Migrate to the Convenience of Mobile Access

Easy Mobility Upgrade Solution

The SABRE DECAL is a Bluetooth Low Energy (BLE) to RFID (proximity, smart-cards) gateway module that allows an existing building access reader to communicate securely with a mobile device. The SABRE DECAL allows organizations to replace or supplement existing building access credentials with one or more digital credentials stored within the Safetrust Wallet application.

How it works: The SABRE DECAL attaches to a building access reader and is powered using the readers RFID field. Building access credential data is sent encrypted from a mobile device via BLE to the SABRE DECAL. The SABRE DECAL then translates the data into a supported RFID format, allowing users to replace their existing physical access cards with digital credentials stored within their mobile device. The SABRE DECAL does not prevent existing physical access cards from communicating with the reader which means migration to mobile credentials can be gradual.

Installation: The installation of the SABRE DECAL is a simple procedure that involves (peel & stick) placement of the SABRE reader module on an existing host reader. The SABRE DECAL requires no special tools, no system downtime, and supports a mixed population of traditional plastic credentials, and mobile credentials. Enabling mobile credentials can be achieved without the need to modify existing door readers or back-end control systems.

The small footprint of the SABRE Reader Module measures just 1.29” H x 1.53” W x 0.11” D (33 x 39 x 3.0 mm). No battery required, power source comes from the RFID field.

safetrust SABRE Reader Benefits & Features:

- **Migrate to the convenience of mobile access:** A SABRE DECAL enables organizations to move to mobile credentials without the need to replace their existing readers.
- **Quick & Simple Installation:** The SABRE DECAL is a “Peel & Stick” upgrade that requires no external wiring or battery to be operational.
- **Reduce issuance and management cost:** Mobile credential management eliminates costs associated with deployment and re-issuance of traditional physical access cards.
- **Universal compatibility:** Interoperable with most reader brands and formats.
- Supports most popular readers in use today. Contact PCSC to confirm compatibility.

3541 CHALLENGER ST., TORRANCE, CA 90503 USA
PH 800.899.PCSC or 310.303.3600 PCSCsecurity.com

Details / Specifications

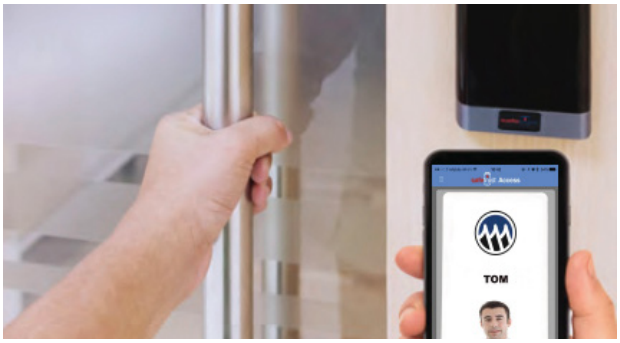
SABRE Reader Module	
Hardware Technologies	Bluetooth Low Energy (2.400 GHz - 2.4835 GHz), proximity 125 kHz, and 13.56 MHz
Bluetooth Range	1 ft to 100 ft (.31 to 30 meters)
Compatibilities	Most popular 125kHz proximity brands, MIFARE Classic and MIFARE DESFire
Mounting	Within host reader RF field (under bezel, surface mount or back potting), varies by host model
Mobile Operating Systems	Apple iOS 9.0 or later, Android 4.1 or later
Encryption	AES 256, x.509
Power Source	RFID field (no battery required)
Dimensions	1.29 x 1.53 x 0.11 in (33 x 39 x 3.0 mm)
Operating Conditions	Temperature: 35 - 65°C Humidity: 5-95% (non-condensing)
Weight	2 oz (56 g)
Warranty	2 Years (limited warranty, review warranty for complete details)

Technical data is subject to change without notice.

Quick & Simple Installation:

The SABRE DECAL is a "Peel & Stick" upgrade that requires no external wiring or battery to be operational. Place on the inside or outside of the existing reader.

Bluetooth SMART



PCSC

3541 CHALLENGER ST., TORRANCE, CA 90503 USA
PH 800.899.PCSC or 310.303.3600 PCSCsecurity.com

Safetrust Wallet Application

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.

- **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.

