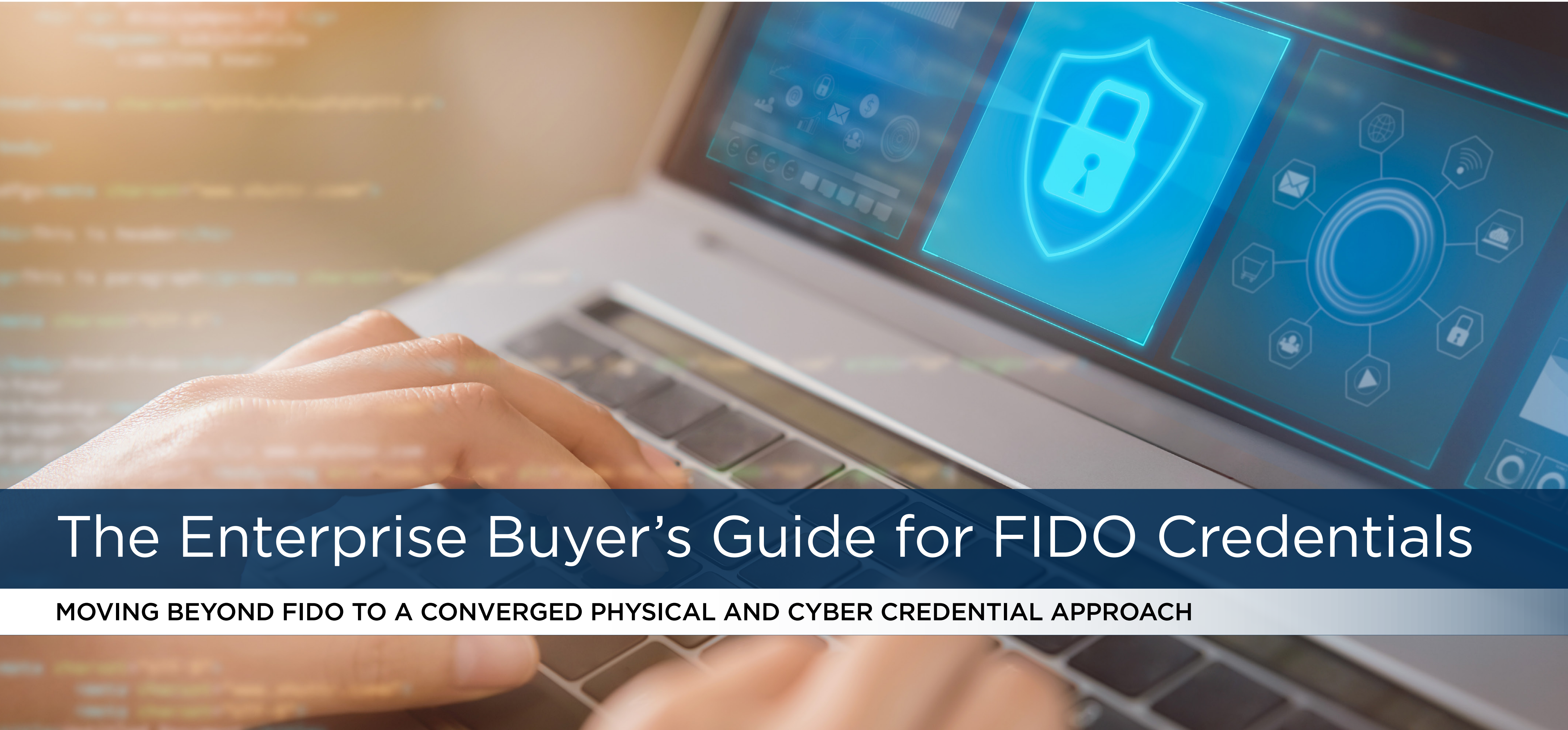
HID®



The Enterprise Buyer’s Guide for FIDO Credentials

MOVING BEYOND FIDO TO A CONVERGED PHYSICAL AND CYBER CREDENTIAL APPROACH

CONTENTS

TO NAVIGATE A PACKED MARKETPLACE, EDUCATION COMES FIRST.

