

HID SiPass Installation and Configuration Guide

Siemens - Mobile Access Portal Integration

v 1.7 | November 06, 2020



hidglobal.com

Document Control

Document Contributor(s)

Name	Department
Neerav Mittal	Partner Services
Sonu Singal	Partner Services
Chirag Seksaria	Partner Services

Document Reviewer(s)

Name	Department
Julian Figueroa	Partner Services

Document Revision(s)

Date	Author	Version	Description
19-11-2018	Neerav Mittal	1.1	Created Document
20-03-2019	Neerav Mittal	1.2	Updated document to include Credential Profile changes
15-04-2019	Sonu Singal	1.3	Updated document to include Database Access permission section and added MSSQL server 2016 pre-requisite
17-04-2019	Sonu Singal	1.4	Updated document to change the log level configuration. Section 3.6
30-10-2019	Chirag Seksaria	1.5	Updated document with note to include restarting service information and mandatory fields for cardholder addition. Section 3.2 and 3.5
13-01-2020	Chirag Seksaria	1.6	Updated document to include subscription changes, migration process. Section 4
06-11-2020	Chirag Seksaria	1.7	Updated document to include detailed explanation with pictures to identify all the config file properties

Related Document(s)

Reference	Author	Version	HID PS Reference	Description

i

Table of Contents

Int	roduction	3
1.1	Scope	3
1.2	Audience	3
1.3	Pre-requisites	3
Ins	stallation	4
Co	nfiguration	8
3.1	Grant Database File Permissions	8
3.2	Configuring SiPass Adapter Properties	9
3.3	Import HID Mobile Access Tab.	13
3.4	Add New Credential Profile	15
3.5	Configure Dropdown in HID Mobile Access Tab	16
3.6	Configuring SiPass Adapter Logging level	18
Re	lease Notes	19
4.1	Credential Status Field	19
4.2	Employee Number	19
4.3	Subscription License	20
4.4	Migration Process – SIS Portal to Origo Portal	20
4.5	Subscription Configuration Parameters	21
4	5.1 Configuring SiPass Adapter Properties - SiPassAdapterService.exe.config	21
4	5.2 Configuring SiPass Operation Client - Adding credential profile	21
Glo	ossary	22
Tra	ademarks	23
	Int 1.1 1.2 1.3 Ins Co 3.1 3.2 3.3 3.4 3.5 3.6 Re 4.1 4.2 4.3 4.4 4.5 4.4 4.5 4.4 Glo Tra	Introduction 1.1 Scope 1.2 Audience 1.3 Pre-requisites 1.3 Pre-requisites Installation Installation Configuration

1 Introduction

1.1 Scope

The scope of this document is to provide step by step details on how to install and configure the SiPass Mobile Access Portal Integration. The respective installer includes support two for the two HID Mobile Access environments:

- HID SIS Portal (Perpetual) and
- HID Origo Portal (Subscription) HID Origo Portal.

By default, the integration is configured to support the HID Origo Portal environment. Note: The former environment is now End of Services as of the 30 September 2020 and future releases of this integration may no longer include support for both.

1.2 Audience

The target audience for this installation and configuration guide include:

- Siemens Product Management.
- HID Global Partner Services and Global Accounts.

1.3 Pre-requisites

Below is the list of pre-requisites that must be installed prior to the installation of HID SiPass Adapter

- Windows 10 or Windows 2016 Server machine,
- SiPass integrated v2.76,
- An active organisation in the HID Origo (or HID SIS) Portal environment,
- Microsoft SQL Server 2017 Express
- SQL LocalDB 2016

2 Installation

The following steps are required when installing the SiPass HID Adapter.

1. Install SQL LocalDB 2016 on the host intended to run the adapter.

Note: The setup file is available as part of the SiPass HID Adapter installer package.

🞜 Sc	ull ocalDB.msi	
	neocure entities	

Figure 1: SQL LocalDB 2016

2. Using Windows explorer, navigate to the SiPass HID Adapater installer and launch the **SiPass HID Adapter** installer.

