

# Product Architecture

This section describes the product architecture and its logical components. Understanding the logical units of the application should help you with designing the actual implementation of the product to meet the deployment and security requirements of your organisation.

In this guide we use the term **server** for any software component that can be accessed via a client application, in a standard client/server architecture. To avoid any confusion we use the term **physical server** when referring to the hardware itself.

## Internal Components

### Main Components

The main components of ActiveAccess are:

- [Access Control Server](#)
  - Authentication Server
  - Verify Enrolment Server
  - Challenge Server
  - RMI Server
  - AHS Client
  - Rules Engine
  - External Messaging Adapter
  - Risk Engine Adapter
  - Out of Band Authentication Adapter
- [Administration Server](#)
- [Registration Server](#)
- [Enrolment Server](#)
- [Database Server](#)

Server components are implemented as servlets that can be deployed to any one of the commercial application servers supported by ActiveAccess.

## Access Control Server (ACS)

ACS is the authentication component of the system. It provides a facility allowing communication and messaging with other authentication components during an authentication.

ActiveAccess ACS supports **3-D Secure** and **ActiveDevice protocols**.

**3-D Secure 1** is an authentication standard for online eCommerce transactions introduced by Visa and adopted by Mastercard, JCB, American Express and Diners Club International.

**3-D Secure 2** is an update of the 3-D Secure 1 authentication standard, created by EMVCo to support app-based authentication and integration with digital wallets, as well as a frictionless authentication flow.

**ActiveDevice** is a device agnostic protocol for strong authentication of online users, which uses a variety of two-factor authentication techniques.

### Authentication Server

Default port: Determined by the application server

Default path: Refer to the table in [Access Control Server](#)

Protocol: HTTP/HTTPS

Inbound connections: Directory server

Outbound connections: Database server

**Other requirements:** Must be able to access the HSM

The authentication server is used for user authentication in 3-D Secure and ActiveDevice processes. The user is redirected to the authentication server by the merchant plug-in during the 3-D Secure process and by the ActiveDevice plug-in in the two-factor authentication. The authentication pages are stored in the database and served via the authentication server itself.

The authentication server is responsible for processing of the PAREq and generation of PAREs message pair in the 3-D Secure process.

The authentication server is responsible for processing of the UAREq and generation of UAREs message pair in the ActiveDevice process.

### Verify Enrolment Server (3DS1)

Default port: Determined by the application server

Default path: Refer to the table in [Access Control Server](#)

Protocol: HTTP/HTTPS

Inbound connections: Directory server, DPI (ActiveDevice Plug-In)

Outbound connections: Database server

Other requirements: Must be able to access the HSM

The verify enrolment server is used in the 3-D Secure 1 and ActiveDevice processes. The verify enrolment server consumes VEReq and UEReq messages and generates VERes and UERes messages accordingly.

Note that any changes to the fully qualified URL of the verify enrolment server must be reported to the 3-D Secure 1 providers in order to update the corresponding directory servers.

### **Challenge Server (3DS2)**

Default path: /acs/ca

Inbound connections: User's browser, 3DS SDK app

### **RMI Server**

Default port: 4242 and 4241

Protocol: JRMP (TCP) | <sup>1</sup>

Inbound connections: Other ActiveAccess RMI servers, MIA

Outbound connections: Database server, Other ActiveAccess RMI servers

Other requirements: Must be able to access the HSM

The RMI server is used to synchronise a cluster of ActiveAccess servers. This is mainly to notify other ActiveAccess servers of changes in the settings of the cluster or to apply settings to multiple ActiveAccess servers from a single ActiveAccess administration interface.

RMI server is used when ActiveAccess components are deployed on multiple servers or multiple ActiveAccess servers are used for load balancing.

### **AHS Client (3DS1)**

Default port: N/A

Default path: N/A

Protocol: HTTPS

Inbound connections: None

Outbound connections: Authentication history server, Database server

Other requirements: Must be able to access the HSM

In accordance with 3-D Secure 1 specification, a copy of transaction response (PAREs) must be sent to the card scheme's designated server known as the Authentication History Server (AHS). The AHS client is responsible for sending the transaction record (PATransReq) to the designated AHS server.

Note that some 3-D Secure providers may not require or support an AHS.

## **Rules Engine**

Default port: None

Default path: None

Protocol: None

Inbound connections: None

Outbound connections: Database server

Other requirements: None

The Rules engine is used for applying business rules for checking authentication requests processed or transparently authenticated by local or remote authentication servers.

Authentication exemption rules for local and remote authentication servers are:

- Soft Launch List
- Merchant Whitelist
- Merchant Watchlist
- Location Watchlist
- Domestic & International Transaction Amount Threshold
- Stand-In Transaction Threshold (remote authentication model)

Registration enforcement rules for local authentication servers are:

- Amount Threshold
- Merchant Blacklist

### **External Messaging Adapter**

Default port: N/A

Default path: N/A

Protocol: HTTP/HTTPS

Inbound connections: N/A

Outbound connections: Centralised Authentication and Authorisation Service (CAAS), Database server

Other requirements: Must be able to access the HSM

The external messaging adapter manages the messaging requirements for connecting ActiveAccess to the issuers' remote systems.

### **Risk Engine Adapter**

Default port: N/A

Default path: N/A

Protocol: N/A

Inbound connections: N/A

Outbound connections: RESTful RBA adapters

Other requirements: N/A

The Risks engine is used for applying risk rules for checking authentication requests processed or transparently authenticated by local or remote authentication servers. In an authentication, a challenge may be necessary because the transaction is deemed high-risk, e.g. above certain thresholds.

For risk assessment, ACS sends/receives proper data elements to/from risk assessment systems via middleware.

There are two types of risk adapters available:

- Native API version of Risk Adapter
- Restful API version of Risk Adapter

### **Out of Band (OOB) Authentication Adapter**

Default port: N/A

Default path: N/A

Protocol: N/A

Inbound connections: N/A

Outbound connections: RESTful OOB adapters

Other requirements: N/A

The OOB is challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow.

ActiveAccess performs Out Of Band (OOB) challenges through OOB adapters. OOB adapters connect the existing OOB authentication system with ActiveAccess. During 3-D Secure 2 challenge flows where OOB authentication is required, the ACS will trigger the external OOB process, perform interactions with the cardholder via the OOB adapters.

For this purpose, the ACS communicates with the existing OOB system via a middleware. This middleware is the OOB adapter. The OOB adapter can either be loaded locally by the ACS (Native API) or communicated with via HTTP calls (REST API).

## **Administration Server**

The management and reporting utility for the system is the administration server used by administrative users.

Default port: Determined by the application server

Default path: /mia/

Protocol: HTTP/HTTPS

Inbound connections: Administrator browser (Issuers admin staff and internal admin staff)

Outbound connections: Database server, Registration Server, RMI Server

Other requirements: Must be able to access the HSM

The administration server is used by technical and issuer and helpdesk staff who are in charge of operations, maintenance and customer support. The administration server allows access to various system and business settings, and cardholder and user information, transactions, reports and logs.

## Registration Server

A web service providing issuers the ability to enrol cardholders in real-time with the authentication schemes.

Default port: Determined by the application server

Default path: /registration/

Protocol: HTTP/HTTPS

Inbound connections: Issuer's registration software (such as Card Loader utility), Administration server

Outbound connections: Database server

Other requirements: Must be able to access the HSM

The registration API is used by issuers to register users (pre-registration and final registration models).

## Enrolment Server

A fully customisable enrolment website, which allows cardholders to enrol their cards with the authentication schemes.

Default port: Determined by the application server

Default path: /enrolment/

Protocol: HTTP/HTTPS

Inbound connections: User's browser

Outbound connections: Database server

Other requirements: Must be able to access the HSM

The enrolment pages are stored in the database. These pages are customised per issuer. The enrolment server uses XSL to combine issuer's customised look and feel and enrolment process with the cardholder enrolment and authentication criteria provided as XML.

The enrolment server is only used for enrolment of pre-registered cardholders with static password to allow them to participate in authenticated e-commerce transactions via 3-D Secure 1 protocol.

## Database Server

Default port: 1521

Default path: N/A

Protocol: TCP

Inbound connections: Authentication server, Verify enrolment server, RMI Server, AHS Client, Rule Engine, External Messaging Adapter, Administration server, Registration server, Enrolment server.

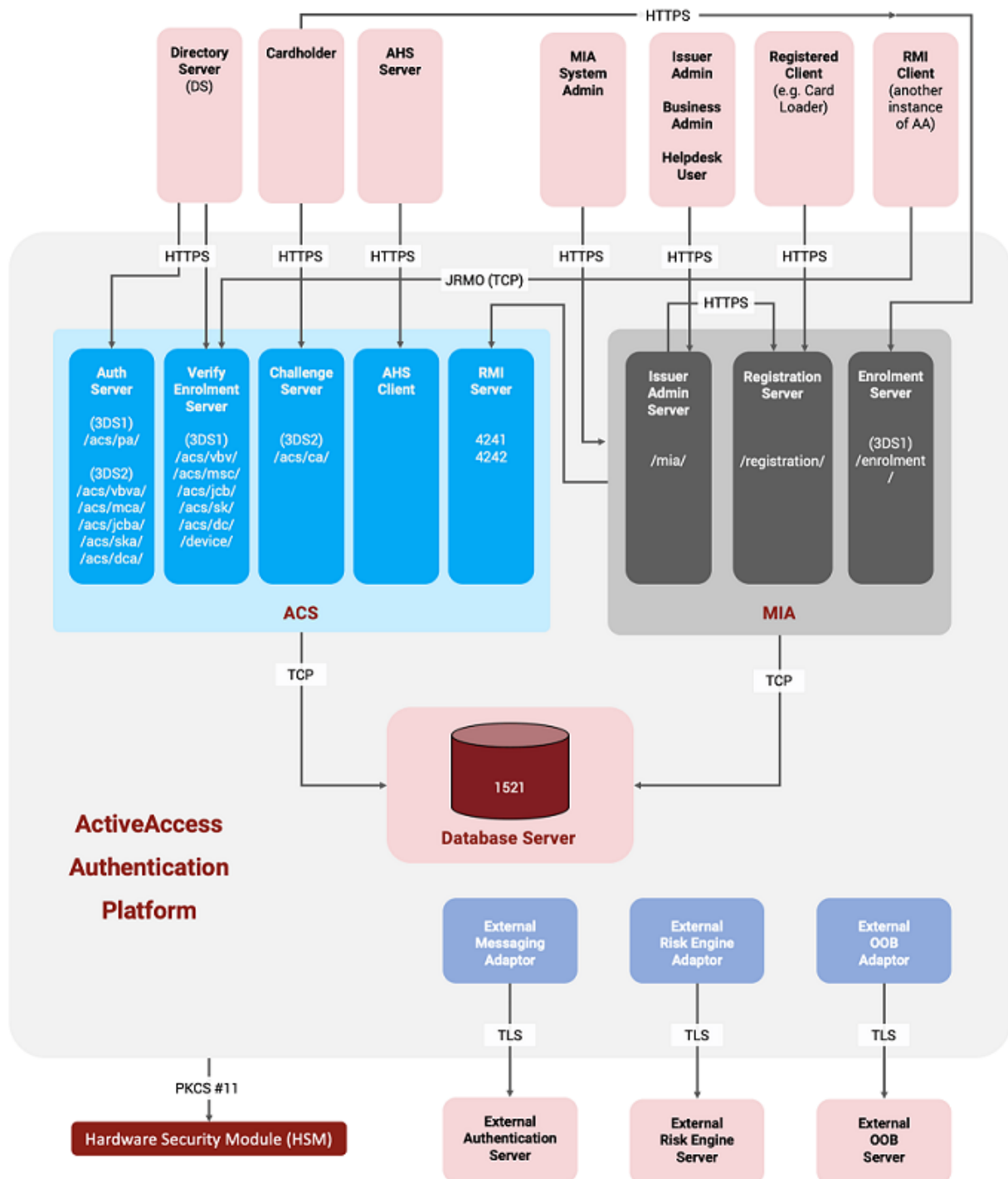
Outbound connections: None

Other requirements: None

## Logical View of ActiveAccess

The following diagram displays the logical view of ActiveAccess with the components explained earlier on this page.