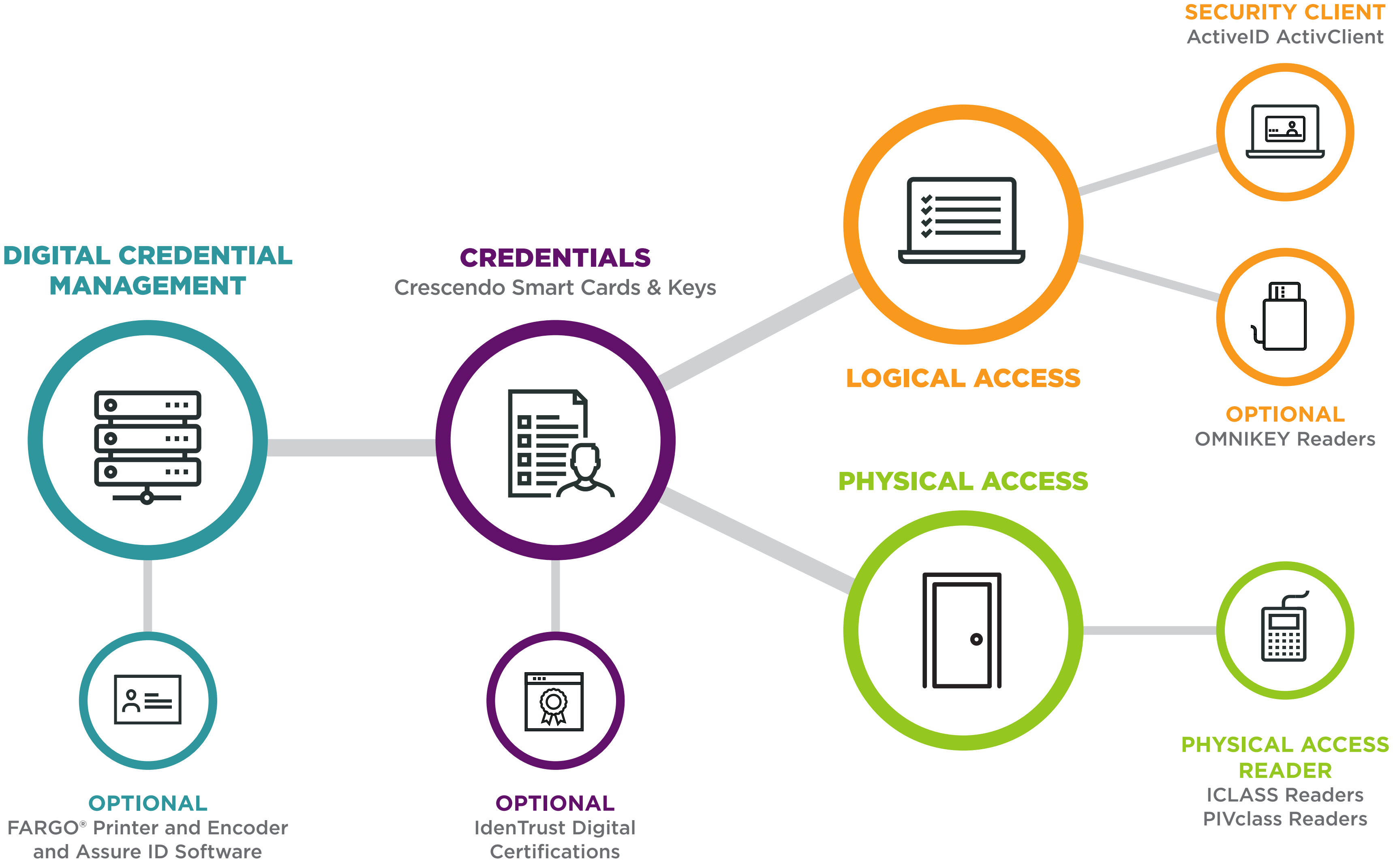
When it comes to protecting enterprise data and securing access, technology has come a long way from the days of multiple passwords and clunky numerical authentication devices. This is great news for organizations looking to minimize the risk of breach and loss, but potentially not-so-great news for decision makers who face a herculean task when selecting credentials. To add to the complexity, terminologies and technologies in this robust ecosystem vary widely.