/ SiPass HID Adapter

Figure 2: SiPass HID Adapter

3. Click Next

		_	
		_	
Welcome to the SiPass HI	D Adapter S	etup Wizard	
The installer will guide you through t your computer.	he steps require	d to install SiPass H	HD Adapter on
WARNING: This computer program i treaties. Unauthorized duplication or result in severe civil or criminal pena possible under the law.	is protected by c distribution of thi ties, and will be	opyright law and ir s program, or any prosecuted to the i	nternational portion of it, may maximum extent
	Cancel	< Back	Next >

Figure 3: Installation Wizard -1

4

4. Click Next

률 SiPass HID Adapter	-	[×
Select Installation Folder				
The installer will install SiPass HID Adapter to the following folder.				
To install in this folder, click "Next". To install to a different folder, ent "Browse".	erit b	oelow	or cli	ck
Eolder:				
C:\Program Files (x86)\HID\SiPass HID Adapter\		Brow	/se	
[Disk (Cost	
Install SiPass HID Adapter for yourself, or for anyone who uses this o	omp	uter:		
⊖ Everyone				
Just me				
Cancel < Back		I	Next	>

Figure 4: Installation Wizard -2

5. Click Next



Figure 5: Installation Confirmation

V

6. The installation is now complete.



Figure 6: Installation Complete

7. Launch the Windows Services Manager (services.msc) and confirm that a new Windows service has been added to the Services list:.

Washington Hardware Herection		g automatic	Local system
🆏 SiPass HID MA Adapter Service	SiPass HID	Automatic	Local Service
Smart Card	Manages ac	Manual (Trig	Local Service

Figure 7: Service added

- 8. By default, the new service runs as a Local Service. It needs to run as a Windows user with administrator rights. The following steps describe how to make this amendment:
 - i. Right-click the new service and select Properties
 - ii. Select the Log On tab

SiPass HID MA Ad	apter Servi	ce Properties (Local (Compu	ter)	×
General Log On	Recovery	Dependencies			
Log on as:					
C Local System a	account ce to interac	t with desktop			
This account:	Loc	al Service		Browse	
Password:	••	•••••			
Confirm passw	ord:	•••••			
		ОК	Cancel	Apply	

Figure 8: Log On Tab

- iii. Select Browse and select a Windows user with Administrator rights.
- iv. Click OK and confirm that the change has taken affect.

3 Configuration

3.1 Grant Database File Permissions

To configure the new service with the relevant database, the **Administrator** user set in the previous step needs to be given permissions to the database files. The following are the steps required to configure these permissions.

1. Using Windows explorer, navigate to the folder where the new SiPass Adapter has been installed (default location - C:\Program Files (x86)\HID\SiPass HID Adapter):



Figure 9: Database location and files

- 2. Right-click the "HID-SiPassDb2.mdf" file and select Properties.
- 3. Go to Security Tab.
- 4. Locate the Administrator user (set in the previous steps) under the "Group or username" section.
 - i. If the user is listed, grant the user "Full Control" permissions...
 - ii. If the user is not listed, click Edit and then Add the **Administrator** user by assigning "Full Control" permissions to user.

🕝 HID-SiPassDb2.mdf Properties	>	<
General Security Details Previous Versions		
Object name: C:\Program Files (x86)\HID\Sil	Pass HID Adapter\HID-S	
<u>G</u> roup or user names:		
ALL APPLICATION PACKAGES	^	
E ALL RESTRICTED APPLICATION PACKAG	GES	
SYSTEM		
Admin (SiPass\Admin)	~	
A Juli (LETT (0 (D + 1) A Juli (LETT))	>	
To change permissions, click Edit.	<u>E</u> dit	
Permissions for Admin	Allow Deny	
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		
For special permissions or advanced settings, click Advanced.	Advanced	
OK Ca	ncel <u>Apply</u>	

Figure 10: Properties Tab

5. Repeat the above steps for the "HID-SiPassDb2_log.ldf" file.

8

3.2 Configuring SiPass Adapter Properties

To run the SiPass Adapter service successfully, certain properties need to be configured. Below are the details of the properties and steps to configure these.