- **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.

- **Leashing:** The Safetrust Wallet supports “leashing mode” for fast one-to-one credential usage in concentrated environments.

- **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.

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.

How do we get started?

The Safetrust Wallet application is available through the SafeLogon and SafeAccess starter kits which include the SABRE reader/s, a number of employee licenses (with unlimited mobile credentials), and complete step-by-step instructions. These starter kits are available through authorized local system integrators, resellers and OEM partners.

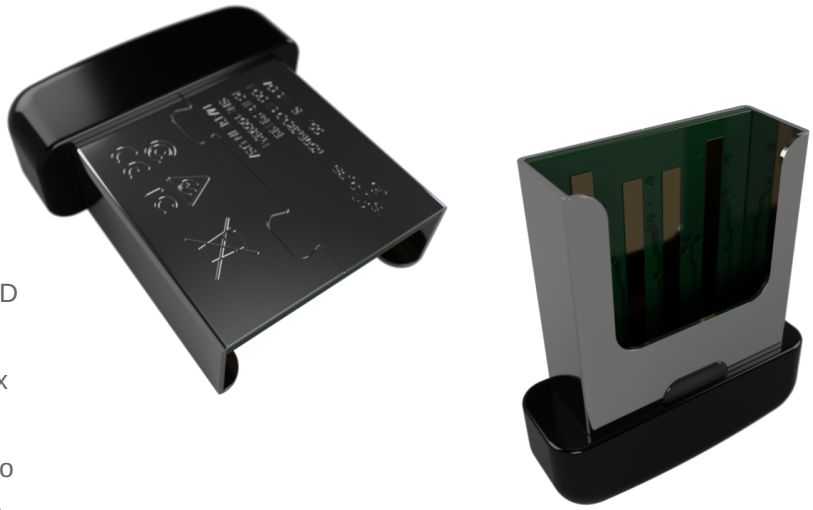
Safetrust Wallet

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.

SABRE USB

Tap your phone to logon



The SABRE USB is a Bluetooth Low Energy (BLE) to CCID reader module that enables virtual credentials stored in a mobile device to be used within Windows, MAC, and Linux platforms. When plugged directly into any spare USB port in a computer, the SABRE USB enables a mobile device to be used for tap-in/ tap-out authentication with configurable activation ranges for auto-authenticating and disconnection, meaning your mobile device never needs to leave your pocket.

Key Features

- **CCID Compliant:** Natively supported by Windows, MAC, and Linux with no requirement to install additional device drivers
- **Supports Multiple Emulation Modes:** Can be firmware enabled to run as a smartcard reader or in keyboard wedge mode for custom applications.
- **Configurable Range:** Can be configured for individual environments with adjustable connection and disconnection range
- **Onboard LED:** Can be configured to display different colour LED when powered and in use.
- **Small Form Factor:** Small form factor makes the SABRE USB suitable for mobile users with laptops.

How does it work?

When installed, the SABRE USB appears to the operating system as a CCID compliant smartcard reader. When a mobile device running the Safetrust Wallet application connects to the SABRE USB, the operating system natively accepts the virtual credential stored in the Wallet as a NIST SP 800-73 (PIV) secure smartcard. Authentication formats include certificates (SP800-73), smartcard emulation, or FIDO.

