HID Mobile Access®

Information Security and Privacy Overview

PLT-02226, Rev. A.5

June 2018

Copyright

Trademarks

Revision history

Date	Description	Revision
June 2018	Annual update.	A.5
June 2017	Updates for formatting.	A.4
June 2017	Annual update.	A.3
October 2015	Updated with privacy information.	A.2
February 2015	Second release.	A.1
December 2014	Initial release.	A.0

Contacts

For additional offices around the world, see **www.hidglobal.com/contact/corporate-offices**

Americas and Corporate

611 Center Ridge Drive
Austin, TX 78753
USA
Phone:866 607 7339
Fax:949 732 2120

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong
Phone:852 3160 9833
Fax:852 3160 4809

Europe, Middle East and Africa (EMEA)

Haverhill Business Park Phoenix Road
Haverhill, Suffolk CB9 7AE
England
Phone:44 (0) 1440 711 822
Fax:44 (0) 1440 714 840

Brazil

Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP
Brazil
Phone: +55 11 5514-7100

HID Global Technical Support: www.hidglobal.com/support

Contents

Section 1: Introduction 5

Section 2: About Mobile Access security level 5

2.1 What is HID Mobile Access? 5

2.2 What is Seos? 5

2.3 Foundation of HID Mobile Access security 6

2.3.1 HID Mobile Access consists of multiple layers of security 7

Section 3: Common security related questions 10

3.1 What is a Mobile ID? 10

3.2 Is HID Mobile Access as secure as a physical card? 10

3.3 Best practice policy recommendations outside of Seos Security Framework 11

3.4 What are the differences between BLE and NFC for reader device communication 11

3.5 What personal data does the App collect? 12

3.6 What happens if I lose my device? 12

3.7 What is the security level on the Mobile device? 12

3.8 When someone downloads the HID Mobile Access App, can they use it automatically? . . 12

3.9 What should I do before reissuing the device to another user? 12

Section 4: Data protection architecture 13

4.1 We collect the following data 13

4.2 Why does HID Global collect this data? 13

Section 5: How we secure our networks 14

5.1 How we secure authentication to HID Mobile Access 14

5.2 How we build secure HID Mobile Access 14

Section 6: HID Global employees 15

6.1 Security staff 15

6.2 Legal counsel 15

6.3 Assessments 15

6.4 Policies 15

Section 7: How we build secure products 16

7.1 Design phase 16

7.2 Coding phase 16

7.3 Testing phase 16
7.4 Incident management 16
Section 8: Return of customer data and deletion 17

1 Introduction

HID Mobile Access® has introduced a new era of convenience and functionality to access control. It is a methodology for managing secure identities on mobile devices for physical access control. The HID Mobile Access solution is tailored for security professionals seeking higher levels of secure user convenience to protect doors, gates, parking facilities, networks and physical assets while having the confidence that identity data is secure and privacy is protected.

This document will serve as a reference and provide you with the information you need to understand the security characteristics in HID Mobile Access.

2 About Mobile Access security level

2.1 What is HID Mobile Access?

HID Mobile Access complements existing access control solutions, replacing key cards or fobs to get access to buildings. This access uses Mobile IDs stored and processed on a mobile device, enabling communication between a reader and a mobile device (either NFC or Bluetooth Low Energy (BLE)).

The HID Mobile Access service, powered by Seos® (see, *What is Seos?*) consists of the following components:

- HID Mobile Access Portal: A cloud-based management portal allowing user management (securely create/issue/revoke Mobile IDs for user mobile devices)
- HID Mobile Access Portal SDK: A web services interface that exposes user and credential management functions for custom applications
- HID Mobile Access App for Android and iOS
- HID Mobile Access App SDK for Android and iOS
- iCLASS SE® and multiCLASS SE® Mobile Access enabled readers
- Seos protocol and security framework
- Mobile IDs with integrated Seos technology for management of trusted identities

2.2 What is Seos?

Seos is an HID Global technology, developed as a common standard that establishes privacy and trust in the communication of secure identity data on physical cards, smartphones, tablets and wearables.

The Seos-capable Enterprise applications encompasses solutions for a broad and growing range of use cases, including PC login and authentication to IT systems, secure print job collection, automated vending, building access, opening door locks, elevator access, parking access, and time and attendance management. HID Global will continue to expand the solutions of Seos-interoperable products and services.