- Using Windows explorer, navigate to the folder where the SiPass Adapter has been installed (default location - C:\Program Files (x86)\HID\SiPass HID Adapter).
- 2. Open the SiPassAdapterService.exe.config using any file editor.
- 3. Under the appSettings section configure the following properties:

```
<add key="ServerThumbprint" value="ServerThumbprint" />
 <add key="ClientCertificatePrincipalName" value="sipass server name" />
 <add key="username" value="sipass_username" />
 <add key="password" value="sipass_password" />
 <add key="serverName" value="sipass_server_name" />
 <add key="clientId" value="hid client id" />
 <add key="clientSecret" value="hid client secret"
 <add key="HrApiHostUrl" value="https://sipass_server_name:8745" />
 <add key="environment" value="PROD" />
 <add key="pollingTime" value="5" />
 <add key="ApiTimeout" value="180" />
 <add key="ApiVersion" value="2.0"/> <!--either 1.0 or 2.0-->
 <add key ="ApplicationId" value="HID-SIEMENS-SIPASS"/> <!--required only if ApiVersion = 2.0-->
 <add key="HeaderMediaType" value="application/hal+json" />
 <add key="AuditMessageMaxRows" value="50" />
 <add key="ClientSettingsProvider.ServiceUri" value="" />
</appSettings>
```

Figure 11: Configuration Properties

- ServerThumbprint To set this value follow the following steps:
 - Login to the SiPass integrated Configuration Client,
 - Navigate to System Tab → Client Configuration → Save Server Thumbprint →

SiPass integrated Configuration Client AP001HIDAP0001	
<u>File</u> Edit <u>V</u> iew <u>D</u> ata <u>O</u> peration <u>P</u> rogram <u>System</u> Op <u>t</u> ions <u>W</u> indow <u>H</u> elp	
📄 Data 🗛 Operation 👮 Program 📰 System 🗂 🔩 🖸 Components	de
ELN Configuration	
🦄 Initialize	
😟 Intrusion <u>A</u> rea	🗟 Client Configuration - New - 🗆 🗙
External Intrusion Area	Configurations
Elevator Configuration	Full computer name:
Door Interlocking	
Messaging +	Certificate Thumborint:
🛞 Egternal Alarm Monitoring	
Smartcard Profile Configuration	Only check thumbprint for authentication
Advanced Security Programming	Generate Self-Signed Certificate
Custom Page Design	
Client Configuration	
	Generate All Self-Signed Certificates New Save Server Thumbprint Save Delete Close

Figure 12: ServerThumbprint

- Save this file locally e.g. 'ServerThumprint.txt'.
- Open this file with a file editor,

 Copy the contents from this file i.e. 'ServerThumprint.txt' and paste the content into the following field:

<add key="ServerThumbprint" value="ServerThumbprint" />

- o ClientCertificatePrincipalName
 - Launch the Windows System properties i.e. Windows key + Pause/Break key on the keyboard.
 - Click on System protection → Computer Name tab → Full computer name



Figure 13: System Properties

Copy the content from the Full computer name field and paste this value into the following field:

<add key="ClientCertificatePrincipalName" value="sipass_server_name" />

- o username
 - Enter the SiPass Integrated Workstation login username into the following field:
 <add key="username" value="sipass username" />
- o password
 - Enter the SiPass Integrated Workstation login password into the following field:
 <add key="password" value="sipass_password" />
- serverName
 - Copy the value used for 'ClientCertificatePrincipalName' into the following field:
 <add key="serverName" value="sipass_server_name" />

o clientId

- Login to the <u>HID Origo Management Portal (https://portal.origo.hidglobal.com/).</u>
- Click on the top-right menu (denoted by the 3 vertical dots) and select Organization Administration.
- Scroll to the bottom of the page to the System Accounts section:

HID HID Origo Management Portal	Ø 9 🗄
Administration Dashboard	HID Origo Services Organization Administration
System Accounts System Accounts are used to authenticate requests to the HID Origo APIs.	ADD SYSTEM ACCOUNT
↑ User ID	Actions @
~	e în

Figure 14: Organization Administration

Copy the User ID from above and paste into the following field:

```
<add key="clientId" value="hid_client_id" />
```

- o clientSecret
 - The clientSecret will be the password set for the above User ID in the HID Origo Management Portal. Note: If you are unsure of this value, please reset this through the Management Portal.
 - Enter the password value into the following field:

```
<add key="clientSecret" value="hid_client_secret"
```

- HrApiHostUrl
 - Copy the value used for 'ClientCertificatePrincipalName' into the 'HrApiHostUrl' value field prefixed with 'https://' and appending port 8745 to the end e.g. https://<FQDN>:8745

<add key="HrApiHostUrl" value="https://sipass_server_name:8745" />

- environment
 - The default value for this property should be PROD. Note: If the adapter is being used against the HID Origo Pre-Production or HID Origo Partner Integration Environment, then set this value to TEST. This property should only be changed from the default value when development testing is being undertaken by HID Global Partner Services or Siemens Product Management.
- ApiVersion
 - This property value should be set to 2.0 indicating the integration of the 2.0 version API in use with the HID Origo Portal.
- ApplicationId
 - This property value should be set to HID-SIEMENS-SIPASS. Note: This property should only be modified to an alternative value when instructed by HID Global Partner Services.

API version used is 2.0]

Dashboard.]



Important: [On installation, default value set for 'Environment' is 'PROD' and 'ApiVersion' is '2.0']

Important: [On installation, default value set for 'ApplicationId' is 'HID-SIEMENS-SIPASS'. This is only applicable if the



Important: [The 'clientID' and 'clientSecret' values will vary from one end user organization to another and will be site specific. In the case of an end user organization using the HID SIS Portal, when the API has been enabled against that respective organization, the ability to define System Accounts (User ID/Password) becomes available under the Administration tab. The same values should be set here to allow the adapter to authenticate to the Portal API. If the end user organization is using the HID Origo Management Portal, values for these should be obtained from the Administration



Important: [Whenever 'SiPassAdapterService.exe.config' file values are changed; the SiPass Adapter Service requires a restart to load respective values into the service]

3.3 Import HID Mobile Access Tab

- 1. Launch the SiPass Integrated Configuration Client.
- 2. Under System → Custom Page Design
- 3. Click on Import Pages to launch the Custom Page Designer:

Advanced Control Definition HID Mobile Access High Level Bevator Personal Tracking Vehicle Visitor Definition Visitor Details Visitor Manag Work Groups	gement Porter Attachment A Label Image
	Choose
Ringer Prints	Delete Selected Object:
	Properties
Smart Card Data Profile Profil	Appearance Label Advanced Behavior Page Number 2 Page Size 860, 640
General Data	Vidth 860 Pages Used Cardholder And V
	Appearance

Figure 15: Importing Custom Page

4. Using Windows explorer, navigate to the SiPass HID Adapter installer and select the **HIDMobileAccess_Custom Page,xml** provided with the installer:

Name	Date modified	Туре	Size
🛃 HID PS - Installation and Configuration G	4/17/2019 1:41 PM	Adobe Acrobat D	929 KB
HIDMobileAccess_CustomPage.xml	1/25/2019 2:26 PM	XML Document	10 KB
📚 setup.exe	4/17/2019 10:57 A	Application	763 KB
🕼 SiPass HID Adapter.msi	4/17/2019 10:57 A	Windows Installer	2,554 KB