The potentially mindboggling number of credential options on the market include SMS-based or mobile app-based two-factor authentication (2FA), as well as hardware-based credentials like smart cards and USB encrypted keys that provide a fast, easy route for 2FA without dependence on a phone. Many of these options are based on the **FIDO standard**, which is an open security protocol that's known for being difficult to intercept.

Google and some security companies joined the FIDO Alliance with the idea of an open, second factor authentication protocol. While Yubico may have helped develop the standard, it's not the only company that produces FIDO security keys. Plus, FIDO may not be the only security standard that's relevant to your needs.

We've created this buyer's guide to help you navigate the complexity of the credential selection process. Read on for ways to align your organization's unique needs with the right technologies and ecosystem components in this crowded landscape.

Enterprise-Ready Converged Credential Ecosystem



DIGITAL CREDENTIAL MANAGEMENT

CREDENTIALS
Crescendo Smart Cards & Keys

LOGICAL ACCESS

SECURITY CLIENT
ActiveID ActivClient

OPTIONAL
OMNIKEY Readers

PHYSICAL ACCESS

PHYSICAL ACCESS READER
ICLASS Readers
PIVclass Readers

OPTIONAL
FARGO® Printer and Encoder and Assure ID Software

OPTIONAL
IdenTrust Digital Certifications

WHEN SELECTING A SECURITY KEY OR ACCESS CARD, HAVING THE RIGHT PRIORITIES MATTERS.

Ultimately, choosing secure credentials for your organization is a balancing act. Matching your use cases with the right technology and user experience is crucial—but first you should understand the criteria in play:

What should you be considering when you select a smart card or USB key?

TOP CONSIDERATIONS:

- Which enterprise use cases the card or key should cover
- Which security standard or technology supports the credential's features

ADDITIONAL FACTORS:

- The access patterns of your workforce
- Which credentials integrate easily with your IT infrastructure
- Compliance standards for data protection within your jurisdiction & industry
- Your organization's physical & geographical footprint
- Plans for expansion or major changes to your workforce

With these considerations in mind, it's time to explore which **enterprise use cases** for smart credentials fit your needs and get a brief rundown of relevant **technologies**.

SOME CREDENTIAL OPTIONS WILL ALIGN WITH YOUR ENTERPRISE USE CASES—AND SOME WON'T.