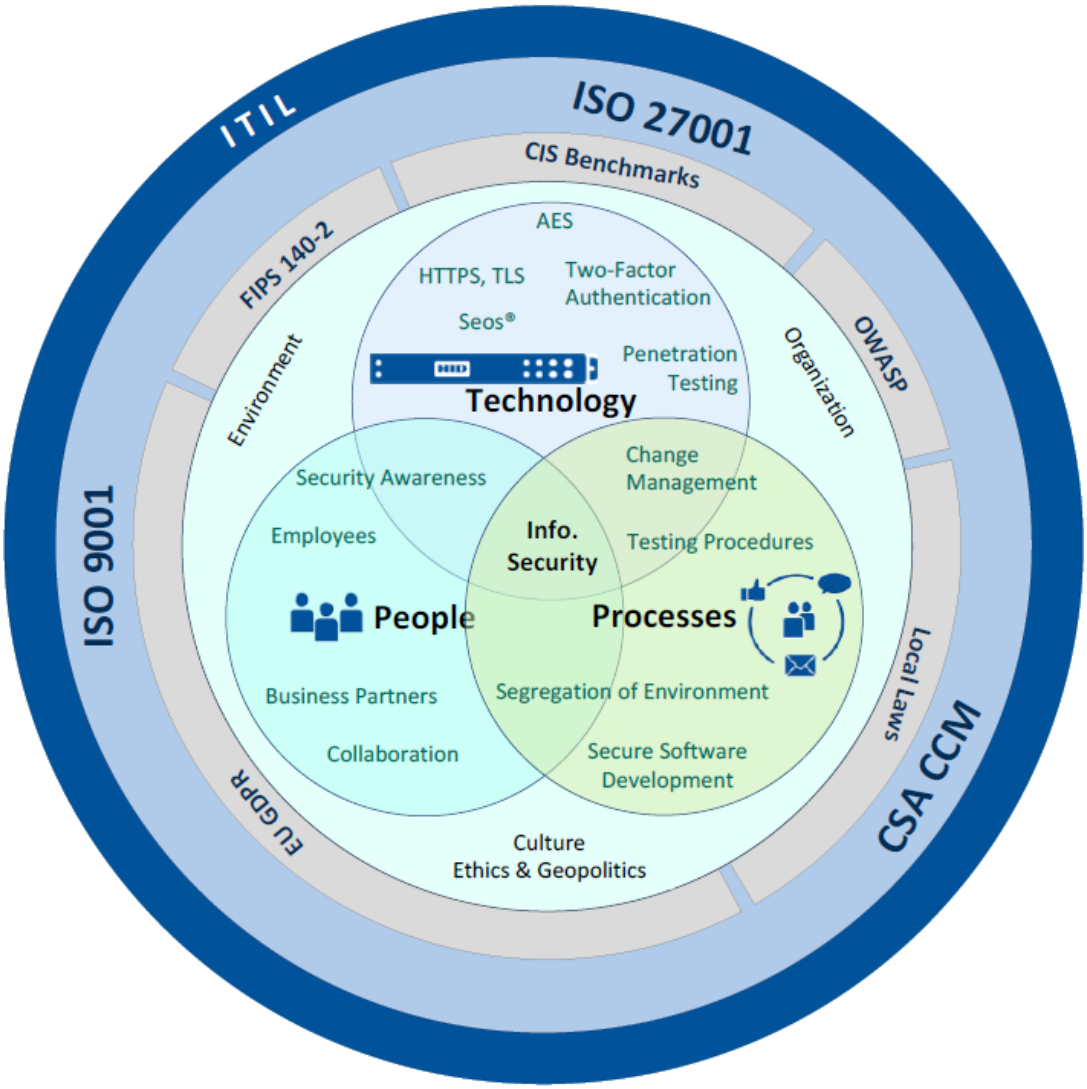
Seos technology is chip-independent, enabling easy porting across a variety of hardware devices of different manufacturing origin. Most importantly, Seos enables a smart device to become a trusted credential, replacing mechanical keys and access cards, to open doors in homes, hotels, offices, hospitals, universities, and industrial and commercial buildings. Seos technology has been widely adopted, and powers HID Mobile Access and HID Global's iCLASS SE platform.