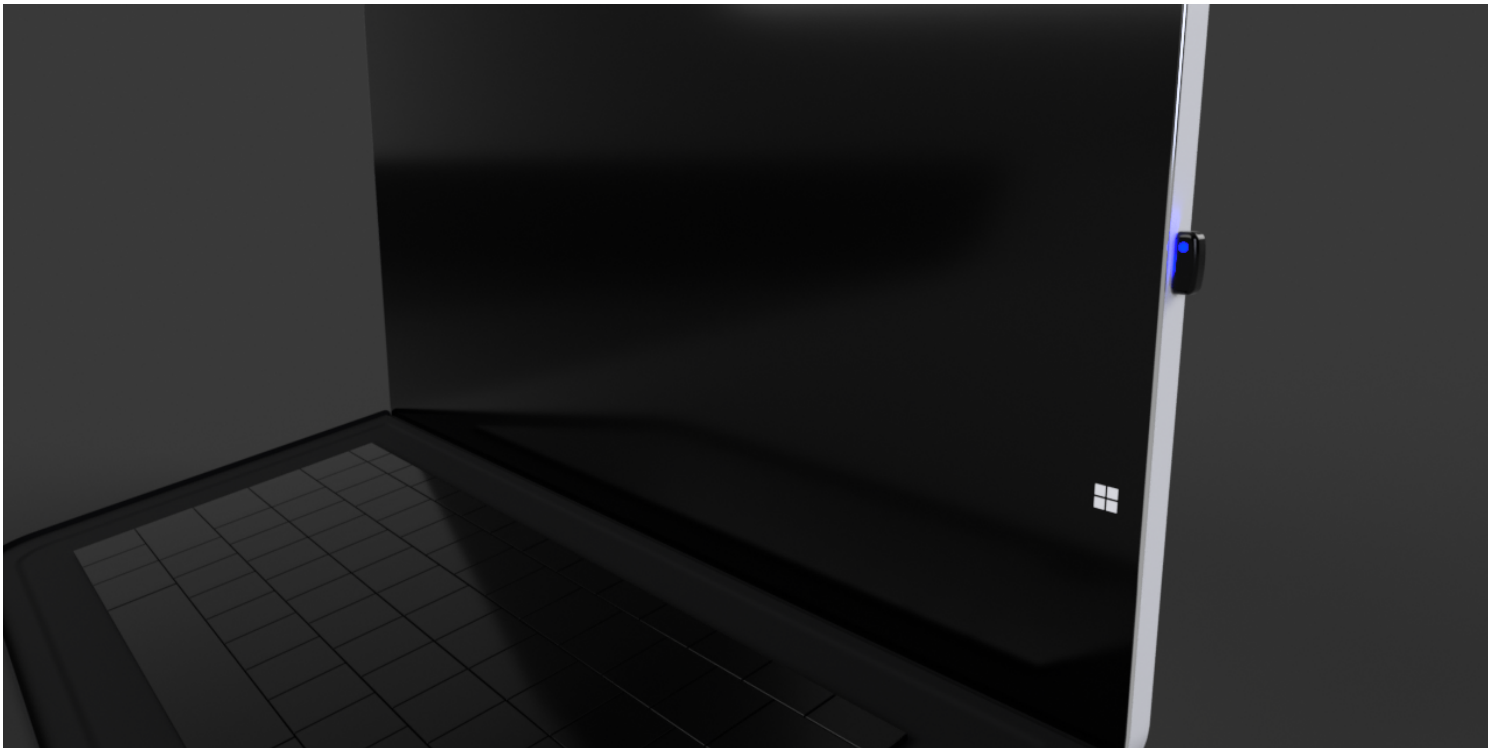
What is the installation process?

Simply install the SABRE USB into a free USB computer port and the operating system will recognize the device as a CCID compliant smartcard reader.

How do we get started?

SafeLogon starter kits include the SABRE USB, a number of employee licenses (with unlimited mobile credentials), and complete step-by-step instructions. SafeLogon is available through authorized local system integrators, resellers and OEM partners.

Bluetooth SMART



SABRE USB Specifcations

Description		• Full speed USB 2.0 (12Mbps) • USB BLE powered device • CCID compliant
Mobile Operating Systems		• Apple iOS 9.0 or later, Android 4.1 or later
Desktop Operating Systems		• Windows 7 and above • MacOS Version 10.11" El Capitan" or higher • Linux: REL 6, CentOS v7, Ubuntu 17.10 or above
Smartcard emulation from a mobile device	**Contact**	• ISO/IEC 7816 CCID compliant • T=0, T=1 protocol support • Communication speed up to 244, 105 bps (PPS, FI parameter)
	Contactless	• Support of ISO 14443 A and B (13.65 MHz) smartcards • ISO 14443 Part 1 to 4 complaint • MIFARE: Classic, DESFire • Communication speed: up to 848 Kbit/s
LED		• RGB (Tri colour)
Hardware		BLE 2.400 GHz - 2.4835 GHz , CCID
Network Access Credentials		NIST 800-73 certificate authentication, smartcard emulation, FIDO
Power Source		5 VDC
Bluetooth Range		0.3 - 30 metres
Encryption		AES 256, x.509, NIST 800-73
Dimensions		15 x 5 x 5 mm (External to USB port) 18 x 7.5 x 7 mm (total size)
Operating Conditions		• Temperature [c]: 0-65 • Humidity [%]: 5-90 (non condensing)
Regulatory Compliance		• Functional:FCC, IC, CE, RCM • Environmental: RoHS2, WEEE
Warranty		1 Year (limited warranty, review warranty for complete details)

Technical data subject to change without notice.