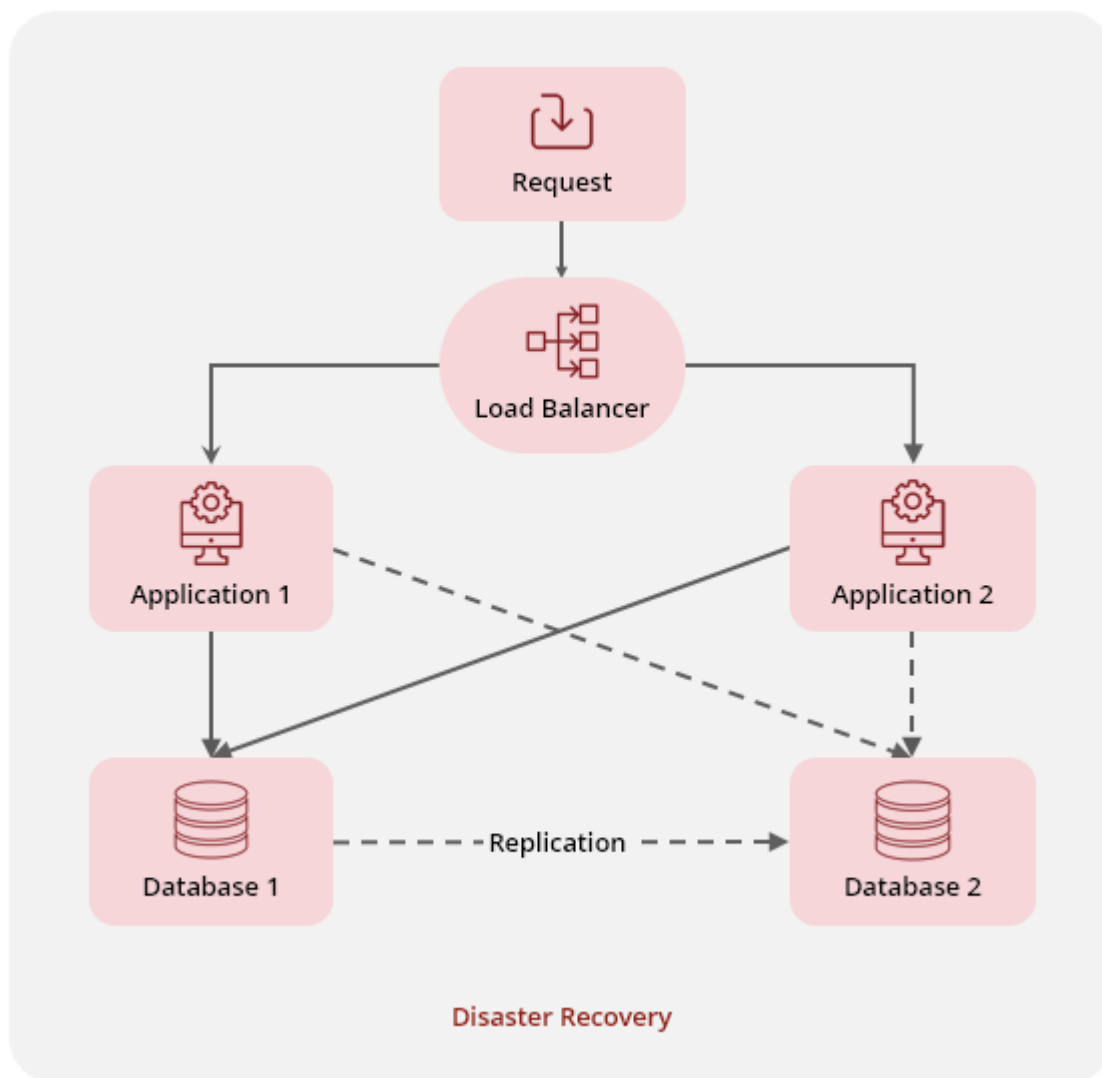




## Production Setup with Disaster Recovery

In this setup, the ActiveAccess application is setup on Application 1 and Application 2 servers, using one database server (Database 1). Requests sent to the ACS will be forwarded to the Application servers (Application 1 and Application 2), as configured by the load balancer.

Both Application 1 and Application 2 servers will use Database 1. Database 2 is a replication of Database 1, and is on stand-by. If connection to Database 1 fails, Database 2 will be used.



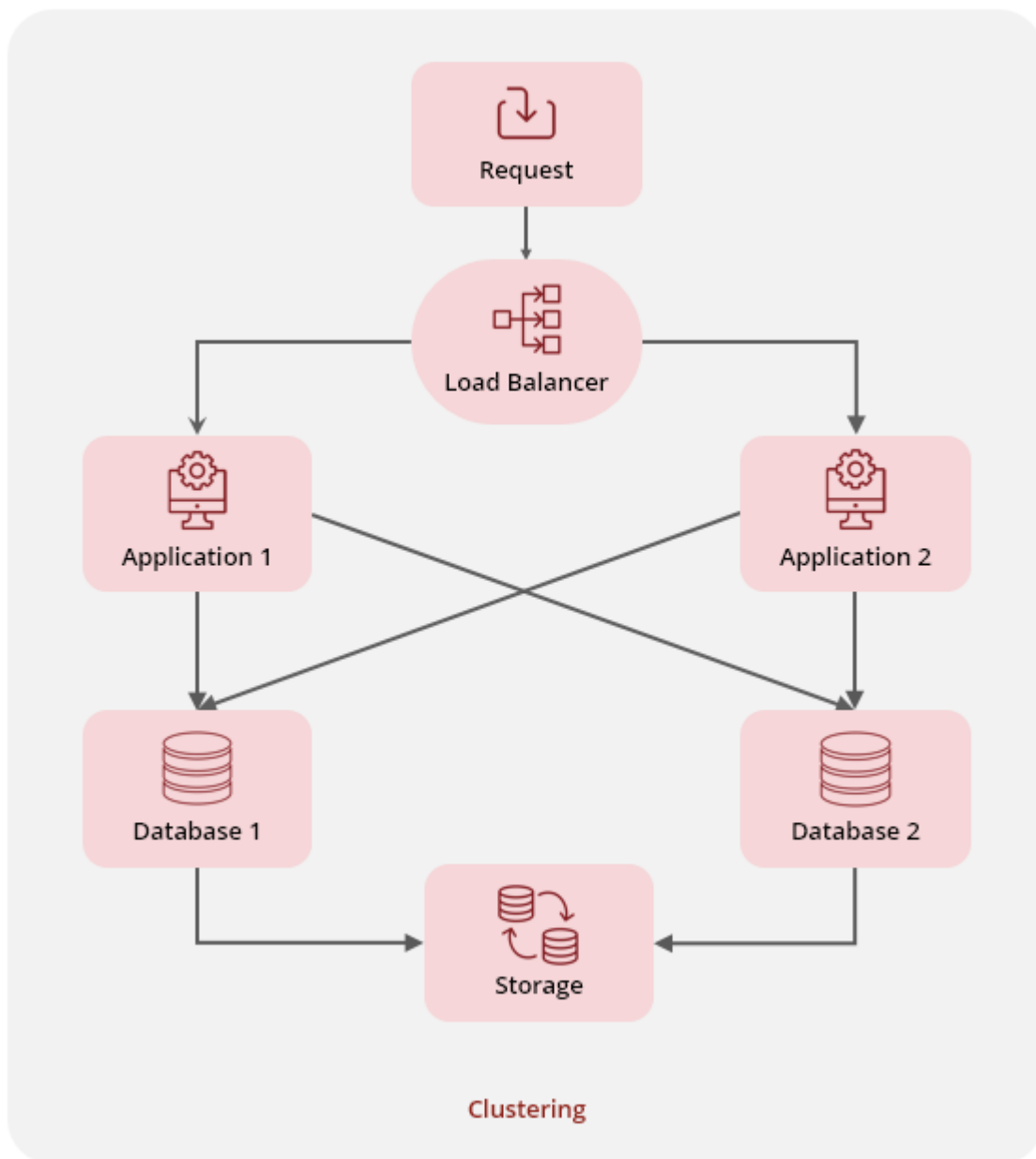
## Production Setup with Clustering

In this setup, the ActiveAccess application is setup on Application 1 and Application 2 servers, using two database servers (Database 1 and Database 2) which share the same storage. Requests sent to the ACS will be forwarded to the Application servers (Application 1 and Application 2), as configured by the load balancer.

All application and database servers are active. Application 1 and Application 2 servers will use Database 1 and Database 2 based on the configurations and their ability to establish a connection.

### Info

Oracle RAC can be used for the database clustering.



## Hardware and Software Requirements

### Minimum Hardware Requirements

#### Processor

- Intel® Xeon® X5550, or equivalent
- 16GB RAM

**Minimum Hardware Requirements****Hardware Security Module (HSM)**

- PKCS #11 enabled General Purpose HSMs (with the latest PKCS #11 driver as recommended by the HSM vendor)
- Sun JCE (for testing purposes)

**Software Requirements****JDK**

- Oracle JDK 1.8
- OpenJDK 1.8

**Application Server**

- Java Application Servers compatible with Servlet specification 3.0 (e.g. Tomcat 7.0.x and later)

**Database**

- Oracle 11g
- Oracle 11gXE
- Oracle 12c

- 
1. A proprietary wire-level protocol designed by Sun Microsystems to transport Java RMI. JRMP serves the same function as IIOP, but also supports object passing. It is also referred as the "RMI transport protocol" for Java

# External Components

## Installation of External Components

### External Components

- [Java Development Kit \(JDK\)](#)
- [Hardware Security Module](#)
- [Application Server](#)
- [Oracle Database](#)
- [Two-Factor Authentication Devices](#)

### Java Development Kit (JDK)

JDK can be freely downloaded from Sun Microsystems at <http://java.sun.com/>. JDK must be installed with the default settings. Follow the on screen installation instructions for the JDK to complete the installation.

ActiveAccess and ActiveAccess+RuPay require the installation of Oracle JDK 1.8 or OpenJDK 1.8. It is generally advisable that you install the latest minor version within a supported JVM.

You must only use one of the specified JVM versions. This is referred to as a compatible JDK in this document. Note that a newer version of JVM may not necessarily be backward compatible.

### Hardware Security Module

ActiveAccess supports PKCS #11 Cryptographic API. For installation of the HSM module, please refer to your HSM manual.

#### Note

For testing purposes, you can use the Sun JCE provider, available during setup.

## Installing the HSM module

- The path of the PKCS #11 library file will need to be specified during ActiveAccess installation.
- The slot number must be selected during ActiveAccess installation.
- The PIN created during the installation of your HSM will be required during ActiveAccess installation.