2.3 Foundation of HID Mobile Access security

At HID, we apply a holistic approach to information security by considering all threat vectors and aspects including, but not limited to, technology, processes and people.

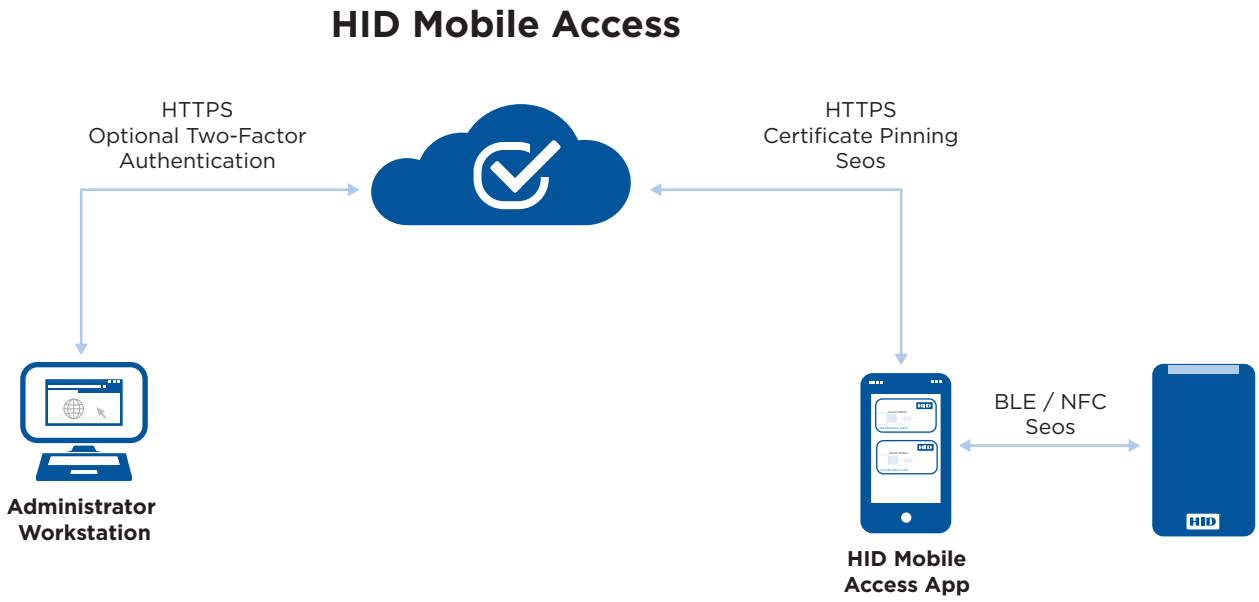
We use industry best practice guidelines, frameworks and standards, such as:

- ISO/IEC 27001 Information Security Management System
- ISO 9001 Quality Management System
- ITIL®
- Center for Internet Security Benchmarks
- OWASP
- Cloud Security Alliance Cloud Controls Matrix



HID Mobile Access - Holistic approach to Information Security:

Success is built on trust, and trust starts with transparency. HID Global is dedicated to ensuring secure access and storage for our Cloud Services. To this end, we continuously evolve our security features and processes as new best practices emerge. Additionally, HID Mobile Access is regularly subjected to security assessments and penetration testing by external security experts.



HID Mobile Access - Multiple layers of security

2.3.1 HID Mobile Access consists of multiple layers of security

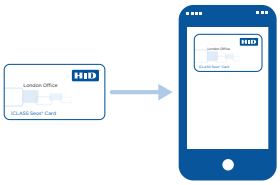
On a Mobile Device: Mobile IDs are stored in the Application Sandbox, an area within the mobile operating system which ensures file access is limited to the application embedding the HID Mobile Access SDK. Additionally, the keychain of mobile device is used to store cryptographic key information. Mobile IDs leverage **HID Secure Identity Object™** (SIO) technology, which uses strong cryptography for encryption and digital signatures. The Mobile IDs are tied to the device through a diversifier and device-specific keys (no master key), assuring it will not work on another device.

Note: The transaction between mobile device and reader is independent of the communication protocol.

