safelogon

Your trusted mobile identity solution

Secure authentication from your mobile device

SafeLogon replaces outdated usernames and passwords with secure mobile credentials, providing convenience, high-security authentication, and information protection all in the palm of your hand.

With the SafeLogon solution, a person taps their phone against their computer to perform a safe and secure login to their desktop, active directory, web site, banking site, email, VPN or remote desktop. When the person leaves the vicinity of their computer, their sessions can be configured to log off or suspend, preventing unauthorized use.

SafeLogon uses industry standards such as NIST 800-73 to facilitate file, disk, email, and information encryption from an authorized phone. Virtual credentials stored in your mobile device can now be used to secure your business and its assets, providing a cost-effective balance between security and convenience.

Improving data-privacy and business intelligence

SafeLogon provides event-based monitoring and integration with analytics engines to allow business to gain insights into operations within their business that otherwise remain unseen. Event-based data analytics allows administrators to better understand who used a digital credential to gain access to a particular system or application, when it was used, and more importantly from where it was used. Providing valuable intelligence across the entire organization allows administrators to add additional controls where required to reduce risk. This includes geo-locking of credentials, hours of use, and biometric or PIN-based re-authentication before use.

INCREASED SECURITY

SafeLogon allows Administrators to quickly and easily increase their security by replacing outdated usernames and passwords used for network logon and application authentication with certificate based virtual credentials stored securely within a mobile device.

FAST CONNECT / DISCONNECT

SafeLogon can be configured for Credential Auto-Authenticate mode, allowing users to use their virtual credential when their mobile device is presented within a configurable activation zone. When the mobile device is removed from the activation zone, the user can be automatically logged out or have their session closed.

LIFECYCLE MANAGEMENT

With SafeLogon, virtual credentials can be quickly issued, suspended or revoked over-the-air with the click of a button. Virtual credentials can easily be replaced or updated without impacting end users, providing increased flexibility for Administrators wanting to issue short and long-term credentials

Key Features

SUPPORTS MULTIPLE VIRTUAL CREDENTIALS

SafeLogon allows users to store multiple virtual credentials that emulate the NIST 800-73 smartcard specification securely within a mobile device. Each virtual credential supports up to 4 digital certificates including a User Authentication, Signing, Encryption and Card Authentication certificate.

CONFIGURABLE AUTO-ACTIVATION RANGE

SafeLogon can be configured to support varied distances for automatic activation and deactivation that can be tailored to your needs. Distance for automatic operations are set by default to 30cm, but configurable to larger distances with the option of adjusting the sensitivity level based on a device-by-device basis. This feature can be enabled at the mobile device or virtual credential level.

TAP TO LOG ON - TAP TO LOG OFF

SafeLogon includes a Tap to Log On - Tap to Log Off feature supporting those users working in a busy kiosk type environment. Users simply tap their mobile device on the SABRE to insert their virtual credential in the computer and tap a second time to eject their virtual credential from the computer.

SUPPORTS EVENT BASED MONITORING

SafeLogon supports customer-specific event based monitoring that can be connected to your analytics engine. Event information can include who used the virtual credential, when the credential was used and where in terms of geographical location the credential used.

GEOGRAPHICAL LOCKING OF CREDENTIALS

Virtual credentials may be individually locked to a specific geographical region, whereby they are unavailable for use outside of a selected area. Regions are defined by longitude and latitude using either a multipoint polygon or a single point radius configuration.

BIOMETRIC NON-REPUDIATION

SafeLogon may be configured to work in background mode when the mobile device is locked. Access rules for virtual credentials may be used to force a user to biometrically re-authenticate to their mobile device before the specific virtual credential is released for use, further securing access to the credential.

SafeLogon starter kits are available with a SABRE reader, retail license (unlimited mobile credentials), and complete step-by-step instructions. SafeLogon is available through authorized OEM partners.