### Thales e-Security HSM

If you are using a Thales e-Security nShield HSM, the environment variable `CKNFAST_OVERRIDE_SECURITY_ASSURANCES` is required to be set for key generation.

#### LINUX

- Edit the startup file (`~/.bashrc`)
- Add the following to the end of the file:  

```
export KKNFAST_OVERRIDE_SECURITY_ASSURANCES=all
```
- Save and close the file.
- Load the startup file using the following:  

```
\$ source ~/.profile
```
- Verify that the variable is set by executing the following:

```
echo \${CKNFAST_OVERRIDE_SECURITY_ASSURANCES}
```

The output should be `all`.

#### WINDOWS

- In your system's **Control Panel\System and Security\System**, click on **Advanced system settings** link.
- Click **Environment Variables....**
- In the System variables section, create a new environment variable:

Variable name: `CKNFAST_OVERRIDE_SECURITY_ASSURANCES`

Variable value: `all`

- To verify if the variable has been set, open a new Command Prompt window, and execute the following:

```
echo %CKNFAST_OVERRIDE_SECURITY_ASSURANCES%
```

The output should be `all`.

## Application Server

ActiveAccess supports Java Application Servers compatible with Servlet specification 3.0. Install your preferred compatible application server with default settings. Please follow the installation instructions from the application server's documentation.

### Tomcat

Tomcat is freely available for download from Apache at <http://tomcat.apache.org/>.

- Install Tomcat with default settings. Please follow Tomcat installation instructions from the Tomcat documentation.
- Tomcat HTTP server starts on port 8080 by default. In order to change the port settings edit **Tomcat/conf/server.xml**
- Update the following section in the configuration for this port number:

```
<!-- ===== Connectors ===== -->

<!-- Normal HTTP Connector -->

<Connector executor="tomcatThreadPool"
port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
```

## Configuring SSL

ActiveAccess requires that communication between client and server uses HTTPS. Configure the application server to run in HTTPS mode.

## Tomcat SSL Configuration

To configure Tomcat running in HTTPS mode, please refer to the following:

For Tomcat 8.0+: <https://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html>

For Tomcat 8.5+: <https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html>

Please note Tomcat supports two modes of SSL Connectors: JSSE and APR, for which the configuration is different; please refer to the relevant configuration sections in the above Tomcat documentation, for details.

An example configuration for JSSE SSL configuration taken from the Tomcat 8.0 documentation is provided below:

### Create KeyStore (using Java Keytool):

- To create a new Java KeyStore from scratch, containing a single self-signed Certificate, execute the following from a terminal command line:

#### WINDOWS

```
"%JAVA_HOME%\bin\keytool" -genkey -alias appserver -keyalg RSA
```

#### UNIX

```
\$JAVA_HOME/bin/keytool -genkey -alias appserver -keyalg RSA
```

(The RSA algorithm should be preferred as a secure algorithm, and this also ensures general compatibility with other servers and components.)

This command will create a new file, in the home directory of the user under which you run it, named ".keystore". To specify a different location or filename, add the `-keystore` parameter, followed by the complete pathname to your KeyStore file, to the keytool command shown above. For example:

#### WINDOWS

```
"%JAVA_HOME%\bin\keytool" -genkey -alias appserver -keyalg RSA  
-keystore \path\to\my\keystore
```

#### UNIX

```
\$JAVA_HOME/bin/keytool -genkey -alias appserver -keyalg RSA  
-keystore /path/to/my/keystore
```

You will also need to reflect this new location in the application server's configurations, for example, `server.xml` configuration file for Tomcat:



### Example

Configure the Tomcat connector (in the file **TOMCAT\_HOME/conf/server.xml**)

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector

protocol="org.apache.coyote.http11.Http11NioProtocol"

port="8443" maxThreads="200"

scheme="https" secure="true" SSLEnabled="true"

keystoreFile="${user.home}/.keystore" keystorePass="changeit"

clientAuth="false" sslProtocol="TLS"/>
```

## Bypassing the HSM Password Dialog Box

ActiveAccess displays a dialog box for HSM password entry, when you start Tomcat.

- In order to suppress the dialog box and enter the password in the console, add the following parameter to JAVA\_OPTS in the catalina.sh file of Tomcat:

`\-Dconsole`

- *Or alternatively*, you can directly bypass the HSM password by adding the following line in **activeaccess.properties** configuration file (located in the AA\_HOME directory created during installation):

`HSM_PASSWORD= < password >`

Replace `< password >` with the base64 encoded format of your HSM password.

### Base64 encoding

For base64 encoding, the following command can be used in Ubuntu Linux to generate a base64 encoded string with default settings:

```
echo -n 'YourPlainTextPassword' | base64
```

The output of the command above will be:

```
WW91c1BsYWluVGV4dFBhc3N3b3Jk
```

## Increasing the Java Heap Size

JRE allocates 64MB of heap memory to a Java process by default. It is quite often necessary to increase this rather conservative memory allocation for server applications.

### Tomcat

To increase the heap size available to Tomcat add the following line to catalina.bat (Windows) or catalina.sh (UNIX):

```
set JAVA_OPTS= -Xms<min_heap> -Xmx<max_heap>
```

For example in order to set the minimum heap size to 256MB and allow the heap to grow up to 512MB use:

```
set JAVA_OPTS= -Xms256m -Xmx512m
```

## Oracle Database

### Character Set

The database character set **must** be AL32UTF8 to support all Unicode characters.

### User Name and Password for a database

This is the user name and password that you use to access the database. You may set these database user names to the same user (schema) that you have specified for the database owner (The schema that holds all ActiveAccess database objects). However, if you wish to reserve the database owner for administration purposes and set up a more restricted user for ActiveAccess to access the database schema, please the grant the following permissions to the restricted database user:

These permissions require confirmation:

Objects: EXECUTE

PL/SQL: EXECUTE

Sequences: ALTER, SELECT

Tables: DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE

### Note

Please refer to your database server documentation for the installation and configuration of Oracle server.

## Configuring DCD (Dead Connection Detection)

Set the optional parameter `SQLNET.EXPIRE_TIME` to 10 (for 10 minutes) in the `sqlnet.ora` configuration file.

The configuration file is normally located at `$ORACLE_HOME/network/admin` directory.

The value of this parameter determines how often SQL\*NET attempts to verify that the connection is still alive. This is to prevent shadow connections to be left open indefinitely.

There are a number of processes that hold a permanent or temporary lock on the database. If the connection to database is abruptly terminated (network disconnected or the server is turned off), the lock remains and will not be reclaimed by other competing processes. This affects sending notification messages via email, scheduling card upload and user upload jobs or registration services.

Configuring DCD ensures that this situation is automatically rectified after the specified time out.

## Connection Pooling and Firewall

This section provides important operational information for proper configuration of the environment, when the database server is behind a firewall.

ActiveAccess components use a technique known as **connection pooling** to improve the performance of database related tasks. Connection pooling improves performance by reusing previously established connections. However, this may cause a problem when the database server is behind a firewall. The usual symptom is that the application appears to become unresponsive or frozen after a long period of inactivity.

This is due to firewall idle connection time-out setting. A firewall typically drops idle connections after a configurable time-out has expired. This causes further data transmission through these connections to be ignored by the firewall. Since most firewalls simply ignore the data packets and do not respond, this leaves the sender in a state of wait. The length of this wait state depends on the operating system's time-out setting. For Windows this is typically 15 seconds while the default Solaris time-out is 8 minutes during which the application appears to be frozen.

To prevent this problem ActiveAccess and ActiveIssuer components close idle database connections after 15 minutes. Make sure that your firewall time out setting is at least 1 minute longer than the default application idle connection time out.

The default can be changed by setting the `DB_IDLE_TIMEOUT` configuration option (in seconds) for each component.

## Find Transactions Performance

The performance of transaction search can be greatly improved by analysing the HISTORYSESSIONS table on a regular basis.

- Run the following SQL commands on the database monthly:

```
analyze table HISTORYSESSIONS compute statistics;
```

```
analyze table AUTHSESSION compute statistics;
```

```
analyze table CARD compute statistics for all indexed columns;
```

```
analyze table CARDDATA compute statistics for all indexed columns;
```

```
analyze table REQUEST compute statistics for all indexed columns;
```

Analysing a table can take a long time and puts extra load on the database. Analyse the tables at a time when database activity is low.

## Two-Factor Authentication Devices

### CAP

Currently two CAP schemes are supported: M/Chip 4 and M/Chip 2.1. CAP functionalities are supported only with the *Thales e-Security* HSM device. The *Thales e-Security* HSM module must be setup to support EMV functionalities (nShield / SPP).

#### CAP KEYS

Appropriate CAP keys must be created for an issuer that requires CAP support. The keys must be manually created in the HSM using the key management facilities provided by the HSM vendor.

Issuer keys must follow particular naming conventions as follows:

- For M/Chip2.1: `cap2mchip< Issuer_ID >`
- For M/Chip 4: `cap4mchip< Issuer_ID >`

where `< Issuer_Id >` specifies the Issuer ID of the corresponding issuer as assigned by ActiveAccess.

When creating the keys select key roles mkac2r and mkac4r for M/Chip 2.1 and M/Chip 4, respectively. You also need to specify a field named IIPB by SPP module which is the AC part of the CAP IPB (Issuer Proprietary Bitmap).

Please refer to 'Key-loading Solutions Guide' by *Thales e-Security*, for further information on creating and handling keys.

#### SOFTWARE MODE

For testing purposes only ActiveAccess can run CAP in software emulation mode, without the need for setting up CAP keys in the HSM. The CAP emulation mode is only available for M/Chip 4.

- In order to run ActiveAccess in CAP emulation mode, create a text file containing the CAP keys. The file may contain a key entry for each issuer in the form:

```
<key_alias>=<key_value>
```

where < key\_value > is the value of key expressed in hexadecimal format. For example

```
cap4mchip1234567890=9E15204313F7318ACB79B90BD986AD29
```

- Now save the file and give an arbitrary name. Assuming that the file is named 'capkeys.values' and stored in '/opt/activeaccess' directory, you need to add the following line to ActiveAccess start up script:

```
-Dcom.gpayments.CAPKeys.file = /opt/activeaccess/capkeys.values
```

#### Note

Software mode is only provided for test purposes and must not be used in production.

You cannot use CAP in hardware while software mode is enabled. Be sure to remove reference to your CAP key file, if you wish to use hardware for M/Chip 4 or M/Chip 2.1.

#### CAP LOGGING

CAP uses the global java logger to log the CAP related activities. So by setting the java.util.logging.config.file property to an arbitrary java logging configuration file, you can have different levels of logging (Severe, Warning, Info, Fine, Finer, Finest, All) for CAP authentications. More detail is output when ActiveAccess is run in CAP simulation mode.

## RSA

To Enable RSA devices, you need to download and copy the RSA Java library file (RSASecurIDAuthenticationEngineAPI.jar) site to the library directory of ActiveAccess application server. You may need to contact RSA Security in order to receive the Java library file.

RSA token keys should be uploaded in the system. These files are provided by RSA and can be uploaded to ActiveAccess using the administration interface.

- Browse to **System Management > Device Management** choose **upload file** and then specify the file and relevant parameters.

## SMS

SMS authentication is natively supported by ActiveAccess and does not require additional software. However, ActiveAccess needs to be configured to send SMS messages using SMPP protocol to an SMSC (SMS Centre). ActiveAccess supports SMPP-API-0.3.9.1. An SMSC is normally a gateway to the mobile communication network provided by a Telco or third party service provider.

You need the following details in order to configure SMS authentication in ActiveAccess administration:

**Name:** A unique name to identify this SMS centre in ActiveAccess

**IP:** The IP address of the SMS Centre

**Port:** The port which that SMS Centre is listening on

**System ID:** The username that is used by SMS Centre for authentication

**Password:** The password that is used by the SMS Centre for authentication

**Sender's mobile number:** The mobile number displayed to the message recipient.

### Note

Note that to be able to send SMS with templates other than English language or using symbols in SMS Template, you must set following system property in the **TOMCAT\_HOME/bin/catalina.bat** or **catalina.sh**:

```
-Dsmpp.default_alphabet=ie.omk.smpp.util.UCS2Encoding
```

There are two ways to send OTP to SMSC:

## MAILTO

IP: `MailTo:$DEVICE_SERIAL_NUMBER@example.com`

`$DEVICE_SERIAL_NUMBER` will be replaced by ACS with the mobile number that is stored for the card.

### Note

To use this option, mail server must be configured in **System Management > Settings**.

## SMS VIA JMS

- Approach 1:

IP: `SmsViaJms:[IP_ADDR_STAND_ALONE_APP]`

- Approach 2:

IP: `SmsViaJms`

### Note

Note that to be able to send SMS with templates other than English language or using symbols in SMS Template, you must set following system property in the **TOMCAT\_HOME/bin/catalina.bat** or **catalina.sh**:

`-Dsmpp.default_alphabet=ie.omk.smpp.util.UCS2Encoding`

## Email OTP

Email authentication is natively supported by ActiveAccess and does not require additional software. However, ActiveAccess needs to be configured to send OTP via Email. You need the following details in order to configure Email authentication in ActiveAccess administration:

**Mail server address:** The address of the mail server

**Mail server port:** The port which the mail server is listening on

**Mail server username:** The username that is used by the mail server for authentication

**Mail server password:** The password that is used by the mail server for authentication

**Mail server protocol:** The protocol that is used by the mail server for secure communications over the network

**Mail sender:** The sender's name displayed to the email recipient.

## VASCO

To enable authentication using VASCO tokens you need to:

- Install VASCO native libraries first.
- Obtain a copy of Java library 'aal2wrap.java' from VASCO and copy to the lib folder of your ActiveAccess application server.

The native library should be accessible to the java application. For this purpose in UNIX the variable LD\_LIBRARY\_PATH should contain the address of the native library which normally is /opt/vasco/VACMAN\_Controller-3.4/lib.

In Windows the address of the DLL file should be added to the PATH variable. Also the VASCO token keys should be uploaded in the system. These files are provided by VASCO with the devices and can be uploaded to ActiveAccess using the administration interface.

- Browse to **System Management > Device Management** choose **upload file** and then specify the location of the file and relevant parameters.



# Installation

## Prerequisites

- Ensure that a compatible JDK is installed
- Ensure that the hardware security module is properly installed and configured

### HSM keys

If this is a first time installation, ActiveAccess keys will be generated automatically.

For subsequent installations of ActiveAccess on other servers ensure that the AES (128 Bits) key aliases `AA_Administration` , `MIA_DB_DESede` and the issuer key aliases (e.g. `VbVA< Issuer_ID >` , `VbVB< Issuer_ID >` , `RSABVbV< Issuer_ID >` , `ECVbV< Issuer_ID >` , etc) have been transferred from the primary installation in the current instance of HSM used by the ActiveAccess which is being installed.

- Ensure that the application server is properly installed and configured
- Ensure that the database server is properly installed and you have created a database for ActiveAccess.

### Database details

Have the database name, username and password and address at hand for the installation process.

## Pre Installation Configurations

### Upgrades

For upgrades from **any** version of ActiveAccess to the latest version of ActiveAccess, follow the steps below.

### Before the upgrade:

1. Shutdown all instances of ActiveAccess, stop the current Tomcat servers.
2. Back up ActiveAccess directories. Archive the ActiveAccess directory and store in a safe place. Do this for all instances of ActiveAccess.
3. Back up the Tomcat application server directories. Archive directories where the application has been deployed and store in a safe place.
4. Back up the database. The upgrade contains schema level changes. You will not be able to roll back, unless the database is fully backed up.
5. Back up all the HSM key data.

### • Go to **TOMCAT\_HOME/lib**. If the following files exist, back up and remove them:

- gpcomp.pki-\*.jar
- gpcomp.hsm-\*.jar
- spp-\*.jar
- nfjava-\*.jar
- lunaprovider-\*.jar
- kmjava-\*.jar
- kmcsp-\*.jar
- jprov-\*.jar
- commons-codec-\*.jar
- aal2wrap-\*.jar

### Info

If you are using two different database users in setup (for **db\_owner** and **db\_user**), from ActiveAccess v8.0.1 onwards, grant scripts are run automatically during setup and no longer need to be run manually.

## Upgrades from v7.x.x

If you are upgrading from ActiveAccess v7.x.x, **in addition** to the upgrade steps above, follow the steps below.

- An **AA\_HOME** directory is required from which ActiveAccess will load the configurations it requires for installation. Create a directory and set an **AA\_HOME** environment variable to this directory.

 **Note**

Refer to your Operating System and application server documentation for any specific instructions for setting an environment variable.

- Add the following line in the **acsconfig.properties** file (located in **TOMCAT\_HOME/bin/config**)

```
HSM_PASSWORD= < password >
```

Replace **< password >** with the base64 encoded format of your HSM password.

 **Warning**

After the installation, a new configuration file, **activeaccess.properties**, will be created automatically in the **AA\_HOME** directory. This new configuration file combines **acsconfig.properties**, **eb\_config.properties**, **miaconfig.properties** and **regconfig.properties** and these files will be removed during the installation process.

If you have configured any parameters that are not specific to ActiveAccess, you must take a back up of these files before running the installation and move these parameters manually to **activeaccess.properties**.

## New installations

- An **AA\_HOME** directory is required from which ActiveAccess will load the configurations it requires for installation. Create a directory and set an **AA\_HOME** environment variable to this directory.

 **Note**

Refer to your Operating System and application server documentation for any specific instructions for setting an environment variable.

- In the installation package, go to the **ActiveAccess** directory, copy **activeaccess.properties** to your **AA\_HOME** directory.
- Open **activeaccess.properties** and fill in the required configuration parameters.

## Deploying WAR packages

Download and extract the ActiveAccess installation package from [GPayments MyAccount > ActiveAccess > Download](#).

Access Control Server, Administration Server, Enrolment Server and Registration Server are distributed in the ActiveAccess installation package as WAR packages. To install these packages, deploy **acs.war**, **enrolment.war**, **mia.war** and **registration.war** packages from **ActiveAccess/files** to your application server.

#### Deployment mechanism

Depending on the application server, the deployment mechanism would be different. For example for Tomcat, the war files should be copied to **TOMCAT\_HOME/webapps**. Please refer to your application server's documentation for instructions.

## Installation

To initialize the installation process, start the application server.

This process may take a couple of minutes to complete.

An installation log will be created in **AA\_HOME/logs/install\_log.log**.

#### Warning

ActiveAccess modules have specific configuration files such as `log4j.xml`, `sms_jms_config.properties`, which allow the client to customise various parameters based on their environment settings.

In some releases, new parameters are introduced or deprecated. The installer will compare the dates of the configuration files in the installation package with the ActiveAccess working directory and raise warnings if there are any differences.

Following each update/upgrade, the **install\_log.log** file should be checked by the Admin for warnings in order to ensure that no changes in the configuration files have been missed.

The warnings will appear in the following format:

```
The date or size of [full path of the config file in installation package]
is different from [full path of the config file in AA_HOME], compare the
content and make sure all the required and optional parameters are OK.
```

## Installation of Individual Components

The Access Control Server handles greater loads than other components and may be installed on a physical machine, dedicated to transaction processing.

Administration, Registration and Enrolment servers are usually installed on the same physical machine.

To install individual components:

- Ensure that you have the [prerequisites](#) properly installed and configured for each component that is being installed individually.
- [Deploy](#) the component's WAR package to the application server.
  - Access Control Server: **acs.war**
  - Administration Server: **mia.war**
  - Registration Server: **registration.war**
  - Enrolment Server: **enrolment.war**
- Configure the [installation parameters](#) (**AA\_HOME** directory and configuration file).
- Start the application server.
- Ensure that the AES (128 Bits) key aliases `MIA_DB_DESede` , `AA_Administration` , `Card< Issuer_ID >` and the issuer key aliases (e.g. `VbVA< Issuer_ID >` , `VbVB< Issuer_ID >` , `RSABvV< Issuer_ID >` , `ECVbV< Issuer_ID >` , etc. for all card scheme providers) exist in the HSM.

 **Tip**

It is important to note that the issuers and issuer keys are generated on the local HSM used by the Administration server.

If you are installing a component on the same machine as the Administration server, these keys will be created. However, if these servers are installed on physically separate machines that use their own HSM, you will need to export these keys from the Administration server HSM and import them to the local HSM of the Access Control Server, Enrolment and Registration servers' HSM devices.

**Do not attempt to create the keys directly as it will result in creation of physically different keys and the component will not be able to interact with the database server.**

## Post Installation

On successful installation and when the application server is started, the internal components are started on the default port. These components are:

## Access Control Server

**Base URL:** `https://< server-address >:< port >/acs/`

The following extensions can be added to the base URL:

| Card Scheme                          | 3DS1 VE/UE | 3DS1 PA/UA | 3DS2 AReq | 3DS2 CReq |
|--------------------------------------|------------|------------|-----------|-----------|
| Verified by Visa                     | /vbm       | /pa        | /vbva     | /ca       |
| Mastercard SecureCode/IDC            | /msc       | /pa        | /mca      | /ca       |
| JCB J/Secure                         | /jcb       | /pa        | /jcba     | /ca       |
| American Express SafeKey             | /sk        | /pa        | /ska      | /ca       |
| Diners Club International ProtectBuy | /dc        | /pa        | /dca      | /ca       |
| ActiveDevice authentication          | /device    | /pa        |           |           |

### Example

**Verified by Visa VE:** `https://< server-address >:< port >/acs/vbm`

### Info

The PA and CReq paths determine the **ACS URL** as seen by the user.

**3DS Method URL:** `https://< server-address >:< port >/acs/tdsmethod`

**Monitoring the availability of ACS:** `https://< server-address >:< port >/acs/ping`

 Info

If the ACS is up and running, a JSON message will be displayed, which reports the availability of Database as well as the HSM. If the ACS is down, an error will be displayed. If Database or HSM is unavailable the value will be “not connected” in displayed message.

**JSON Response Elements:**

| Attribute           | Possible value                                                                                                                                                                   |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dbConnectionStatus  | <ul style="list-style-type: none"><li>- Connected</li><li>- Connection limit reached</li><li>- Can't establish connection</li><li>- Connection pool is not initialized</li></ul> |
| hsmConnectionStatus | <ul style="list-style-type: none"><li>- Connected</li><li>- Not connected</li></ul>                                                                                              |

 Example