Smart Security: Seos secure messaging protocol is used to secure the over-the-air communication between the device and reader (independently if NFC or BLE is used as the communication protocol). In addition, through configuration of the HID Mobile Access app, it is possible to prevent the Mobile ID from being used without first unlocking the device.

Back-end: The Mobile Access Portal processes the incoming credential payload and protects the data using the device specific diversified keys, managed and generated within Hardware Security Modules. HID Mobile Access uses the HID Secure Delivery Infrastructure to securely wrap the credential payload for secure transportation. The HID Secure Delivery Infrastructure is used for cryptographic key management and for cryptographic processing. This infrastructure and related systems are also used in the HID Global manufacturing of secure iCLASS cards, and proven to be highly secure.

Building blocks	Key security features
 **Seos Transaction**	■ Seos secure messaging protocol is used to secure the over-the-air communication between the device and reader (independently if NFC or BLE is used). Seos is not dependent on the security of the transport technology. ■ Seos is standards-based for secure messaging, strong authentication and data confidentiality, leveraging strong cryptography such as AES-128 and SHA-256. ■ Every Seos transaction is unique and cannot be cloned (recorded and replayed). Seos is resistant to man-in-the-middle attacks, reflection attacks, replay attacks, message deletion, message reordering, message modification, message concatenation and message insertion. ■ The Seos protocol supports strong privacy, meaning that it is not possible to track the identity of a device.
 **Mobile App**	■ The Seos vault used in the HID Mobile Access app includes binary protection and anti-hacking techniques for reverse engineering, tampering, unauthorized access, code injection and obfuscation. The mobile app can be configured so that the Mobile ID is only active when the screen is unlocked to prevent relay attacks. ■ The Invitation Code used to securely register trusted mobile devices has One-Time Password security. ■ All cryptographic keys are device diversified, with no master keys stored on the device. Each Mobile ID is unique per device. ■ The Mobile IDs are stored in an AES-encrypted vault in the App sandbox. ■ Mobile IDs are stored AES-128 end-to-end encrypted in an SIO which is unpacked in the secure element in the HID reader and origins from the HID Secure Delivery Infrastructure.

 **Mobile ID Over-the-Air**	■ Over-the-Air delivery of Mobile IDs is end-to-end encrypted using AES-128/CMAC96.
	■ Mobile IDs are transported via HTTPs, TLS 1.2 encryption with strong cipher suites and pinned certificates
	■ The transport service does not store and maintain any credential or access control data and is not aware of the structure and generation of the credential payload.
	■ The HID Secure Delivery Infrastructure:
	  ■ Supports Global Platform requirements, including full lifecycle tracking of every key and key use, policy enforcement and logging of all activity.
	  ■ Uses cryptographic modules certified according to FIPS 140-2.
	  ■ Is used for cryptographic key management and for cryptographic processing.
	  ■ Is also used in the HID Global manufacturing of iCLASS SE cards and readers, which are proven to be highly secure.

Building blocks	Key security features
 **iCLASS SE Reader or Embedded Module for HID Solution Partners**	■ An example of a reader for HID solution partners is a multiCLASS SE Reader with 13.56 MHz contactless smart card technology. ■ Supports BLE and/or NFC in addition as transport technology. Seos is used to secure transactions independently of transport technology. ■ No Bluetooth pairing is required between reader and device. Instead, only eligible devices can interact. The device and reader both use high-security cryptographic communication techniques to prove to the other that it is trustworthy. ■ Ensures data authenticity and privacy through the multi-layered security beyond the card technology, providing added protection to identity data using SIOs. Keys and crypto operations are contained within a secure element (EAL5+ hardware). ■ Protection from electronic hacks with velocity checking to detect brute force attacks. ■ The reader uses Open Supervised Device Protocol (OSDP) for secure, bidirectional communication.
 **Secure Storage in Cloud**	■ Authentication data, such as usernames and passwords, is stored in a HID Global ActivID® Authentication Server. ■ HID Mobile Access is certified for compliance with ISO/IEC 27001. ■ HID Global administrative staff are required to use multi-factor authentication to securely access the systems. ■ Access to HID Global servers is protected via redundant firewalls. Firewall rules are managed via standard change control processes. ■ Both production and non-production assets reside in highly professional data center environments.