5. Launch the SiPass integrated Operation Client,

6. Confirm that the HID Mobile Access tab is now visible under the Cardholder record:

Cardholder									
finition Advance	ed Personal Vehicle	Tracking Control	HID Mobile	e Access	Imaging				
ardholder Identifica	ation Last Name	1			First Nan	ne			Sourch
	Employee Number					view Modification	History		Next >
	Workgroup			~		Define Workg	oup		< Previous
Credentials									
Card Number		Credential Profile	PIN	Void	Start Date	End Date	PIN Error Disabled		Add
		Base			11/19/2018	11/19/2118			Delete
									Credential Profil
Start Date End Date Status	11/19/2018		Sup	ervisor ate 3 Exclusio	n	Void Cardł	nolder rize Exclusion tv		
Access Control							9		
Name		A Time Sche	dule		Start	Er	nd	Control Mo	Access Privileo
<								>	
	0	Pond & Sonrah				N	Sava	Delete	Class
Read 💌	Assign	neau a Search			8	INEW	Jave	Delete	Close

Figure 16: Custom Page Imported Successfully

7. Select the HID Mobile Access table and confirm that the following fields are visible:

🔊 Cardho	older												\times
Definition	Advanced	Personal	Vehicle	Tracking	Control	Siemen	is Corporate (Card HID N	Nobile Access	Imaging			
Creden	tial Actions												
	Issue			~				Credential				_	
	Credential							status					
Read	*	Assign	+	Read &	Search	-			N	ew	Save	Delete	Close

Figure 17: Imported Custom Page

3.4 Add New Credential Profile

- 1. Launch the SiPass integrated Operation Client.
- 2. Launch the **Cardholder** Screen,
- 3. Click on the Credential Profile button:

💧 Cardhol	lder													×
efinition /	Advanced	Personal	Vehicle	Tracking	Control	HID Mo	bile Access	Ima	ging					
Cardholder	Identificatio	on												
	I	Last Name							First Nar	ne [Searc <u>h</u>	
	1	Employee N	lumber						١	View Modification	History		Next >	
		Workgroup					~			Define Workg	roup		< Previous	
Credentials	5													
Card Nur	mber			Credential	Profile	PIN	Void	Star	t Date	End Date	PIN Error Disable	ed	Add	
				Base				11/	19/2018	11/19/2118			Delete	
													Credential Profi	file

Figure 18: Credential Profile

4. Add a new **Credential Profile** with Name matching the corresponding part number from the HID Origo Management Portal that you intend to issue. When viewing the list of available Mobile IDs in the HID Origo Management Portal, this is referred to as the Part number API. Note: It is important that both values match exactly. If they do not match, then Mobile credential issuance is likely to fail.

Credentiale Cardholder's Credential Profile						×
Name	Card Technology	Facility Code	Validity Code	PIN Mode	PIN Digits	In Use
Base	HID Proximity 36 Bit Asco	0	0	CARD AND PIN	6	X No
CRD633ZZ-TST0025	HID Proximity 36 Bit Asco	0	0	CARD	0	🗸 Yes
Add Delete					OK	Cancel

Figure 19: Add new credential profile

3.5 Configure Dropdown in HID Mobile Access Tab

- 1. Launch the SiPass integrated Operation Client.
- 2. In the Navigation pane, expand Imported Data:

😪 SiPass integrated Operation Client SiPassAda	pter2 - [Live Audit Trail - A]
🖳 File Edit View Options Window Help		
🛅 New 🔹 🎯 Log Off 🌚 Exit 🚽 Save 🛕	Print Preview 🎒 Print	P Fir
Navigation	Unit Date Occur 🔺	Unit
Navigation SiPass integrated Operation Client My favorites Alam Queue Cardholder & Access Management Image: Cardholder & Access Management Site Plans Audit Trail Logs Image: Customized Reports Predefined Reports Imported Data Watchlists Look Up Table Listed Company Visitor Profile Log Book Subjects HID Credential Type High Level Elevator T&A Calculation DVR Message Queue	Unit Date Occur	Unit 09:00 09:01 09:01 09:10

Figure 20: Configure Dropdown

- 3. Select HID Credential Type.
- 4. Add the Credential Profile names in Column 1 as shown below:



Figure 21: Add Credential Profile Names



Important: [*Email ID and Part number are mandatory fields to be entered/selected while adding a cardholder for the SiPass Adapter Service to process the MobileID for the respective cardholder. If these are not available, then issuance of the Mobile credential is likely to fail.*]

17

xvii

3.6 Configuring SiPass Adapter Logging level

By default, the log level of the HID SiPass Adapter is set to "INFO" (informational messages that highlight the progress of the application at coarse-grained level) and logs can be found under "C:\Program Files (x86)\HID\SiPass HID Adapter\Log".