```
{"dbConnectionStatus":"connected","hsmConnectionStatus":"connected"}
```

## Administration Server

**Base URL:** `https://< server-address >:< port >/mia/`

**Monitoring the availability of MIA:** `https://< server-address >:< port >/mia/ping`

### Info

If the Administration Server is up and running, a JSON message will be displayed, which reports the availability of the Database as well as the HSM. If the Administration Server is down, an error will be displayed. If the Database or HSM is unavailable the value "not connected" will be displayed in the message.

#### JSON Response Elements:

| Attribute           | Possible value                                                                                                                                                                        |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dbConnectionStatus  | <ul style="list-style-type: none"> <li>- Connected</li> <li>- Connection limit reached</li> <li>- Can't establish connection</li> <li>- Connection pool is not initialized</li> </ul> |
| hsmConnectionStatus | <ul style="list-style-type: none"> <li>- Connected</li> <li>- Not connected</li> </ul>                                                                                                |

### Example

```
{"dbConnectionStatus":"connected","hsmConnectionStatus":"connected"}
```

## Registration Server

**Base URL:** `http(s)://< server-address >:< port >/registration/`

### Info

Entering the URL above in a browser will display the message:

The Registration Server has received a `GET`.

Your signed XML (application/xml) should be sent via HTTP POST.

Login to the Administration Server as Administrator and set the **Registration server URL** in the **System Management/Settings** section to the base URL of the Registration server.

The Registration Server accepts HTTP Post commands for the purpose of uploading cardholder registration data.



### Info

When using SSL, the Registration server certificate should be signed by a public CA. If you intend to use a self-signed certificate or a certificate signed by a certificate authority other than commercially known certificate authorities, you must import the CA's root certificate into the Administration server's TrustStore.

The Administration server TrustStore (cacerts) can be found in the config directory of the Administration server. Export your CA root certificate as a DER encoded or Base-64 encoded X509 certificate and use Keytool to import this into the cacerts file:

```
keytool -import -trustcacerts -alias myca -file cacert.cer -keystore cacerts -storepass changeit
```

Replace cacert.cer with the CA certificate file you wish to add to the KeyStore.

The following extensions can be added to the base URL:

| Process                      | URL Extension |
|------------------------------|---------------|
| Card registration requests   | /card         |
| User registration requests   | /user         |
| Notification report requests | /notification |

### Note

The base URL can be used for **card registration requests**. Using the extension is optional.

**Monitoring the availability of Registration:** `http(s)://< server-address >:< port >/registration/ping`

### Info

If the Registration Server is up and running, a JSON message will be displayed, which reports the availability of Database as well as the HSM. If the Registration Server is down, an error will be displayed. If Database or HSM is unavailable the value will be "not connected" in displayed message.

#### JSON Response Elements:

| Attribute           | Possible value                                                                                                                                                                        |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dbConnectionStatus  | <ul style="list-style-type: none"> <li>- Connected</li> <li>- Connection limit reached</li> <li>- Can't establish connection</li> <li>- Connection pool is not initialized</li> </ul> |
| hsmConnectionStatus | <ul style="list-style-type: none"> <li>- Connected</li> <li>- Not connected</li> </ul>                                                                                                |

### Example

```
{ "dbConnectionStatus": "connected", "hsmConnectionStatus": "connected" }
```

## Enrolment Server

**Base URL:** `https://< serveraddress >:< port >/enrolment/< IssuerID >`

### Info

The Enrolment Server uses a unique URL for each issuer. When an issuer is created, it is assigned a unique, system generated Issuer ID. Enrolment pages can only be viewed after an issuer has been successfully enrolled and the enrolment package for that issuer has been uploaded to the system through the Administration server.

**Monitoring the availability of Enrolment:** `https://< serveraddress >:< port >/enrolment/ping`

 Info

If the Enrolment Server is up and running, a JSON message will be displayed, which reports the availability of the Database as well as the HSM. If the Enrolment Server is down, an error will be displayed. If the Database or HSM is unavailable the value "not connected" will be displayed in the message.

**JSON Response Elements:**

| Attribute           | Possible value                                                                                                                                                                   |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dbConnectionStatus  | <ul style="list-style-type: none"><li>- Connected</li><li>- Connection limit reached</li><li>- Can't establish connection</li><li>- Connection pool is not initialized</li></ul> |
| hsmConnectionStatus | <ul style="list-style-type: none"><li>- Connected</li><li>- Not connected</li></ul>                                                                                              |

 Example

```
{"dbConnectionStatus":"connected","hsmConnectionStatus":"connected"}
```

## Configuration Files

### ActiveAccess Configuration File

*AA\_HOME/activeaccess.properties*

The ActiveAccess Configuration file, **activeaccess.properties**, is automatically created/updated by the ActiveAccess installation. Common options such as database information are required to be configured during installation. The following sections document all the available parameters in case you need to change the defaults.

 Note

ActiveAccess server must be restarted for changes to configuration files to take effect.

## Common Configuration Parameters

### DBNAME, DBOWNERPASSWORD

This is the database owner name and password that you use to create the database. When you first set or change the database owner password, you may set it in clear text. You should also add (PLAIN\_TEXT=) to your configuration file.

#### Note

This parameter must always have a value.

### DBUSERNAME, DBPASSWORD

This is the **username** and **password** that you use to access the database. In a simple configuration this username may be the same as the database owner name. When you first set or change the database password, you may set it in clear text. You should also add (PLAIN\_TEXT=) to your configuration file.

#### Note

This parameter must always have a value.

### PLAIN\_TEXT=

This instructs the server to read DBOWNERPASSWORD and DBPASSWORD in clear text and replace them with the encrypted values.

### DBURL

For Oracle the default URL is:

```
jdbc\:oracle\:thin\:@127.0.0.1\:1521\:ORCL
```

Replace 127.0.0.1:1521 with the IP address and port number of the Oracle instance you have installed. ORCL is the SID of the database and must be replaced with the SID you selected during the installation of the database server.

```
DBURL=jdbc\:oracle\:thin\:@192.168.0.202\:1521\:ORCL
```

## DBDRIVER

For Oracle, leave the default value unchanged as shown below:

```
DBDRIVER=oracle.jdbc.driver.OracleDriver
```

## INITIALCONNECTIONS

Specifies the initial length of database connection pool allocated by the application.

## MAXCONNECTIONS

Specifies the maximum length of database connection pool that can be allocated by the application.

## WAITIFBUSY

Can be set to either true or false. The default is true. When set to true, connection requests exceeding the maximum connections will be queue until a connection is freed. When set to false, the application immediately returns an connection error if no free connection can be found in the pool.

## DB\_IDLE\_TIMEOUT

The database idle connection time out in seconds. Idle database connections are closed in the application's connection pool after the specified time. The default is 900 seconds.

## DBENCODED

If this parameter sets to false reading and writing to database is done in ISO-8859-1 character set and ActiveAccess uses its own encoding (Default value is **false**). Otherwise database's own encoding is used.

## HSM PROVIDER

Used to specify the HSM provider name.

For ActiveAccess instances which were originally installed prior to ActiveAccess v7.4.0, the value would be **nCipherKM** for Thales e-Security, **ERACOM** for SafeNet, or **SUN** for Sun JCE. In ActiveAccess instances originally installed after and including v7.4.0, this parameter would be **PKCS11** or **SUN**.

 **Note**

This parameter should always have a value.

## KEYSTORE\_DIR

Used to specify the physical location of the HSM KeyStore (Thales e-Security or SunJCE). Use forward slash as the path separator e.g.: `KEYSTORE_DIR=c:/nfast/kmdata/local`

## PKCS11\_CONFIG\_FILE\_PATH

Used to specify the path to the PKCS #11 configuration file with a `.properties` extension.

The contents of the configuration file should contain `library`, `slot` and `name` parameters.

 **Note**

If this file does not exist, it will be generated automatically.

## nShieldHSM

Only if you are using an nShield HSM, set the value to Yes. For all other HSM types, it should be left blank.

## HSM\_PASSWORD

Used to set the HSM password in the configuration file. This option takes precedence over the java option `-Dcom.gpayments.hsm.password`. The HSM password must be provided in base64 encoded format in both cases. Leave empty for a blank HSM password.

## HSM\_LIB\_DIR

Use to specify the path of `.dll` or `.so` file which will be added to `pkcs11config.properties` file, if the file does not exist.

## HSM\_SLOT

Use to specify the slot number that will be added to `pkcs11config.properties` file, if the file does not exist.

## HSMENCALIAS

When the MIA/ACS Settings Encryption Key is automatically or manually retired and replaced with a new one using the PCIDSS Key Retiring Utility, the default key alias is changed. Therefore, the new key alias is specified by HSMENCALIAS.

## **TOMCAT\_KEYSTORE**

Used to specify the path of the Tomcat KeyStore in case the timeout error fails with SSL Handshake in browser-based authentication.

### **Note**

Use forward slash as the path separator.

## **TOMCAT\_KEYSTORE\_PASS**

Used to specify the password of the Tomcat KeyStore in case **TOMCAT\_KEYSTORE** is set.

## **TOMCAT\_TRUSTSTORE**

Used to specify the path of the Tomcat TrustStore in case the timeout error fails with SSL Handshake in browser-based authentication and the SSL connection is not one-sided.

### **Note**

Use forward slash as the path separator.

## **TOMCAT\_TRUSTSTORE\_PASS**

Used to specify the password of the Tomcat TrustStore in case **TOMCAT\_TrustStore** is set.

## **CARD\_MOD\_10\_CHECK**

Used to enable/disable mod 10 check when creating cards via the administration interface, for testing purposes. It can be set to **true** or **false**. The default value is **true**.

## **TESTING\_MODE**

Can be set to either **true** or **false**. Set it to true during certification testing. Default value is **false**.

## **PROVIDER\_TEST**

Can be set to either `true` or `false`. Set it `true` during certification test only if the test card bin is not supported in default providers.xml file. If set true providers\_test.xml should be created and placed at `AA_HOME`.

## TEST\_AUTH\_SERVER

Set URL of authentication server. This parameter is developed to support UL tests.

## ACS\_REFERENCE\_NUMBER\_TEST

Set ACS reference number during certification test.

## TIMEZONE\_ID

Used to set the time zone of the application.

Refer to **ActiveAccess/timezones.txt** which has a list of acceptable time zones.

### Example

