PRODUCT DATASHEET

safetrust

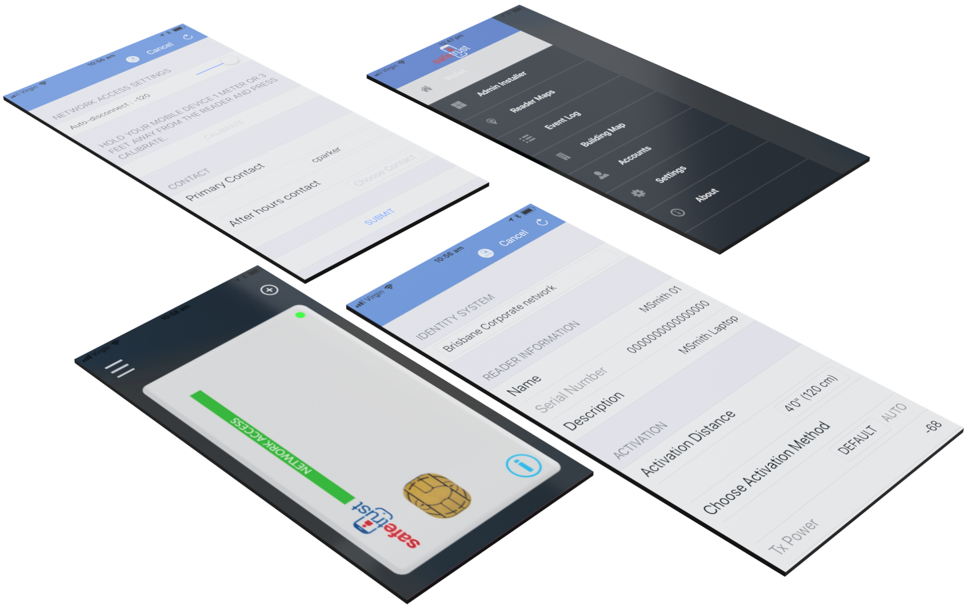
Safetrust Wallet App

All your cards, all in one place

No need to write down pass-codes or worry about leaving your access cards laying around. The Safetrust Wallet allows users to store Virtual Credentials from multiple trusted sources. Virtual Credentials such as building access cards, corporate identities, club memberships or payment cards can be securely stored in your Safetrust Wallet, allowing you can carry your credentials with you everywhere you go.

Key Features

- **Virtual Credential Consolidation:** Store all your virtual credentials in a single, secure location that is with you wherever you go. The Safetrust Wallet uses public key infrastructure (PKI), backed by hardware security modules (HSM's), and device-based TPM security to ensure your virtual credentials are kept secure at all times.
- **Leashing:** The Safetrust Wallet supports “leashing mode” for fast one-to-one credential usage in concentrated environments.
- **Low Battery Consumption:** Unique architecture ensures that the Safetrust Wallet does not place a heavy drain on local batteries, due to excessive polling for supported devices.
- **Local PIN / Biometric Authentication:** The Safetrust Wallet supports local PIN/Biometric authentication for increased security over local credentials. Credential access rules can be defined to ensure that physical possession of the mobile device alone is not enough to release a credential.
- **Auto Authentication & Tap to Authenticate:** The Safetrust Wallet can be configured to automatically send a virtual credential to a supported reader (IoT sensor) when the mobile device is placed inside the preconfigured activation range. The Wallet also supports “Tap to Logon” / “Tap to Logoff” functionality for logical access to computers.



How does it work?

To begin, download the Safetrust Wallet from either the App Store for iOS devices or from Google Play for Android devices. Alternatively, the Safetrust Wallet application can be installed by customers who wish to control their deployments using their existing Mobile Device Manager (MDM). Login to the Safetrust Wallet using your email address and password, as defined in the Credential Manager portal. If this is the first time your device has been used with your Credential Manager account, you will be required to enter a PIN (sent to you via email) to link the device to your account. Assigned virtual credentials are automatically synced to the Safetrust Wallet for use.

Simply present your mobile device to a door reader for physical access or “Tap to Logon” for access to a local computer. Manual activation of the virtual credential can also be achieved by holding down the required credential within the Safetrust Wallet with your finger.

Safetrust Wallet Specifications

Description	Mobile device application for Android and Apple iOS that securely stores virtual credentials.
Configuration Method	Credential Manager - Identity and People Management
Supported Operating Systems	Requires Apple iOS 9.0 or later, Android 4.1 or later
Supported Virtual Credentials	NIST 800-73 Smartcard Emulation (unlimited)
Bluetooth Version	Bluetooth (BLE) 4.0 or later
Bluetooth Range	1 ft to 100 ft (.30 to 30 meters)
Security	PLAID / AES 256
Availability	The App Store for Apple iOS devices, Google Play for Android devices (search for Safetrust)

Technical data subject to change without notice.