- 1. For fine-grained informational events that are most useful to debug an application, modify the log4net.config file as follows:Using Windows explorer, navigate to the folder where the SiPass Adapter has been installed (default location C:\Program Files (x86)\HID\SiPass HID Adapter).
- 2. Open the log4net.config file in a file editor,
- 3. Update level value to "DEBUG":

```
<root>
```

```
<level value="DEBUG" />
<appender-ref ref="Console" />
<appender-ref ref="RollingFile" />
</root>
```

4. Use Windows Services Manager (services.msc) to restart the SiPass Adapter Service.

4 Release Notes

4.1 Credential Status Field

SN	Action	MA Portal	SiPass - Credential Status Field
1	Issuance of an invitation code	Invitation Active	
2	Invitation code is actioned by the cardholder	Invitation Code Redeemed	ISSUING + Part Number
3	When the credential container is created	Ready for Mobile ID	
4	Credential Status on MA portal	Delivering Mobile ID	
5	When the Invitation Code expires	Invitation Expired	EXPIRED CREDENTIAL
6	When the credential is delivered	Mobile ID Delivered	ISSUED + Part Number
7	When the credential is triggered for delete	Revoking Mobile ID	REVOKED
8	When credential is deleted	Mobile ID Revoked	
9	Credential issuance but no email address supplied (Only part number selected)	(Not Applicable)	FAILED
10	Credential issuance but email address already exists in Portal	(Not Applicable)	FAILED
11	General communication error during issuance	(Not Applicable)	FAILED

4.2 Employee Number

Within the HID Origo Management Portal, organisations may define enrolment settings to define which fields are required as part of the Mobile credential issuance. When fields are set as mandatory, these fields must be captured for the cardholder prior to issuing that cardholder a Mobile credential.



Figure 22: Enroll Settings



Important: [Employee number is not mandatory]

By default, to issue Mobile credentials through HID Origo, the cardholder must have First name, Last name and Email address set i.e. mandatory fields. If the User ID field is set as mandatory within the settings of that organisation under the HID Origo Management Portal, then the cardholder Employee number field becomes mandatory. For such organisations that choose to have the User ID captured in the HID Origo Management Portal, if the Employee number is not set within SiPass integrated prior to issuance, then Mobile credential issuance will fail.

4.3 Subscription License

The following sections are additional considerations and configuration items that should be noted if the end user organization is using HID Origo/Subscription user licenses:

HID Global have introduced a new service for the fulfilment of Mobile Identities as part of their HID Origo offering. HID Origo user licenses are available as part of a subscription. The subscription model ensures that the customers are provided with an unlimited number of Mobile credentials for the duration of the subscription to cover the needs of their user base.

This release of the SiPass HID Adapter provides the following level of support for HID Origo Portal (subscription model):

- 1. Supports credential issuance,
- 2. Supports credential revocation,
- Does not handle license state management i.e. will not notify SiPass or the end user of the current status of the subscription or licenses,
- 4. Does not check the available user licenses prior to user creation,
- 5. Does not include any period state handling i.e. notifying SiPass or the end user if the subscription has not yet started or lapsed.

4.4 Migration Process – SIS Portal to Origo Portal

Plan for End-User Organization Migrations to Support HID Mobile Identities

The below is a recommended process for migrating end-user's organizations from the legacy HID SIS Portal to the HID Origo Portal. The following process only applies to customers who are not already on the HID Origo Portal environment.

