EXECUTIVE BRIEF

Zero Trust Authentication and Beyond

ORGANIZATIONS REQUIRE ADVANCED AUTHENTICATION TO MEET TODAY'S CHALLENGES

Identity solutions that meet the dire need for authentication

The growing complexity created by increasingly mobile workforces and business models and the unrelenting tide of data breach and compliance challenges are transforming cybersecurity practices. In addition, the widely adopted Zero Trust architecture models require that digital entities (people and things) cannot be trusted until they have been authenticated through integrated digital ID services.

Therefore, organizations need to provide their employees, contractors and customers with secure identities to protect access to on-premise and cloud applications, facilitate secure collaboration across and outside of the organization, protect corporate data and secure access to the organization's premises.

The successful deployment of advanced authentication requires a complete solution that manages the lifecycle of authenticators, streamlines replacement of lost/stolen authenticators and securely updates and revokes credentials when the user leaves the organization. HID Global's Crescendo® family delivers on all of these needs as part of a comprehensive advanced authentication suite that makes it possible to deploy secure identities at scale.

Authentication capabilities and beyond

Authentication is a critical process to ensure cybersecurity; Crescendo authenticators support secure authentication via open standards such as PIV / PKI, FIDO2 and OATH.

The wide range of Crescendo authenticators offers organizations extensive choices:

- Secure access to IT applications, networks and systems like Virtual Private Networks, and Microsoft Active Directory and Azure Active Directory
- Secure access to web and cloud applications such as G Suite, Dropbox, etc.
- Secure access to premises with a converged corporate badge (including with Seos®) that can also be used to access IT applications
- Protect communication and data with public key certificates, by digitally signing and encrypting emails, and by encrypting data at rest
- Digitally sign documents, ensuring they have not been tampered with and confirming their provenance
- Provide secure printing, ensuring that a sensitive document is only released from the printer after the user is authenticated at the printer

Crescendo's support for open standards like PKI / PIV, FIDO and OATH enables those use cases as software vendors implement support for the open standards into their applications.

Comprehensive advanced authentication solution

Crescendo is part of a comprehensive advanced authentication solution that makes it possible to deploy secure identities to scale. This integrated authentication solution is comprised by wide range of authenticators, credential management systems, authentication services, client applications and digital certificates to suit organizations' most complex needs, user population diversities and use cases.

AUTHENTICATOR PORTFOLIO

The HID Crescendo portfolio family provides different form factor options, all with a common authentication platform that provides a common set of security services and a number of benefits for the modern enterprise.

HID Crescendo 2300

The Crescendo C2300 Series is the next generation of smart cards, providing organizations with secure authentication for access to IT applications that integrates with existing physical access technologies and creates a flexible platform for unified enterprise badges. The card can be inserted into a standard smart card reader or used via its Near Field Communications (NFC) antenna for use with mobile devices. It provides:

- Seamless compliance while protecting networks, computers and applications with strong authentication
- Digital signature, enabling users to verify the origin of emails and documents
- Data encryption, allowing only authorized users to access sensitive information
- A converged corporate badge, allowing the use of one single smart card for visual identity, network, cloud authentication and physical access
- Secure printing ensuring confidentiality and guaranteeing stronger data protection

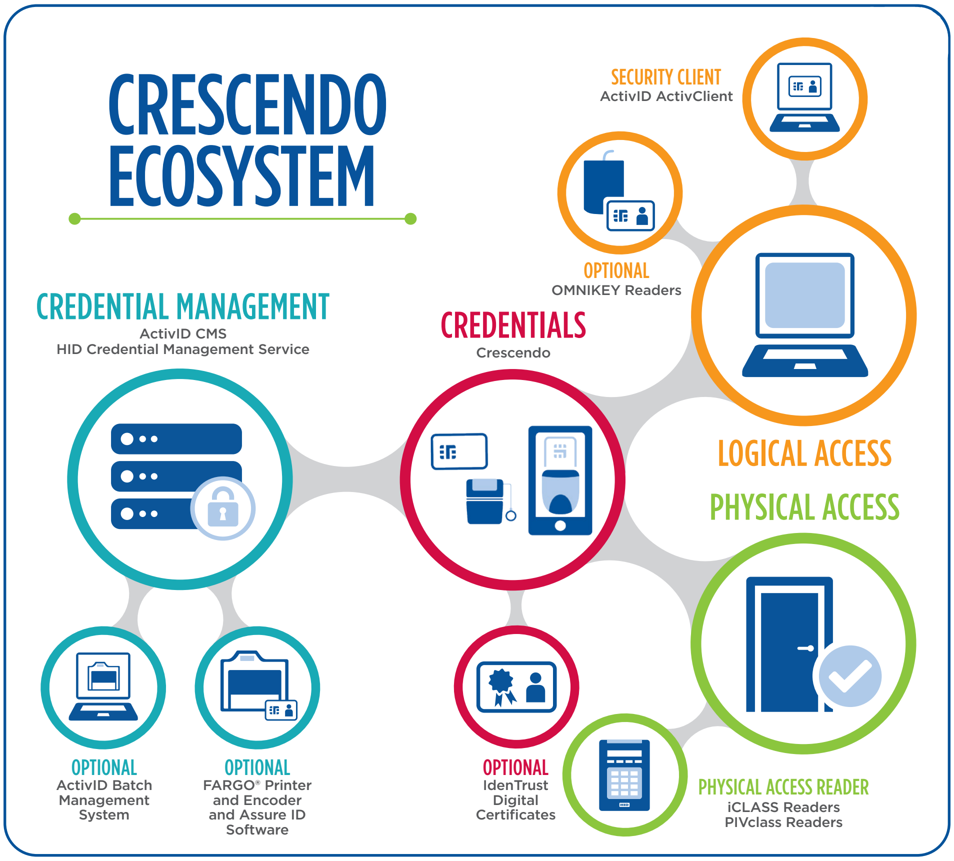
HID Crescendo Key

The HID Crescendo Key Series is a convenient, unobtrusive smart USB key that enables seamless and secure authentication. This authenticator provides strong security, enabling NFC and USB ports with the same two-factor authentication, digital and encryption capabilities of a Crescendo smart card.