3 Common security related questions

3.1 What is a Mobile ID?

Mobile ID is a credential in the form of a HID Secure Identity Object™ carried on a mobile device. This data object is transferred using the Seos protocol to a door environment (for example, reader, controller) which verifies the access permissions and either grants or denies access per the results of the check.

An SIO consists of one or more Secure Objects, including one for identification purposes.

A Secure Object is a data object consisting of:

- **Tag(s):** Data object type identifier
- **Payload:** (plain or encrypted) main use case
- **Privacy context:** if payload is encrypted and consisting of a cryptographic algorithm identifier, and a cryptographic key reference
- **Authenticity context:** consisting of a cryptographic algorithm identifier and a cryptographic key reference for the cryptographic signature of the SO

An SIO can be ASN.1 represented and coded as BER-TLV object according to ISO/IEC 8825-1.

Structure of a Secure Object (SO)

3.2 Is HID Mobile Access as secure as a physical card?

Seos® in the form of Mobile Access or processed with smart cards is more secure than legacy access cards, without processing capabilities. Seos includes modern and well-established security features to session key, non-reputation, and non-reply attacks.

The nature of a mobile device creates a higher level of security. For example, if an employee loses their physical card it can be used by anyone. The loss of a mobile device is normally noticed and reported very quickly, and until it is reported, the passcode can be used to protect usage of the Mobile ID. Through the HID Mobile Access Portal, the administrator can revoke the Mobile ID, if the device still has coverage.

3.3 Best practice policy recommendations outside of Seos Security Framework

HID recommends implementing the following policies within the Enterprise environment in combination with HID Mobile Access, as part of the IT or HR policy:

- Define and implement reporting process for loss of device and subsequent revoking of Mobile ID and disabling of Mobile ID in the Access Control System.
- Ban jailbroken devices where the operating system has been compromised. To jailbreak (or root) a device circumvents the built-in security and protection of the operating system, opening up the device for high risk from malware and unsupported uses. The HID Mobile Access Portal provides functionality to receive notifications of devices suspected to be jailbroken.
- Mandate the use of passcode or fingerprint scan as additional security mechanism against the loss of a mobile device (setting within the App).
- Use a mobile device management system to manage company devices (useful not only for mobile access, but to secure company email and other vital company information) and addresses the challenge of acquiring, distributing, securing and tracking mobile applications like HID Mobile Access app.

3.4 What are the differences between BLE and NFC for reader device communication

The use of Bluetooth Low Energy or NFC to communicate with the reader depends on the reader infrastructure installed at the premises. Seos is independent of 13.56 MHz contactless smart card technology, or mobile device over Bluetooth Low Energy. The distance set-up provides the flexibility to create a more secure surrounding (for example, set the reader on the secure side of the door). The following are the key differences between NFC and BLE:

Communication Technology	NFC (Near-Field Communication)	BLE (Bluetooth Low Energy)
Supported Operating Systems	Android 4.4+	Android 4.4+ iOS 8+
Storage of Enrolled Mobile IDs	Encoded in device operating system (host card emulation)	Encoded in device operating system
Supported Readers	iCLASS SE® or multiCLASS SE® readers (Rev E or newer)	■ New iCLASS SE or multiCLASS SE readers ■ Bluetooth Low Energy requires an additional BLE module, which has to be ordered together with the reader and fitted in factory or in the field
Transaction experience	Tap (short range, and RFID like), and ideal for: ■ Standard use case (most doors) ■ Meeting zones (many doors close by) ■ Combination security (ex. Phone + PIN) ■ Tap-in" when counting transactions is required	Tap (configurable distance, but mostly used as NFC although via BLE) Twist and Go (long range), and ideal for: ■ Car park gates and garages ■ Warehouses ■ Hidden readers in less obtrusive places. ■ Reader placed on secure/warmer side (protection against vandalism)

3.5 What personal data does the App collect?

The HID Mobile Access Apps collect certain information about the mobile device and application usage, such as the operating system version and unique identifiers for the device. This information is used to provide support and improve the services. Detailed information on the data collected and how it is used is provided in the Privacy Policy that is made available to the user during the App installation process.