3541 CHALLENGER ST., TORRANCE, CA 90503 USA
PH 800.899.PCSC or 310.303.3600 PCSCsecurity.com

SABRE RELAY

Mobile control for electronic switches

The SABRE RELAY is a combination Bluetooth Low Energy (BLE) reader with access controller management capabilities. By presenting a virtual credential within the SABRE activation range, authorized users can trigger the onboard relay from their mobile device. The SABRE RELAY provides mobility for parking garages, remote buildings and single door offices, all within seconds from the Safetrust Wallet application.

Key Features

- **Combination Reader Controller:** Complete controller functionality, perfect for parking garages, single door businesses, and remote buildings.
- **Multiple I/O Interfaces:** Includes 24v / 12v relay, 5v input / output trigger, internal/ external antennas, Wiegand, RS-485, and optional Wi-Fi module.
- **OTA (Over-the-air configuration):** Firmware updates and configuration management can be made over-the-air through the Safetrust Wallet application or optional Wi-Fi module.
- **Configurable Extendable Range:** Activation range can be configured based on environmental requirements. Where additional range is required, the module supports the use of external antennas for both the BLE and optional Wi-Fi interfaces.
- **Online / Offline Operation:** The Credential Manager provides regular data exchanges to the Safetrust Wallet application and the SABRE RELAY, eliminating the need for constant online connectivity for authentication.

How does it work?

The SABRE RELAY is wired to an existing locking hardware and registered to an identity system within a customer account. Users are assigned virtual credentials for the specific identity system. When a mobile device with the corresponding credential comes into range of the SABRE, the encrypted credential is sent via BLE. The SABRE RELAY validates the mobile credential, triggers the relay module, and opens the gate or door.

What is the installation process?

Installation of the SABRE RELAY involves powering the relay module with 12VDC and selecting the relay output. Control lines on the SABRE RELAY are then physically wired to the locking hardware. When the SABRE RELAY relay is in place, it is assigned to an account and individually registered to an identity system within the Safetrust Credential Manager. The registration process for the SABRE RELAY is facilitated using the admin installer tab within the Safetrust Wallet application.

How do we get started?

SafeAccess starter kits include the SABRE RELAY, a number of employee licenses (with unlimited mobile credentials), and complete step-by-step instructions. The SABRE RELAY is available through authorized local system integrators, resellers and OEM partners.

SABRE RELAY Specifications

Description	The SABRE RELAY is designed for use with gates, overhead doors and other entry control devices.
Mobile Operating Systems	Apple iOS 9.0 or later, Android 4.1 or later
Hardware	BLE 2.400 GHz - 2.4835 GHz
Output	Form C relay, Wiegand (in / out)
Power Source	12 VDC
Bluetooth Range	.30 to 30 metres
Encryption	AES 256, x.509
Case Dimensions	139.3 x 67.3 x 40.1mm
Antenna Length	5dB - 80mm, 15dB 200mm
Certifications	FCC, CE, RCM, IC
Warranty	2 Years (limited warranty, review warranty for complete details)

Technical data subject to change without notice.

3541 CHALLENGER ST., TORRANCE, CA 90503 USA
PH 800.899.PCSC or 310.303.3600 PCSCsecurity.com

Credential Manager

Cloud based portal for all of your digital credentials

Safetrust's Credential Manager is a feature-rich portal used for registering users and activating devices for use within your environment. It is also used for assigning virtual credentials, over-the-air to mobile devices and activating controls (rules) around the use of those credentials. The Credential Manager can accept data from a third party trusted source, such as a Physical Access Control System, Identity Management System or HR System. The Credential Manager can be used to monitor virtual credential usage, and where required can also be configured to send event-based information to supported third-party analytics engines.