The Crescendo Key's small footprint is particularly convenient when used with mobile devices, tablets and Ultrabooks since it is nearly flush with the device casing. Thanks to its convenient USB interface, workstations and laptops do not require additional readers, so IT operational costs are reduced.

HID Crescendo Mobile

The HID Crescendo mobile app provides strong multifactor authentication to cloud applications, VPNs, desktops and Microsoft Active Directory. It can be downloaded on Android or iOS devices and behaves as a regular PKI smart card with no need for specific middleware — protecting the user's digital certificates, private keys and other credentials. The Crescendo mobile app works on personal smartphones and tablets and is fast and cost effective to deploy — particularly for contractors or remote workers.



CREDENTIALS LIFECYCLE MANAGEMENT – CREATING, MANAGING AND REVOKING CREDENTIALS

The effort required for the management of credentials within organizations can be significant and a number of situations create additional complexity:

- A lost or stolen authenticator requires replacement of the device along with the user's credentials, including the ability to continue decrypting data which was encrypted with the previous authenticator
- In the case of a forgotten PIN code, the user will need to securely reset the PIN code to continue using the authenticator
- When an employee leaves the organization, all credentials stored on the authenticator must be revoked to cut off access to protected applications, regardless of whether the authenticator was physically given back to the organization

Depending on their security policies, organizations also may require a different workflow for issuing authenticators, such as self-service, helpdesk assisted, or when a specific approver is necessary. Organizations may also want to audit administrative events, especially if specific laws and regulations govern them.

The HID Credential Management System (HID CMS), available on-premise and in the cloud, provides a full range of capabilities to help organizations deploy and manage the lifecycle of authenticators at scale while complying with regulations and mandates.

AUTHENTICATION SERVICES

In many cases, whether they are on-premise or in the cloud, applications do not handle advanced authentication themselves but rather delegate the authentication process to an authentication server. The benefit of this approach is that the authentication server acts as an identity provider to the applications (relying parties) and helps keep the authentication, management and auditing of secure identities in one place, providing better security and also ease of use thanks to single sign-on.

HID Global's integrated authentication solution provides multi-layered, versatile authentication for transaction verification and approval available both on-premise or via the cloud. Thanks to its adaptive security approach — from any location and device going beyond simple passwords — it enables organizations to tailor their authentication methods to specific user groups and risk levels while providing users with convenient and secure access to data from PCs or mobile phones. It can also be used for employee security to protect VPN access, cloud-based and web applications and offers SOAP, SAMLv2, OpenID Connect and RADIUS APIs to easily integrate with them.

HID Global's authentication suite allows organizations to meet growing regulatory requirements and comply with increasing requirements for multifactor authentication or risk-based authentication (like PSD2, HKMA, 23 NYCRR 500, etc) while:

- Proving that the user is who they claim to be (authentication)
- Ensuring that the user's access to resources and services is limited to that for which they are authorized (authorization)
- Keeping a trustworthy record of what the user does (audit)

CREDENTIAL USAGE ON THE WORKSTATION – EMAIL SIGNATURE, ENCRYPTION, PKI LOGIN, ETC.

In some cases, Crescendo authenticators can work without additional software on the end user's computer or phone thanks to its reliance on standards-based security protocols.

ActivID® ActivClient® enables applications that do not natively support Crescendo authenticators. ActivClient also offers a set of automatic configurations, automatic updates, group policies and troubleshooting tools to ensure low cost of ownership when deploying advanced authentication.

DIGITAL CERTIFICATES

One of the most secure options to provide secure identities is the use of digital certificates. The digital certificate and associated private key are protected inside the Crescendo authenticator and can be used for authentication, digital signature and encryption.

HID's IdenTrust™ cloud-based certification authority is able to issue certificates to Crescendo authenticators either directly or managed by HID's credential management solution.

Thanks to its cloud-based nature, IdenTrust removes all the guess work of deploying PKI and provides a secure identity that is trusted by default for most computer and mobile devices, which is quite important when sending secure emails or digitally signed documents outside your organization.

CRESCENDO — THE SOLUTION TO TODAY'S AUTHENTICATION NEEDS

HID Crescendo's family of authenticators provides organizations the secure identities they need to implement Zero Trust security and meet today's cybersecurity challenges as well as the ability to comply with evolving regulations and mandates. HID Crescendo's family of authenticators goes beyond simple authentication by supporting advanced use cases like digital signature, encryption, secure printing, physical access and more.

HID's complete solution includes cloud and on-premise software that enables organizations to keep existing solutions and evolve them in a scalable way while enabling them to choose additional authentication methods. The integrated authentication solution provides customers with centralized PIN management and supports the evolving needs of organizations while allowing compliance with FIDO and FIPS 140-2, which ultimately increases security level.

HID Crescendo authenticators can be easily plugged into an organization's ecosystem, securely manage the lifecycle of the authenticators, and help organizations to quickly and cost effectively deploy those authenticators while also meeting mandates and regulations.

For more information visit:
https://www.hidglobal.com/products/cards-and-credentials/crescendo