```
TIMEZONE_ID=Australia/Sydney
```

### Note

This parameter should always have a value.

## Additional Administration Server Configuration Parameters

### UPLOADCACHE\_DIR

Used to specify a location to copy uploaded file that VASCO and RSA tokens fetched from it. Use forward slash as a path separator e.g.: `UPLOADCACHE_DIR=c:/tempdir`

### MAX\_WARNINGS

Specifies the maximum number of warning messages that the administration server will generate while processing VASCO or RSA token files before an error is returned. In other words, if processing a VASCO or RSA file creates more warnings than this value, the server will terminate processing of the file and will return an error response. If this parameter is not specified, a default value of 50 is used.

## MODULE



Used for initialising of the key manager for CAP functions. Select HSM for secure computation and cryptographic functions. A value of zero results in load sharing among all nShield capable modules. Default value is **0**.

## PSINAME

Used for initializing the key manager for CAP functions. It is the name of the nShield installation to be initialized. Default value is **gpayersTest**.

## Additional ACS Configuration Parameters

### COMPUTERNAME

This is the computer name where the ACS is installed.

### DOMAINNAME

This is the domain name where the ACS is installed. It must be resolved to an IP address and you must add this host name to `/etc/hosts` or in Windows `C:`

`\WINDOWS\system32\drivers\etc\hosts` before installation.

### BINDING\_IP\_ADDRESS

Used to define the binding IP address of ActiveAccess.

### RMI\_PORT

The RMI port of ActiveAccess. The default value for the RMI port is 4242. If you decide to change the RMI port, you can edit this value at any time.

### AHS\_FLAG

Used to enable/disable Authentication History Server. It can be set to either true or false. The default value is true.

### CACHING

This option specifies the caching mode for resources. The default is **everyvisit**.

### DBENCODED

Can have two values **Yes** or **No**. If your Database is set to use encoding, set this option to **Yes**.

### MODULE

Used for initialising of the key manager for CAP functions. Select HSM for secure computation and cryptographic functions. A value of zero results in load sharing among all nShield capable modules. Default value is **0**.

## ZLIBOFF

It can be set to either **true** or **false**. When it is set to true, ACS does not inflate ZIP objects. The default value is false.

### Warning

This option is for test purposes only. Setting the options to **true** in production will cause interoperability problems with other 3-D Secure components.

## Additional Registration Server Configuration Parameters

### VERIFICATION

Can be set to either **true** or **false**. When the verification is true, the registration server checks the authenticity of XML messages by validating the XML signature. Disabling verification should be avoided in a production system for security reasons.

### REQUEST\_LOGGING

Can be set to either **true** or **false**. Used to collect request debug information, intended for testing purposes. This option should not be enabled in production environment.

### MAX\_WARNINGS

Specifies the maximum number of warning messages that the registration server will generate, before an error is returned. In other words, if a message sent to the registration server creates more warnings than this value, the server will terminate processing the message and will return an error response. If this parameter is not specified the default value of 50 is used.

### Notification Report Collector Job Parameters:

Notification Reports are provided based on collected report files by the Notification Report Collector Job on the Registration server. In order to configure this job to collect the required data and cache report files, the following parameters must be set in activeaccess.properties:

### LAST\_REPORT\_TIME

The last time that the notification report collector job was run

Format: DD/MM/YYYY

**OFFICIAL\_START\_HOUR** (Deprecated and is no longer used)

The hour that is used as the start hour of the day. Reports are collected based on this hour.

Values: 00..23 (default: 00)

**OPTOUT\_MODE**

The flag that specifies whether report collector should collect the last cardholder opt out only or all opt outs.

Values: LAST/ALL (default: ALL)

**SCHEDULER\_START\_TIME**

The time that the report collector job starts to collect reports based on LAST\_REPORT\_DATE

Format: HH:mm:ss GMT(+0:00) (default: -1 to disable job).

Example: Assume LAST\_REPORT\_TIME=02/02/2009, SCHEDULER\_START\_TIME=22:30:30, if today is 05/02/2009, report collector starts at 22:30:30 GMT(+0:00) and collects reports from 02/02/2009 00:00 to 05/02/2009 00:00

 **Note**

If SCHEDULER\_START\_TIME is set to a time in past, the job will be scheduled for tomorrow at the specified time.

**NOTIFICATION\_FILE\_PATH**

The path on the server which the report collector job will cache for the collected report files

The default path is a **NotificationReport** directory, located in the deployed directory of Registration on your application server.

**NOTIFICATION\_REPORT\_LIFETIME**

The life time of cached report files on the server in DAY. As soon as the report collector job starts, it removes files if their life time period has already passed

Default: -1 to disable

## NOTIFICATION\_REPORT\_REGEN\_ISSUERIDS

A comma separated list of the IDs of the issuers that have retired their encryption key using PCIDSS Retiring Utility. As the result of retiring the encryption key of an issuer, the pre-collected notification report files are no longer valid. This list is automatically populated at the end of the utility process to indicate that notification reports should be re-collected for the specified issuers at the next run of the notification report collector job.

### Example