Key Features

- **Over-the air Credential Issuance:** Virtual credentials can be issued or revoked in real time to mobile devices, providing rapid deployment for all users, including those in remote locations.
- **Virtual Credential Consolidation:** Supports the issuance of virtual credentials from multiple disconnected sources into a single local user Wallet. Credentials may be issued from private or public sector entities, who maintain control over their individual assigned credentials.
- **Single mobile identity architecture:** Supports the issuance of an unlimited number of building access credentials and logical access credentials within a single platform.
- **API Integration:** Contains a feature-rich REST API for integration with third-party applications including authoritative data sources and analytics engines.

How does it work?

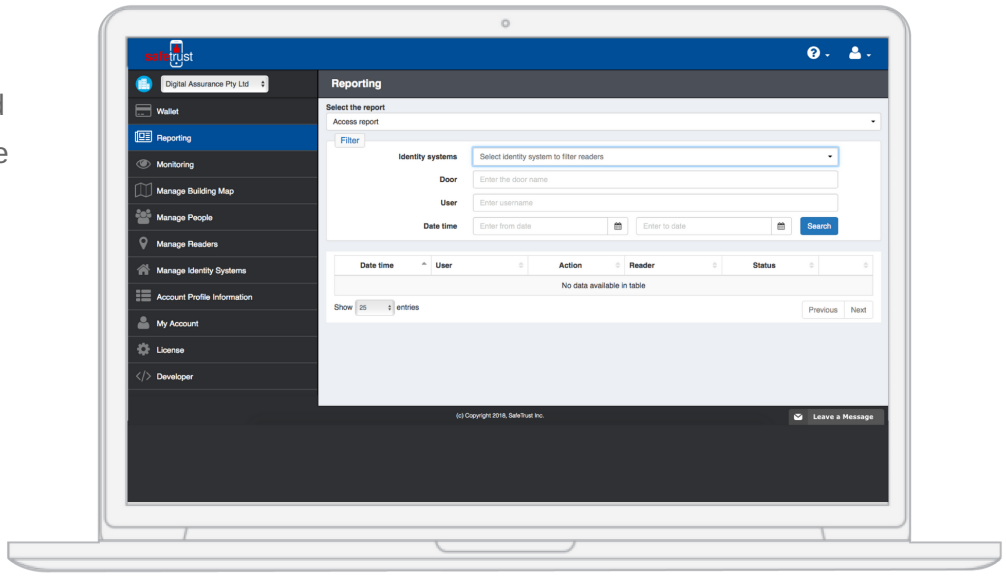
The Credential Manager supports role-based access. Customer Administrators with appropriate rights define the required identity systems for their business. Identity systems can be defined by their operational use (physical or logical), the specific credential format required, and their geographic location. Identity Systems may include either a default or custom design for the visual representation of the virtual credential, as it appears on the mobile device. Supported logical and physical access readers (IoT sensors) are registered within each identity system to ensure that only those devices and credentials associated with the specific system can communicate with each other. Registered users from the customer organisation are then assigned virtual credentials associated with one or more identity system.

Virtual Credentials are pushed to the mobile devices of the registered users that have installed the Safetrust Wallet application. These virtual credentials can include rules regarding the times/dates for when the credentials can be used, the location at which the credential can be used and the credential's expiry date. Additional rules regarding PIN or Biometric reauthentication may also be applied.

Virtual Credentials are updated in real time over-the-air, significantly reducing the cost of typical card-based deployments. Security staff no longer need to follow-up holders of temporary/visitor cards for their return as virtual credentials can be revoked with a click of a button or set to automatically expire at a given time.

How do we get started?

The Safetrust Credential Manager is available through the SafeLogon and SafeAccess starter kits which include the SABRE reader/s, a number of employee licenses (with unlimited mobile credentials), and complete step-by-step instructions. These starter kits are available through authorized local system integrators, resellers and OEM partners.



Credential Manager Specifications

Description	Cloud based Management Portal for configuration and issuance of virtual credentials to mobile device.
Access Methods	Password, Google+, FIDO, Digital Certificate
Session Management	SSL
Access Roles	Developer, Monitoring, Installer, Reporting, People Management, Update Graphics, Admin
Supported Browsers	Chrome, I.E, Edge, Firefox, Mozilla
Registration Types	User & Device

Technical data subject to change without notice.