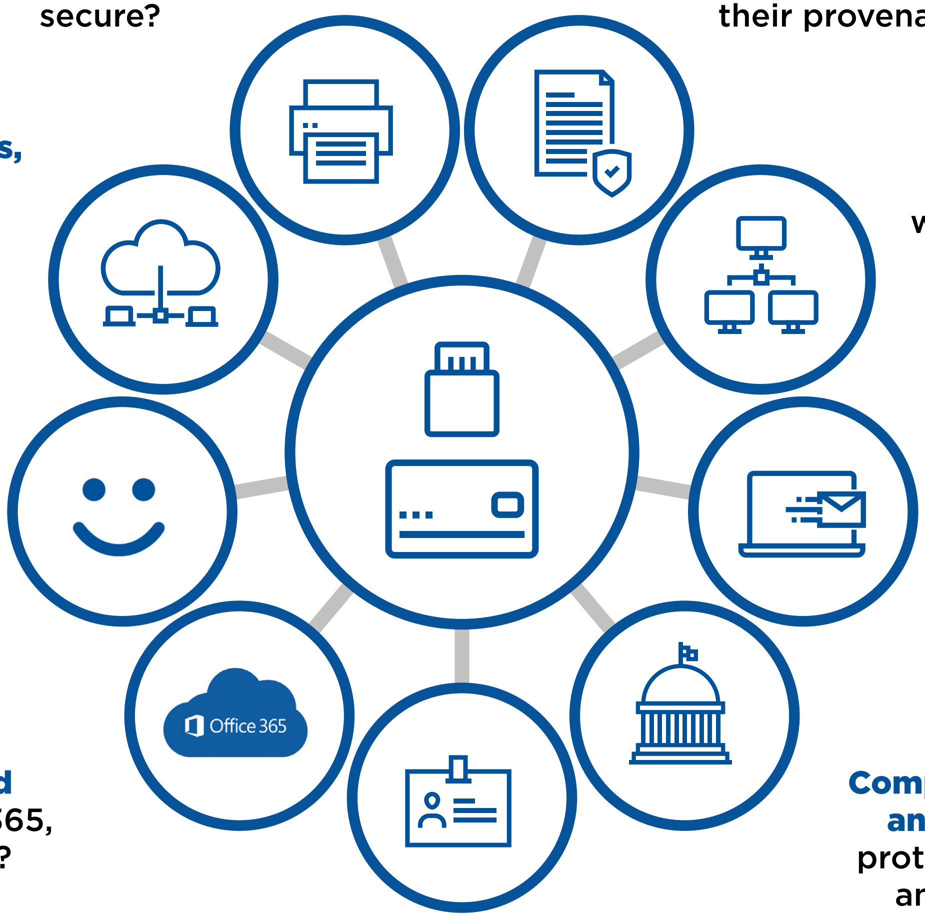
No two organizations work the same way. Understanding how and where you'll need to secure access and protect your enterprise data is key when deciding which credential option is best.

You're probably managing a lot more home workers than you used to. Do they need secure credentials for cloud applications, such as Office 365, or to access your organization's virtual private network (VPN) remotely?

If your mindset is a little more comprehensive, you might be considering options that help you secure the physical workspace as well. When protecting sensitive information is a major concern, you'll need credential options that provide dual encryption and authentication functionality.

What Are *Your* Use Cases?

Do You Need To…



Authenticate at the printer to keep sensitive documents secure?

Digitally sign documents to prevent tampering and verify their provenance?

Deploy, use and manage your devices with an on-premise and cloud ecosystem?

Protect communication and data with public key certificates by digitally signing and encrypting emails, and by encrypting data at rest?

Comply with mandates and regulations to protect access to data and applications?

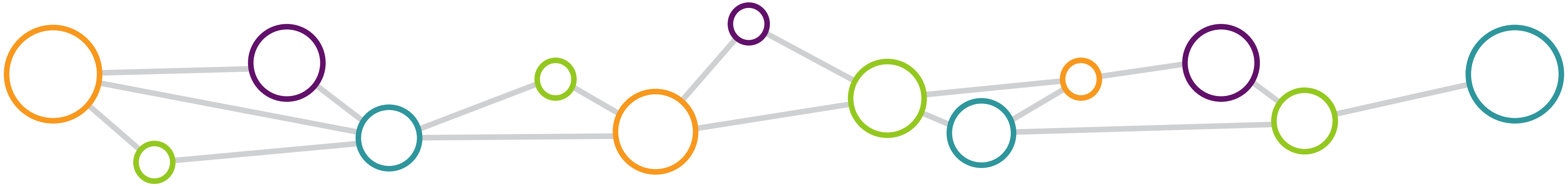
Secure access to your workplace with a converged corporate badge that can also be used for cloud and IT access?

Secure access to cloud applications like Office 365, G Suite, Dropbox, etc.?