3.6 What happens if I lose my device?

The mobile operating system protects data on the device, if the device passcode is enabled. However it is important that a lost device is reported to the portal administrator, so that the Mobile ID is revoked and access rights for the Mobile ID is removed in the Access Control System. HID recommends setting up an internal process for reporting lost devices.

Note: Mobile ID is not part of a phone backup. So, phone backup/restore means that the Mobile ID has been lost.

3.7 What is the security level on the Mobile device?

Seos is open and standard-based and uses multiple layers of security on the device on both Android and iOS, which are continuously updated and evolved. The App processing the Mobile ID runs in a dedicated Sandbox with sole access and ownership of its data. The Mobile IDs are stored in an AES encrypted vault in the App sandbox.

The advantages of mobile devices are the ability to dynamically update the security payload, as changing data on a card takes more time and involves additional costs. As a consequence, the mobile environment allows quick response to security issues.

In addition to the security of the mobile operating system, Seos signs and encrypts all Mobile IDs using AES and uniquely binds the Mobile IDs to the specific device. The HID Mobile Access App offers an optional setting to ensure the passcode is entered before activating the Mobile ID.

3.8 When someone downloads the HID Mobile Access App, can they use it automatically?

No, the user needs a valid Invitation Code to register the App from the manager of the access system. The personalization of the end-point is based on the unique registration code. This code can only be issued from the HID Mobile Access Portal or API, preferably to a secure corporate email address, and can only be used once. Only after the registration code has been successfully authenticated, the device is eligible to be issued a Mobile ID. HID Mobile Access will not work in your facility until the Mobile ID has been entered in the Access Control System.

HID Global strongly advises against sending registration codes to insecure email addresses, such as "free mail" accounts.

3.9 What should I do before reissuing the device to another user?

HID Global recommends performing a full factory reset of the device (to scrub its stored data) before reissuing it to another user or retiring/recycling the device.

4 Data protection architecture

HID Global utilizes some of the most advanced technology for Internet security available today. We take security seriously when it comes to storing and processing our customer's data. We regularly review how data is collected, limit the personal data we store to that which is absolutely necessary for our customers to use Mobile Access, and regularly review how data is protected to ensure the highest standards of privacy and security. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters including customers' data submitted to HID Mobile Access.

HID Global continuously reviews and updates our policies, procedures, and operational practices to align with data protection regulations in the jurisdictions where we operate, including the General Data Protection Regulation (GDPR) in the European Union (EU).

Additionally, HID Global is Privacy Shield certified to enable EU originating personal data to be securely transferred from the EU and Switzerland to the United States where our servers are primarily located.

4.1 We collect the following data

- **End users:** name, email address (for Mobile Access users)
  For end-users with Mobile Access, technical data and related information about the device being used for the Services, including unique push ID, make and model, operating system, and application software

  Note: We do not store IMEI, MSISDN or ICCID
- **Administrators:** name, email and user ID/password and phone number for additional security through two-factor authentication
- For organizations registering for HID Mobile Access, as part of the automated onboarding process, we store a shipping address and VAT number (as applicable) so we know where to send sensitive configuration cards

If we need to collect additional data or information, we will first request consent from data subject. The data, in all cases, will only be collected, processed and stored in accordance with the HID Global Privacy Policy.

HID Global does not store any sensitive personal data, government-issued identification numbers, financial information (such as credit or debit card numbers, any related security codes, and bank account numbers), information related to an individual's physical or mental health, and information related to the provision or payment of health care.

4.2 Why does HID Global collect this data?

- To manage licenses and services
- To provide software updates and support
- To fulfill HID Global legal and administrative obligations
- To enforce the HID Global Privacy Policy and the HID Mobile Access License and User Agreement
- To protect the rights, property and safety of customers and of those of HID Global

We do not sell or trade the data, or collect or use it for advertising purposes.

5 How we secure our networks

HID Mobile Access is hosted in a secure server environment and utilizes industry standard advanced security technologies to prevent interference or unauthorized access. Information stored on these secured servers can be accessed only by authorized personnel. Currently, our infrastructure is located in the United States.

HID Global maintains an Information Security Management System, certified according to the ISO/IEC 27001 standard, to govern security controls for the development and ongoing operations of the HID Mobile Access service.