```
NOTIFICATION_REPORT_REGEN_ISSUERIDS= 284357534937385611, 974922143261996848
```

## Additional Enrolment Server Configuration Parameters

### CACHE:

Specify the caching mode used for caching issuer pages. (0: every visit, 1: automatically, 2: never, default value is **0**.)

### MAX\_CACHE:

Specify the number of issuer pages that will be cached. Default value is: 100.

## Providers File

ActiveAccess requires the default card ranges of all providers in order to process incoming 3D-Secure authentication requests. As card schemes may add new card ranges at any time, the providers file allows for the additions to be made manually, when required. The following options can be updated in **providers.xml** under the **AA\_HOME** directory.

- **Provider name, provider index, cname and provider ID:** within the < providerInfo > element for each of the providers, there are tags for the provider's name (< providerName >), index (< providerIndex >), card scheme authentication method (< cName >), and provider ID (< providerId >). The following table shows the possible values for the aforementioned tags.

| providerName | providerIndex | cName | providerId |
|--------------|---------------|-------|------------|
| Visa         | 1             | vbv   | 2          |
| Mastercard   | 2             | msc   | 1          |

| providerName | providerIndex | cName | providerId |
|--------------|---------------|-------|------------|
| JCB          | 3             | jcb   | 3          |
| AMEX         | 4             | sk    | 5          |
| DinersClub   | 5             | dc    | 6          |

- **Card Range:** the card ranges for each provider are included in the providers file, in the form of minimum range and maximum range. The minimum range should always be lower than, or equal to, the maximum range, with an equal number of digits. You can add any card range to the providers file inside the tag, by copying the tag and inserting the new minimum and maximum ranges. Make sure the newly added card ranges do not overlap with another provider's card ranges. Furthermore, the tag indicates the required number of digits for card numbers, which fall within the specified card range.

 **Note**

If you want to update the providers file, make sure the xml format is followed closely, as any formatting issues may result in ActiveAccess failing to start.

 **Note**

Changes made to the providers file will not take effect immediately, unless the ActiveAccess server is restarted.

## Glossary

This page provides a list of terms relating to 3D Secure 1 and 2, some are not used elsewhere in this documentation but are included for completeness of the subject area. Familiarise yourself with them now or refer back to this page when you come across an unfamiliar word, phrase or acronym.

| Term                      | Acronym     | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>2-F Authentication</b> |             | A generic functionality, which allows for strong authentication of any transaction, commercial or otherwise, for example, strong authentication of users when they login to an Internet banking site or when they authorise funds transfer to a third party. 2-F authentication requires two independent ways to establish identity and privileges as opposed to traditional password authentication, which requires only one 'factor' (knowledge of a password).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>3-D Secure</b>         | <b>3DS</b>  | A payer authentication standard (3D Secure 1 (3DS1)) introduced by Visa (Verified by Visa) and subsequently adopted by Mastercard (Mastercard SecureCode and Mastercard SecureCode), JCB (JCB J/Secure), American Express (SafeKey) and Diners Club International / Discover (ProtectBuy) designed to reduce online credit card fraud and chargeback. The 3DS standard provides an additional layer of protection in card-not-present credit card transactions for the three domains involved: Issuer domain of the card issuing bank, the Interoperability domain of the card scheme's infrastructure and the Acquirer domain of the merchants.<br><br>The second version of the standard, 3D Secure 2 (3DS2) (EMV 3-D Secure protocol), is facilitated by EMVCo, a six member consortium comprised of American Express, Discover, JCB, Mastercard, UnionPay and Visa. It creates a frictionless payment experience for cardholders by facilitating a richer cardholder data exchange, allowing risk-based authentication by issuers for low risk transactions, instead of authentication challenges to the cardholder, such that most authentication activity will be invisible to the cardholder. 3DS2 also supports authentication of app-based transactions on mobile and other consumer connected devices, and cardholder verification for non-payment transactions, such as adding a payment card to a digital wallet. |
| <b>3D Secure</b>          | <b>3DS1</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>3D Secure 1</b>        | <b>3DS2</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>3D Secure 2</b>        |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Term                                                | Acronym        | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3DS Client</b>                                   |                | The consumer-facing component, such as a browser-based or mobile app online shopping site, which facilitates consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.                                                                                                                                                                                                                                      |
| <b>3DS Integrator</b>                               |                | An EMV 3-D Secure participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer.                                                                                                                                                                                                                                                                   |
| <b>3-D Secure Provider</b>                          |                | An entity such as American Express, Diners Club International, Discover, JCB, Mastercard or Visa, which provides interoperability services for issuers and merchants who participate in the authentication process. The 3-D Secure provider is normally in charge of managing the directory server, managing the authentication history server and issuing the digital certificates required for participation in the authentication scheme. |
| <b>3DS Requestor</b>                                |                | The initiator of the EMV 3-D Secure Authentication Request, known as the AReq message. For example, this may be a merchant or a digital wallet requesting authentication within a purchase flow.                                                                                                                                                                                                                                             |
| <b>3DS Requestor App</b>                            |                | An App on a Consumer Device that can process a 3-D Secure transaction through the use of a 3DS SDK. The 3DS Requestor App is enabled through integration with the 3DS SDK.                                                                                                                                                                                                                                                                   |
| <b>3DS Requestor Environment</b>                    |                | This describes the 3DS Requestor controlled components of the Merchant / Acquirer domain, which are typically facilitated by the 3DS Integrator. These components include the 3DS Requestor App, 3DS SDK, and 3DS Server. Implementation of the 3DS Requestor Environment will vary as defined by the 3DS Integrator.                                                                                                                        |
| <b>Three Domain Secure Software Development Kit</b> | <b>3DS SDK</b> | 3-D Secure Software Development Kit. A component that is incorporated into the 3DS Requestor App. The 3DS SDK performs functions related to 3-D Secure on behalf of the 3DS Server.                                                                                                                                                                                                                                                          |
| <b>3DS Requestor Initiated</b>                      | <b>3RI</b>     | 3-D Secure transaction initiated by the 3DS Requestor for the purpose of confirming an account is still valid. The main use case being recurrent transactions (TV subscriptions, utility bill payments, etc.) where the merchant wants perform a Non-Payment transaction to verify that a subscription user still has a valid form of payment.                                                                                               |
| <b>3DS Server</b>                                   |                | Refers to the 3DS Integrator's server or systems that handle online transactions and facilitate communication between the 3DS Requestor and the Directory Server.                                                                                                                                                                                                                                                                            |

| Term                                      | Acronym     | Definition                                                                                                                                                                                                                                            |
|-------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3-D Secure</b>                         | <b>3DS</b>  | <b>Three Domain Secure.</b> An eCommerce authentication protocol that for version 2 onwards enables the secure processing of payment, non-payment and account confirmation card transactions.                                                         |
| <b>Access Control Server</b>              | <b>ACS</b>  | A component that operates in the Issuer Domain, which verifies whether authentication is available for a card number and device type, and authenticates specific Cardholders.                                                                         |
| <b>Accountholder Authentication Value</b> | <b>AAV</b>  | A value providing proof of cardholder authentication, which is generated by the issuer's access control server for each transaction. The AAV is passed by the merchant to the acquirer and then by the acquirer to the issuer through the UCAF field. |
| <b>Acquirer</b>                           |             | A financial institution that has a relationship with a merchant and processes payment transactions for that merchant.                                                                                                                                 |
| <b>ActiveAccess</b>                       |             | GPayments' access control server for card issuers and service providers.                                                                                                                                                                              |
| <b>ActiveDevice</b>                       |             | GPayments' device agnostic two-factor authentication component.                                                                                                                                                                                       |
| <b>ActiveMerchant</b>                     |             | GPayments' payment authentication platform (merchant plug-in) for merchants.                                                                                                                                                                          |
| <b>ActiveServer</b>                       |             | GPayments' 3DS Server for payment processors and merchants (see <i>3DS Server</i> ).                                                                                                                                                                  |
| <b>Attempts</b>                           |             | Used in the EMV 3DS specification to indicate the process by which proof of an authentication attempt is generated when payment authentication is not available. Support for Attempts is determined by each DS.                                       |
| <b>Authentication</b>                     |             | In the context of 3-D Secure, the process of confirming that the person making an eCommerce transaction is entitled to use the payment card.                                                                                                          |
| <b>Authentication Device</b>              |             | A physical device capable of generating a token to be used in the verification of a user's identity.                                                                                                                                                  |
| <b>Authentication Request Message</b>     | <b>AReq</b> | An EMV 3-D Secure message sent by the 3DS Server, via the DS, to the ACS to initiate the authentication process.                                                                                                                                      |



| Term                                   | Acronym     | Definition                                                                                                                                                                                                                             |
|----------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Response Message</b> | <b>ARes</b> | An EMV 3-D Secure message returned by the ACS, via the DS, in response to an Authentication Request message.                                                                                                                           |
| <b>Authentication Token</b>            |             | An unpredictable piece of information generated by an authentication device, which is used to verify the identity of a user. The term token may sometimes be used to refer to the physical device that generated the token as well.    |
| <b>Authentication Value</b>            | <b>AV</b>   | A cryptographic value generated by the ACS to provide a way, during authorisation processing, for the authorisation system to validate the integrity of the authentication result. The AV algorithm is defined by each Payment System. |
| <b>Authorisation</b>                   |             | A process by which an Issuer, or a processor on the Issuer's behalf, approves a transaction for payment.                                                                                                                               |
| <b>Authorisation System</b>            |             | The systems and services through which a Payment System delivers online financial processing, authorisation, clearing, and settlement services to Issuers and Acquirers.                                                               |
| <b>Bank Identification Number</b>      | <b>BIN</b>  | The first six digits of a payment card account number that uniquely identifies the issuing financial institution. Also referred to as an Issuer Identification Number (IIN) in ISO 7812.                                               |
| <b>BankNet</b>                         |             | Mastercard's proprietary payment network.                                                                                                                                                                                              |
| <b>Base64</b>                          |             | Encoding applied to the Authentication Value data element as defined in RFC 2045.                                                                                                                                                      |
| <b>Base64 URL</b>                      |             | Encoding applied to the 3DS Method Data, Device Information and the CReq/CRes messages as defined in RFC 7515.                                                                                                                         |
| <b>Card</b>                            |             | Card is synonymous with the account of a payment card, in the <i>EMV 3-D Secure Protocol and Core Functions Specification</i> .                                                                                                        |
| <b>Certificate Authority</b>           | <b>CA</b>   |                                                                                                                                                                                                                                        |
| <b>Cardholder</b>                      |             | An individual to whom a card is issued or who is authorised to use that card.                                                                                                                                                          |

| Term                                                        | Acronym     | Definition                                                                                                                                                                                                                           |
|-------------------------------------------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cardholder Activation During Shopping</b>                |             | A 3D-Secure 1 process by which cardholders can enrol with the authentication system at the time of making a purchase at a participating merchant eCommerce website.                                                                  |
| <b>Centralised Authentication and Authorisation Service</b> | <b>CAAS</b> | A remote ACS, see <i>Access Control Server</i> .                                                                                                                                                                                     |
| <b>Challenge</b>                                            |             | The process where the ACS is in communication with the 3DS Client to obtain additional information through Cardholder interaction.                                                                                                   |
| <b>Challenge Flow</b>                                       |             | A 3-D Secure flow that involves Cardholder interaction as defined in the <i>EMV 3-D Secure Protocol and Core Functions Specification</i> .                                                                                           |
| <b>Challenge Request Message</b>                            | <b>CReq</b> | An EMV 3-D Secure message sent by the 3DS SDK or 3DS Server where additional information is sent from the Cardholder to the ACS to support the authentication process.                                                               |
| <b>Challenge Response Message</b>                           | <b>CRes</b> | The ACS response to the CReq message. It can indicate the result of the Cardholder authentication or, in the case of an App-based model, also signal that further Cardholder interaction is required to complete the authentication. |
| <b>Chip Card</b>                                            |             | A card with an on-board integrated circuit chip.                                                                                                                                                                                     |
| <b>Consumer Device</b>                                      |             | Device used by a Cardholder such as a smartphone, laptop, or tablet that the Cardholder uses to conduct payment activities including authentication and purchase.                                                                    |
| <b>Cryptography</b>                                         |             | A process that encrypts information for the purpose of protecting it. Information is decrypted when required.                                                                                                                        |
| <b>Device</b>                                               |             | see <i>Authentication Device</i> .                                                                                                                                                                                                   |
| <b>Device Channel</b>                                       |             | Indicates the channel from which the transaction originated. Either: • App-based (01-APP) • Browser-based (02-BRW) • 3DS Requestor Initiated (03-3RI)                                                                                |
| <b>Device Information</b>                                   |             | Data provided by the Consumer Device that is used in the authentication process.                                                                                                                                                     |

| Term                                           | Acronym               | Definition                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Directory Server</b>                        | <b>DS</b>             | A server component operated in the Interoperability Domain; it performs a number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.                                          |
| <b>Directory Server Certificate Authority</b>  | <b>DS CA or CA DS</b> | A component that operates in the Interoperability Domain; generates and Certificate Authority (DS distributes selected digital certificates to components participating in 3-D Secure. Typically, the Payment System to which the DS is connected operates the CA.                                          |
| <b>Directory Server ID (directoryServerID)</b> |                       | Registered Application Provider Identifier (RID) that is unique to the Payment System. RIDs are defined by the ISO 7816-5 standard.                                                                                                                                                                         |
| <b>Electronic Commerce Indicator</b>           | <b>ECI</b>            | Payment System-specific value provided by the ACS to indicate the results of the attempt to authenticate the Cardholder.                                                                                                                                                                                    |
| <b>Digital Signature</b>                       |                       | Equivalent of the physical signature in the digital world. Digital signatures can verify the identity of owner of a piece of information or a document in the digital world.                                                                                                                                |
