Crescendo® Mobile Virtual Smart Card

BENEFITS:

- Security – Uses digital certificates for client authentication
- Compatibility – Leverages platform support for smart card authentication
- Compliance – Satisfies strong authentication requirements for access to sensitive information
- Simplicity – Utilizes the same ActivID Credential Management System for both Crescendo Mobile and physical Crescendo cards

HIGH SECURITY MOBILE AUTHENTICATOR

- **Multifactor Authentication –** Replace passwords with digital certificates protected on the users' phone
- **Signature and Encryption –** Digitally sign and encrypt emails and documents
- **Simplified Rollout –** Leverage your users' phones as authenticators; distribute secure cryptographic credentials to users without the need to ship smart cards or smart card readers
- **Ecosystem Support –** Compatible with existing infrastructure and applications supporting smart cards, including desktop operating systems and applications
- **Bluetooth and NCF compatible –** No need for physical connection to use Crescendo Mobile with your PC

Organizations looking to eliminate passwords have had to make a difficult choice between solutions that are easy to deploy but only protect some enterprise applications and solutions that protect most applications but require physical authenticators and associated hardware to connect those authenticators to PCs.

The Crescendo Mobile App is an authenticator that resolves this conundrum by providing strong multifactor authentication to cloud applications, VPNs, desktop, and Microsoft Active Directory alike. The Crescendo Mobile App can be downloaded onto Android or iOS devices and behaves like a PIV smart card—protecting the user's digital certificates, private keys and other credentials. Because it works on personal smartphones and tablets, Crescendo Mobile is faster and more cost effective to deploy—especially for contractors or remote workers.

Crescendo Mobile is part of the HID's authentication solution that provides full lifecycle management of both the authenticators and the credentials protected by the authenticator.

The Crescendo Mobile App is compatible with highly secure Crescendo smart cards. Instead of being a separate device inserted into a contact smart card reader, however, it connects to a desktop computer using an NFC reader (when running in Android devices equipped with NFC) or Bluetooth (when using a Virtual Bluetooth Smart Card Reader available for Windows 10).

Crescendo Mobile can be used with the in-box Windows PIV minidriver and with ActivClient, which provides additional functionality, including a PKCS#11 library and automatic secure email configuration. Any application that can use digital certificates in smart cards to authenticate to remote sites and networks, digitally sign emails and documents, or encrypt files and email can immediately leverage the certificates residing in the Crescendo Mobile App.

Crescendo Mobile offers the possibility of local issuance like any other smart card, while simultaneously enabling remote issuance of credentials to user phones using the Internet connection of the phone itself.

LOGICAL AND PHYSICAL ACCESS SOLUTIONS

CRESCENDO MOBILE FEATURES:

- Personal Identity Verification (FIPS 201) card edge that allows the virtual credential to be compatible with the built in Windows PIV minidriver for basic authentication and signature or with ActivClient for full access to all PIV certificates.
- Available for Android 7 or later in Google Play and for iOS 11 or later in iTunes App Store
- NFC local issuance and credential use supported in Android devices.
- Bluetooth local issuance and credential use supported in Android and iOS devices
- Remote issuance supported in Android and iOS devices

SUPPORTED USAGE SCENARIOS:

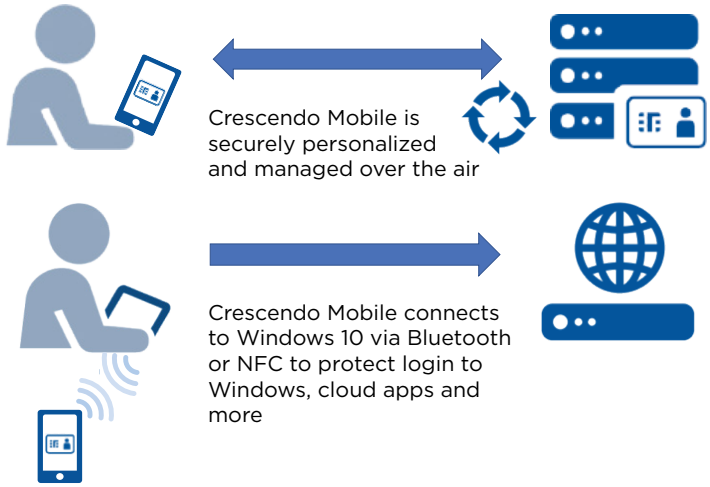
- Authentication - Use the mobile phone to log on and unlock a Windows workstation and automatically lock the workstation when walking away from it. Use the phone to authenticate to a corporate VPN or to cloud applications that support client certificates for authentication.
- Email, Microsoft Office and Adobe Acrobat document signature – Use the phone to carry the keys and digital certificates used to digitally sign documents and messages to guarantee who originated those and that they have not been tampered with
- Email and Windows EFS file encryption – Ensure sensitive data confidentiality by requiring the phone to access encrypted email messages or files encrypted with Windows Encrypted File System

SPECIFICATIONS

Cryptographic Algorithms	AES for management and secure channel, RSA 2048 for signature and key exchange
Mobile Phone Operating System	Android™ 7 or later, iOS® 11 or later
Client PC Operating System	Windows 10 1709 or later
Secure Key Generation and Storage	Android™ KeyStore (hardware backed) iOS® KeyChain (hardware backed)
Lifecyle Management	ActivID® CMS 5.0.3 or later

NOTE: Added trademarks and symbols and adjusted spelling to Cryptographic Algorithms

HOW CRESCENDO MOBILE WORKS



hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

2018-10-24-iam-crescendo-mobile-ds-en PLT-04055

An ASSA ABLOY Group brand