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.
SPECIFICATIONS

**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

---

**LOGICAL AND PHYSICAL ACCESS SOLUTIONS**

**CRESCENDO MOBILE FEATURES:**

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

**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

**HOW CRESCENDO MOBILE WORKS**

- Crescendo Mobile is securely personalized and managed over the air.
- Crescendo Mobile connects to Windows 10 via Bluetooth or NFC to protect login to Windows, cloud apps and more.

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 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design and Crescendo are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2018-10-24-tam-crescendo-mobile-di-en  PLT-04055

An ASSA ABLOY Group brand