount. Security devices (tokens) are available in different form-factors,, such as smartphones, smart cards or USB-A/USB-A keys. These devices rise to the challenge and enable organizations to:

- Build a Zero Trust foundation with secure identities to access physical and IT resources across the organization
- Provide superior user convenience with a single, convenient and hassle-free credential for converged access
- Deploy quickly and scale as security requirements change
- Enable multi-factor authentication, thus complying with regulations and standards to reach required security levels
- Enhance user convenience by providing employees a convenient experience that ensures they have the anytime, anywhere access they need

In our fast-paced reality, it has become more difficult for people to maintain and memorize complicated passwords to keep their data private. Organizations can reduce the financial and reputation hit of all-too-common security breaches caused by weak or exposed passwords by embracing FIDO security keys with NFC technology.

### USE CASES WITH NFC READER TECHNOLOGY

In retail applications, for instance, NFC authentication contributes to improved customer service and increased operational efficiencies. Business owners can also avoid damage of expensive computer ports in point of sales stations as NFC readers allow for touchless transactions.

Touchless transactions have also become popular in healthcare environments, where hygiene protocols have become even more strict during COVID-19. Busy emergency rooms and hospitals can quickly verify patients, doctors and staff securely and seamlessly.

In enterprises, authentication is important particularly in shared workstations, third-party access to computers, and for single sign-on.

Finally, in manufacturing and warehouse environments where manufacturing processes must be carried out efficiently in terms of operations, personnel safety and costs, NFC authentication eliminates time-consuming user verification and access to machines, inventory, shipping docs, etc.