- Update End-Users existing software with new HID Origo Mobile Identities integrated solution that provides support for both HID Origo X and 2.X API
- 2. End User is on 1.X API
- 3. Place Subscription order for End-User Organization to migrate from Perpetual to Subscription
- 4. End-User organization is migrated from to HID Origo Mobile Identities Platform
- 5. Update configuration in HID Mobile Identities Custom integrated solution so end-user is now using 2.X API **Important**: [API 1.0 on the HID Origo Mobile Identities Platform should only be used temporarily to migrate users over to the new organization. Technology Partners must migrate to the 2.0 API to continue to receive new fixes and features.]

4.5 Subscription Configuration Parameters

4.5.1 Configuring SiPass Adapter Properties - SiPassAdapterService.exe.config

- To run the service successfully, certain properties need to be configured.
 - API version = 2.0
 - Application Id = HID-SIEMENS-SIPASS (By default the value will be available in the file)
- Below are the steps to configure these properties

1. Go to the folder where SiPass Adapter has been installed (Default Location - C:\Program Files (x86)\HID\SiPass HID Adapter)

- 2. Open SiPassAdapterService.exe.config
- 3. Under the appSettings section configure the properties



Figure 23: Configuration Properties

4.5.2 Configuring SiPass Operation Client - Adding credential profile



- **Important**: [Once migrated from SIS portal (Perpetual) to HID Origo portal (Subscription), part-number name may change on the HID Origo Portal.
- Post migration, if there are new part-numbers updated on the portal, then add the respective part number in 'Credential Profile' and 'Configuring dropdown' in **SiPass Operation Client** as shown in 3.4 and 3.5 section above.]

5 Glossary

Acronym	Description
Card Number	The serial number identifying the HID Mobile Access Mobile ID
HID Mobile Access SIS Portal	A Web Portal that allows end user administrators to configure Mobile Devices and manage the Mobile IDs
HID Mobile Access SIS Portal API (Perpetual)	The Web Service interface for the HID Mobile Access SIS Portal
HID Origo Mobile Access Portal (Subscription)	A Web Portal that allows end user administrators to create users, configure Mobile Devices and manage the Mobile IDs
HID Origo Mobile Access Portal API	A cloud API that provides the integration interface to the HID Origo platform and will replace the HID Mobile Access API 2.0+
HID SiPass Mobile Access Service	A custom application developed by the HID Professional Services team to manage the lifecycle management between the SiPass System and HID Mobile Access SIS Portal
Invitation Code	A hexadecimal code sent to new users to initiate the Mobile ID registration and assignment process for the SiPass User
Credential Profile	In SiPass, the Credential Profile represents a User's Credential
Mobile ID	In HID Mobile Access, a Mobile ID represents a Mobile Credential assigned to the Mobile User that is stored on Mobile Device
Cardholder	A user in SiPass system being issued a Mobile ID
Part Number	A Part Number refers to a type of Mobile ID available for issuance for a given organization. One organization may have one or many Part Numbers available for selection. The Part Numbers available for an organization are listed in the 'Available Mobile IDs' section in the portal. Each Part Number has a reference, such as 'MOBILE-ID_FTPN_1000' or 'CRD633ZZ-01234', which is referenced when requesting issuance of Mobile IDs.
Application Id	Application Id (Application Identifier) is provided once an application has been certified through HID
API Version	Application Programming Interface version
Expired Credential	Cardholder sent a credential through invitation code. Credential status will change as 'Expired credential' if the cardholder does not redeem the invitation code and the code expires.
Revoked Credential	Cardholder issued with a credential. Credential status will change as 'Revoked', if the operator deletes the credential for a user.

6 Trademarks

HID GLOBAL, HID, the HID logo, 4TRESS, ActivIdentity and ActivID are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein are the trademarks of their respective owners. Any rights not expressly granted herein are reserved.



Americas EMEA +44 Asia Pacific

+1 512.776.9000 +44 (0) 1440.714.850 +852 3160.9800

Corporate Headquarters

611 Center Ridge Drive Austin, TX 78753 U.S.A www.hidglobal.com



hidglobal.com