5.1 How we secure authentication to HID Mobile Access

To minimize vulnerability threats, HID Global strongly recommends administrators of the HID Mobile Access portal utilize the industry best practice of two-factor authentication. Two-factor authentication requires all login attempts use both a login credential and a second authentication factor. In addition, HID Global has included a limited session timeout threshold, reducing risks created by administrators who leave computers unattended or who do not log-off. The HID Mobile Access portal automatically closes sessions after 60 minutes, if no session activity is detected.

HID Mobile Access includes a variety of security controls. These controls include:

- Unique user and device identifiers (user IDs) to ensure that activities can be attributed to the individual users
- Revocation of access after several consecutive failed login attempts
- Requiring users to change their passwords on first use
- Termination of user sessions after periods of inactivity
- Strong passwords with the ability to use two-factor authentication for enhanced security
- Audit logs, displaying a history of actions performed for a user account

To enhance security, HID Mobile Access operates in accordance with the following procedures:

- Users' passwords are stored encrypted and are never in plain text
- User access is logged, and logs are stored for a minimum of 90 days
- Passwords are not logged under any circumstances
- HID Global personnel will never request users to provide their passwords

5.2 How we build secure HID Mobile Access

HID Global's corporate culture is built on security. It starts at the very top with executives who lead teams responsible for the implementation of comprehensive information security governance policies based industry recognized security frameworks and a robust privacy program.

6 HID Global employees

All of our employees are required to complete information security and privacy awareness training. Employees who may handle data receive additional training specific to their roles as well as government security clearance (as needed).

6.1 Security staff

We have a dedicated staff of highly skilled security professionals.

6.2 Legal counsel

Our legal team coordinates with third-party experts and ASSA ABLOY, who are responsible for helping ensure that we comply with global privacy laws.

6.3 Assessments

HID Global is dedicated to the implementation of an active, analytics-driven approach to cyber security. Security testing and improvement is an ongoing activity incorporated into our vulnerability and threat assessment process. HID Global performs continuous testing on all Mobile Access solution components, and to ensure the highest possible level of security we regularly engage with external security auditors to validate our security posture. Ongoing application and system vulnerability threat assessments cover the following:

- Network vulnerability threat assessments
- Penetration testing and code review with leading, independent third parties
- Security control framework review and testing

Our commitment to ensuring security was recently noted by an external auditor who stated *"it is evident that HID Global has taken significant effort to reduce the overall risk facing the organization".*

We strongly encourage customers to take all possible precautions to prevent unauthorized access. In case vulnerabilities are discovered, they should be reported directly to HID Global.

Note: HID Global does not permit third-party vulnerability and penetration tests without prior authorization by HID Global. We have a responsibility to ensure smooth operations. Non-controlled tests carry the risk of impacting system performance negatively.

6.4 Policies

HID Global continuously works for better standards, safer contracts, and to support safe and fair contract terms and conditions for our cloud service in the public and private sector.

- Detailed internal policies dictate how we detect, investigate, and respond to security and privacy incidents.
- HID privacy policies - covers data collected about users via mobile device and web-interface. The data is stored on HID Global servers.

Secure Identity Services Portal Privacy Policy:

https://managedservices.hidglobal.com/privacy.html

HID Mobile Access Privacy Policy:

https://www.assaabloy.com/en/com/global/hid-global-privacy-policy-mobile-access

7 How we build secure products

HID Global incorporates best practices into its system development processes at all stages. Here's a summary of some of the development phases.

7.1 Design phase

Guiding security principles and required security training help ensure that our technologists make the best security decisions possible. Assessing threats to high-risk features helps us identify potential security issues as early in the development lifecycle as possible.

7.2 Coding phase

We address standard vulnerability types with secure coding patterns and anti-patterns, and use static code analysis tools to identify security flaws. We give every HID Global software release a code review and fix all security findings before our applications go live.

7.3 Testing phase

Our internal staff and independent third-party security consultants use open source tools, proprietary tools, and manual security testing to identify potential security issues.

7.4 Incident management

HID Global maintains security incident management policies and procedures and we apply appropriate root cause analysis and corrective action plans. HID Global promptly notifies impacted customers of any actual or reasonably suspected unauthorized disclosure of their respective customer data to the extent permitted by law.

8 Return of customer data and deletion

Customer data is collected, processed, stored and deleted in accordance with the HID Global privacy policies.