Secure Windows Logon?

Secure access to IT applications, networks and systems

ENTERPRISE CREDENTIALS USE A VARIED SET OF TECHNOLOGIES AND STANDARDS FOR SECURE ACCESS—NOT JUST FIDO.



FIDO2

This emerging standard aims to remove passwords from compliant Web applications, eliminating one of the major causes of breaches and security incidents. FIDO is the backbone of Microsoft's Windows Hello Security Key, protecting access to Windows and Azure Active Directory. FIDO-enabled security keys or cards allow users to authenticate without the need for an additional software "middleman." They communicate directly with applications the user is seeking to access, allowing for secure, simple logins.

Public Key Infrastructure (PKI)

PKI is the gold standard in cryptographic security and is the baseline for the US federal government and many other organizations security. PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption. Public key encryption allows for digital signing, email signing, and much more.

The Initiative for Open Authentication (OATH)

This industry collaborative security standard is widely used for VPN authentication. Created as an open standard that outlines the implementation of core authentication credentials, OATH is a collaborative effort by the industry meant to facilitate interoperability between products and enable strong authentication across systems.

Physical Access Technologies

Physical access technologies like iCLASS SE, Seos, Mifare Desfire, and others, allow for contactless authentication via devices or authenticators. The level of security and precise nature of encryption provided by a smart card vary based on the chip's specific hardware and software.

THE RIGHT CHOICE OF CREDENTIAL FOR YOUR WORKPLACE CAN MINIMIZE COSTLY IMPLEMENTATION ISSUES AND STREAMLINE USER EXPERIENCE.

Should you be considering converged credentials?

A converged credential provides the most seamless experience for users, as it allows for both physical and cyber access. Allowing your workforce to access everything they need to do their jobs with a single smart badge or security key can be a game-changer for your organization. If you already provide a badge to your workforce, going for a converged credential will lower the total cost of ownership, both by buying one device for each user instead of two (a badge and an authenticator) as well as saving on logistical costs.

A converged credential can also make it easier to comply with regulations that require securing data both in physical form (e.g.: printed) and in IT systems by ensuring that access is to physical spaces and to IT systems are controlled and deactivated by a single device, and enabling automated offboarding of both domains.

Will your choice mesh with other authentication technologies?

If you use multiple authentication technologies, you'll need a credential that can handle them all. Solutions that don't play well together or don't safely accommodate legacy systems are a source of operational risk that can be easily avoided.

Will your choice ease the password burden on your workforce?

With a secure smart badge or security key you can remove the need for multiple PINs, passwords, or logon procedures across applications, reducing the mental burden on your workforce and the administration burden on your IT support. A single secure credential that can support a single shared PIN across all your applications is ideal.

How do you plan to manage the smart badges and security keys and all the access policies across both physical and cyber resources?

Take a unified approach to credential issuance and access management for both physical and digital identities, Look for management solutions with an ecosystem of applications that work seamlessly together.

HID CRESCENDO® SMART CARDS AND USB KEYS DELIVER VERSATILITY AND SECURITY ACROSS BOTH CYBER AND PHYSICAL SECURITY USE CASES:

HID Crescendo® smart cards and USB keys deliver versatility and security across both cyber and physical security use cases:

- Benefit from **trusted identities**, ensuring that digital and physical access is restricted to authorized individuals.
- **Future-proof** your organization's credentials with solutions designed to work well with both legacy systems and emerging cybersecurity evolutions.
- Go **beyond MFA and open doors** with an authenticator investment that includes digital signing, data encryption, and physical access functionality.
- Enable **seamless compliance** with regulations around access to sensitive data, including GDPR, HIPAA, PCI-DSS, SOX, SP800-171, CMMC. NYC cc part 500, NERC-CIP and more.

Need more information to make a decision, or want to learn more about enterprise FIDO credentials?

SPEAK WITH AN EXPERT