



Secure Mobile Credentials



- Mobile credentials that work with any Bluetooth smart phone
- Public key cryptography with secure private key storage
- Intuitive access app available from iOS or Android app stores
- Multi-factor authentication enables higher security levels
- Simple enrollment into popular access control systems

iPass mobile credentials can be stored on any Bluetooth smart phone to provide intuitive mobile access with iPass multi technology readers and popular physical access systems. Security is enforced through state-of-the-art public key cryptography and optional multi-factor authentication.



iPass secure mobile credentials use state-of-the-art cryptography to control physical access from any Bluetooth enabled smart phone or watch. Available for iOS and Android via authorized app stores, the iPass mobile app turns any smart phone into a high security physical access credential.

iPass mobile credentials support multi-factor authentication at any iPass reader, optionally checking a pin code, facial recognition* or fingerprint matching*. One, two or three-factor authentication uses something you have (your phone), something you know (your pin code) and something you are (your biometric).

* Available on supported phones

iPass provides simple cross-platform software to enroll credentials into popular access control systems. Coupled with public key challenge-response authentication the solution delivers cryptographically secure physical access via users' smart phones without the need for smart cards or access keys.

iPass secure mobile credentials, together with iPass multi-technology access readers, seamlessly convert any Bluetooth smart phone into a secure access credential compatible with all modern access control systems. The intuitive iPass Mobile App can be downloaded from iOS or Android app stores. Simple cross-platform software supports enrollment into all access control software.

		
Features	iPhone	Android
Bluetooth Low Energy (BLE) support	yes	yes
Certified App Store applet	yes	yes
Optional PIN verification	yes	yes
Optional fingerprint matching	yes*	yes
Optional facial recognition	yes	no
Cryptographic Authentication		
Public key algorithm	ECDSA P-256	ECDSA P-256
Challenge-response time (typical)	< 0.5 sec	< 0.5 sec
Credential Enrollment		
Windows 10, 11, Server 16 or later	yes	yes
macOS High Sierra or later	yes	yes
Linux: RHEL, SUSE, Ubuntu	yes	yes

* Dependant on phone model



**Emeryville
California, USA**

**www.ipass.io
info@ipass.io**

Technical specifications are subject to change
Copyright © 2025 iPass Security LLC All rights reserved
All trademarks are the property of their respective owners