| <b>Enrolment</b>                               |                       | A cardholder must pass an initial online authentication procedure in 3D-Secure 1, which is verified by the Issuer prior to gaining eligibility for participation in American Express SafeKey, Diners Club International ProtectBuy, JCB J/Secure, Mastercard SecureCode or Verified by Visa authentication. |
| <b>Frictionless</b>                            |                       | Used to describe the authentication process when it is achieved without Cardholder interaction.                                                                                                                                                                                                             |
| <b>Frictionless Flow</b>                       |                       | A 3-D Secure flow that does not involve Cardholder interaction as defined in EMVCo Core Spec Section 2.5.1.                                                                                                                                                                                                 |
| <b>Issuer</b>                                  |                       | A financial institution that provides cardholders with credit cards.                                                                                                                                                                                                                                        |
| <b>J/Secure</b>                                |                       | JCB's standard for cardholder authentication, based on 3-D Secure.                                                                                                                                                                                                                                          |
| <b>Message Authentication Code</b>             | <b>MAC</b>            |                                                                                                                                                                                                                                                                                                             |

| Term                                          | Acronym      | Definition                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mastercard SecureCode / Identity Check</b> |              | Mastercard's payer authentication brand, which includes SPA Algorithm for the Mastercard Implementation of 3-D Secure, SPA and chip card authentication program (CAP).                                                                                                                                                                     |
| <b>Mastercard 3-D Secure</b>                  |              | The SPA Algorithm for the Mastercard Implementation of 3-D Secure that provides a browser authentication experience to the cardholder (see also <i>3-D Secure</i> ).                                                                                                                                                                       |
| <b>Mastercard Identity Check</b>              |              | see <i>Mastercard SecureCode / Identity Check</i> .                                                                                                                                                                                                                                                                                        |
| <b>Merchant</b>                               |              | Entity that contracts with an Acquirer to accept payments made using payment cards. Merchants manage the Cardholder online shopping experience by obtaining the card number and then transfers control to the 3DS Server, which conducts payment authentication.                                                                           |
| <b>Merchant Plug-in (MPI)</b>                 |              | A software module which can be integrated into a merchant's eCommerce website or run as a managed service on behalf of a number of merchants to provide 3-D Secure authentication.                                                                                                                                                         |
| <b>Non-Payment Authentication</b>             | <b>NPA</b>   | .                                                                                                                                                                                                                                                                                                                                          |
| <b>One-Time Passcode</b>                      | <b>OTP</b>   | A passcode that is valid for one login session or transaction only, on a computer system or other digital device.                                                                                                                                                                                                                          |
| <b>Out-of-Band</b>                            | <b>OOB</b>   | A Challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed. ACS authentication methods or implementations are not defined by the 3-D Secure specification. |
| <b>Payer Authentication Request</b>           | <b>PAReq</b> | Message sent from the MPI to the Access Control Server at the cardholder's issuer via the cardholder browser.                                                                                                                                                                                                                              |
| <b>Payer Authentication Response</b>          | <b>PARes</b> | A digitally signed message sent from the Access Control Server to the Merchant Plug-in which communicates whether the cardholder authentication was successful or not.                                                                                                                                                                     |

| Term                                              | Acronym     | Definition                                                                                                                                                                                                                                    |
|---------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Payment Gateway</b>                            |             | A software system provided by an acquirer or a third party which accepts transactions from the Internet and transfers them to a payment network such as BankNet or VisaNet.                                                                   |
| <b>Preparation Request Message</b>                | <b>PReq</b> | 3-D Secure message sent from the 3DS Server to the DS to request the ACS and DS Protocol Versions that correspond to the DS card ranges as well as an optional 3DS Method URL to update the 3DS Server's internal storage information.        |
| <b>Preparation Response Message</b>               | <b>Pres</b> | Response to the PReq message that contains the DS Card Ranges, active Protocol Versions for the ACS and DS and 3DS Method URL so that updates can be made to the 3DS Server's internal storage.                                               |
| <b>Proof or authentication attempt</b>            |             | Refer to Attempts.                                                                                                                                                                                                                            |
| <b>ProtectBuy</b>                                 |             | Diners Club International and Discover standard for cardholder authentication, based on 3-D Secure.                                                                                                                                           |
| <b>Registered Application Provider Identifier</b> | <b>RID</b>  | Registered Application Provider Identifier (RID) is unique to a Payment System. RIDs are defined by the ISO 7816-5 Standard and are issued by the ISO/IEC 7816-5 Registration Authority. RIDs are 5 bytes.                                    |
| <b>Results Request Message</b>                    | <b>RReq</b> | Message sent by the ACS via the DS to transmit the results of the authentication transaction to the 3DS Server.                                                                                                                               |
| <b>Results Response Message</b>                   | <b>RRes</b> | Message sent by the 3DS Server to the ACS via the DS to acknowledge receipt of the Results Request message.                                                                                                                                   |
| <b>Risk-Based Authentication</b>                  | <b>RBA</b>  | During risk-based authentication, the rich cardholder data exchanged in AReq is taken into account to determine the risk profile associated with that transaction. The complexity of the challenge is then decided based on the risk profile. |
| <b>SafeKey</b>                                    |             | American Express standard for cardholder authentication, based on 3-D Secure.                                                                                                                                                                 |

| Term                                                    | Acronym    | Definition                                                                                                                                                                                                                             |
|---------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secure Payment Application (SPA)</b>                 |            | Mastercard's payer authentication standard designed to reduce online credit card fraud and chargeback using a client-side applet. Also known as Mastercard's PC Authentication Program, Mastercard SecureCode, Mastercard SPA and SPA. |
| <b>Secure Sockets Layer (SSL)</b>                       |            | A protocol designed to maintain the integrity and confidentiality of communication over the Internet.                                                                                                                                  |
| <b>SecureCode</b>                                       |            | see <i>Mastercard SecureCode / Identity Check</i> .                                                                                                                                                                                    |
| <b>Token:</b>                                           |            | see <i>Authentication Token</i> .                                                                                                                                                                                                      |
| <b>Two Factor Authentication</b>                        |            | see <i>2-F Authentication</i>                                                                                                                                                                                                          |
| <b>Uniform Resource Locator (URL)</b>                   |            | Address system for locating unique sites on the Internet.                                                                                                                                                                              |
| <b>Universal Cardholder Authentication Field (UCAF)</b> |            | Data element 48 sub element 43 as defined in Mastercard BankNet to carry authentication data. Mastercard SecureCode uses this element to transport AAV from the acquirer to the issuer.                                                |
| <b>Verified by Visa</b>                                 | <b>VbV</b> | A payer authentication standard introduced by Visa (see <i>3-D Secure</i> ).                                                                                                                                                           |
| <b>VisaNet</b>                                          |            | Visa's proprietary payment network.                                                                                                                                                                                                    |
| <b>Visa Secure</b>                                      |            | A program developed by Visa to make online payments more secure through 3-D Secure 2.                                                                                                                                                  |

# Document Control

 new item
 item changed
 item removed
 no change to item

## Risk Management

| Date         | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|--------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [25/11/2020] | 8.4.4  | 8.4.4:1 | <b>Remote Messaging (Specifications)</b><br> Added <b>Attributes</b> and <b>Descriptions</b> to <a href="#">Table 4 - Transaction</a> , <a href="#">Table 10 - PreAuthReq</a> , <a href="#">Table 11 - HeaderParams</a> and <a href="#">Table 12 - AdditionalParams</a> .                                                                                                                                                                                                                                                                                                                                   |
| [29/10/2020] | 8.4.1  | 8.4.1:1 | <b>System Management (ACS URL)</b><br> Added details to <b>ACS challenge URL</b> for OOB's WebSocket and callback I<br><a href="#">3-D Secure 2 Settings</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|              |        |         | <b>System Management (Issuer Management)</b><br> Added a note to <b>ACS Challenge URL</b> for OOB's WebSocket and callback I<br><a href="#">New Issuer Group</a> , <a href="#">Issuer Group Details</a> and <a href="#">Issuer Details</a> .                                                                                                                                                                                                                                                                                                                                                              |
|              |        |         | <b>Remote Messaging (Specifications)</b><br> Added notes to AuthType and AuthTypeSup at <a href="#">Table 6 - CardInfo</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|              |        |         | <b>Codes (RReq Authentication Method Codes)</b><br> Added a new page: <a href="#">RReq Authentication Method Codes</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| [16/10/2020] | 8.4.0  | 8.4.0:1 | <b>Settings (Admin UI)</b><br> Added a note to <b>Log level</b> in <a href="#">Settings</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|              |        |         | <b>Issuer Management (Admin UI)</b><br> Added <b>Verified by Visa CAVV format</b> and <b>Visa Secure CAVV format</b> to <a href="#">N</a><br><a href="#">Issuer Group</a> and <a href="#">Issuer Details</a><br> Added <b>IAV generation algorithm</b> , <b>Verified by Visa CAVV format</b> and <b>Visa</b><br><b>CAVV format</b> to <a href="#">Issuer Group Details</a><br> Added <b>ACS URL</b> to <a href="#">New Issuer</a> . |
|              |        |         | <b>Issuers (Admin UI)</b><br> Added a note to <a href="#">Custom pages</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Date       | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                               |
|------------|--------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |        |         | <p><b>Transactions</b> (Admin UI)</p> <p>+ Added <b>Failed reason</b> and <b>IAV generation algorithm</b> to <a href="#">Transaction Detail</a>.</p>                                                                         |
|            |        |         | <p><b>Remote Messaging</b> (Specifications)</p> <p>+ Added <b>callBack</b> to <a href="#">Table 14 - InitAuthReq</a>.</p>                                                                                                    |
|            |        |         | <p><b>Out of Band (OOB) Authentication Adapter</b> (Specifications)</p> <p>+ Added <b>purchaseDate</b> to <a href="#">TransactionInfo Data Elements</a>.</p>                                                                 |
| 29/05/2020 | 8.3.0  | 8.3.0:1 | <p><b>Installation</b> (Installation Guide)</p> <p>+ Added an option to change <b>RMI port</b> in <a href="#">Additional Administration Server Configuration Parameters</a>.</p>                                             |
|            |        |         | <p><b>Issuer Management</b> (Admin UI)</p> <p>+ Added <b>IAV generation algorithm</b> to <a href="#">New Issuer Group</a></p> <p>+ Added a warning to <b>Supported devices</b> in <a href="#">ActiveDevice Settings</a>.</p> |
|            |        |         | <p><b>Device Management</b> (Admin UI)</p> <p>+ Added <b>OOB</b> to <a href="#">Edit Default Device Parameters</a> and <a href="#">OOB</a>.</p>                                                                              |
|            |        |         | <p><b>Risk Management</b> (Admin UI)</p> <p>+ Added <a href="#">Upload Connector Encryption Key</a>.</p>                                                                                                                     |
|            |        |         | <p><b>OOB Management</b> (Admin UI)</p> <p>+ Added <a href="#">Upload Connector Encryption Key</a>.</p>                                                                                                                      |
|            |        |         | <p><b>Cards</b> (Admin UI)</p> <p>+ Added <b>Deactivated device type</b> to <b>Status</b> in <a href="#">Assigned Devices</a>.</p>                                                                                           |
|            |        |         | <p><b>CardLoader</b> (Specifications)</p> <p>+ Added encryption of sensitive data to <b>Log directory</b> in <a href="#">Open dialog for se XML file to verify</a>.</p>                                                      |
|            |        |         | <p><b>Remote Messaging</b> (Specifications)</p> <p>+ Added <b>acsTransId</b>, <b>threeDSTransId</b> and <b>dsTransId</b> to <a href="#">Table 4 - Transactic</a></p>                                                         |



| Date | AA Ver | Doc Ver | Change Details |
|------|--------|---------|----------------|
|------|--------|---------|----------------|

## Out of Band (OOB) Authentication Adapter (Specifications)

- Added samples to [Get OOB Adapter Information](#) and [Request OOB Challenge](#)
- Added new **Length** for `acctNumber` in [TransactionInfo Data Elements](#) and `cardholderName` in [CardHolderInfo Data Elements](#)
- Added **Message Inclusion** for `clientId` and `deviceId` in [AdditionalInfo Elements](#).

## Risk Engine Adapter (Specifications)

- Added [AReqWithTransStatus Data Elements](#)
- Added new **Length** for `acctNumber` and `cardholderName` in [AReq Data Elements](#)
- Added **Message Inclusion** for `clientId` in [AdditionalInfo Data Elements](#)

24/04/2020

8.2.3

8.2.3:1

## Risk Engine Adapter (Specifications)

- Changes made to [Parameter Data Elements](#)
- Change made to [Condition Data Elements](#)
- Added [ValueType Data Elements](#), [ConditionAssessor Data Elements](#), and [TxCallback Data Elements](#)
- Changes made to [ConditionValue Data Elements](#)
- Added [Range Data Elements](#)
- Change made to [messageExtension Data Elements](#)
- Removed [AdapterRiskAssessmentOutput Data Elements](#).

17/4/2020

8.2.0

8.2.0:2

## Remote Messaging (Specifications)

- Added attribute lengths to the **Usage** column of [Table 2 - VerifyRegReq, T](#), [Table 4 - Transaction](#) and [Table 14 - InitAuthReq](#).

## Out of Band (OOB) Authentication Adapter (Specifications)

- Changes made to [Out of Band \(OOB\) Authentication Adapter \(Specifications\)](#)

28/02/2020

8.2.0

8.2.0:1

## Installation (Installation Guide)

- Added **TOMCAT\_KEYSTORE**, **TOMCAT\_KEYSTORE\_PASS**, **TOMCAT\_TRUSTSTORE** and **TOMCAT\_TRUSTSTORE\_PASS** to [configuration](#)

## Issuer Management (Admin UI)

- Added **IAV generation algorithm** to [Issuer Details](#).

## Risk Management (Admin UI)

- Change made to **Score range for device** in [Add / Edit Risk Chain](#).

| Date | AA Ver | Doc Ver | Change Details |
|------|--------|---------|----------------|
|------|--------|---------|----------------|

## Servers (Admin UI)

- + Added **OOB info template** to [Edit CAAS Server](#).

## Issuers (Admin UI)

- + Added **Maximum interaction** to [Remote Settings](#).

## Cards (Admin UI)

- + Added **Client ID** to [Find Card](#) and [Card Details](#)
- + Added note to **Expiry date** in [New Card](#) and [Card Details](#).

## Transactions (Admin UI)

- + Added **Client ID** to [Find 3-D Secure](#)
- + Added **Risk decision** and **Client ID** to [Transaction Details](#).

## Local Messaging (Specifications)

- + Δ Additions & changes made for **Client ID** to:
  - Δ [Sample pre-registration request](#)
  - Δ [Sample final registration request for traditional 3-D Secure](#)
  - Δ [Sample final registration request for two-factor authentication over 3-D S](#)
  - Δ [Sample update registration request](#)
  - + [Card Device Update Request](#)
  - Δ [Sample Registration Notification](#)
  - Δ [Sample Device Update Notification](#)
  - Δ [Sample Opt-Out Notification](#)
  - Δ [Sample Lock Notification](#)
  - Δ [Cardholder Registration DTD](#).

## Remote Messaging (Specifications)

- + Added **LanCode** to [Table 3 - Card](#) and [Table 6 - CardInfo](#)
- + Added **twoFA** to [Table 6 - CardInfo](#).

| Date       | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------|--------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |        |         | <p><b>Out of Band (OOB) Authentication Adapter</b> (Specifications)</p> <ul style="list-style-type: none"> <li>Changes made to <a href="#">Adapter Interface Methods</a></li> <li>Change made to <b>Response Description</b> of <a href="#">Get OOB Adapter information</a></li> <li>Change made to <b>Response Description</b> of <a href="#">Request OOB Challenge</a></li> <li>Change made to <b>Request Method</b> and <b>Response Description</b> of <a href="#">Get OOB authentication result</a></li> <li>Added <a href="#">AdapterInfo Data Elements</a></li> <li>Change made to <b>acctNumber</b> <b>Description</b> in <a href="#">TransactionInfo Data Element</a></li> <li>Added <b>deviceId</b> to <a href="#">AdditionalInfo Data Elements</a></li> <li><a href="#">OobRequestChallengeResult Data Elements</a> added</li> <li><a href="#">OobAuthenticationResult Data Elements</a> added.</li> </ul>                                                                                                                                                                                                               |
| 10/01/2020 | 8.1.2  | 8.1.2:1 | <p><b>Installation</b> (Installation Guide)</p> <ul style="list-style-type: none"> <li>Added <b>JSON Response Elements</b> in <a href="#">ACS</a>, <a href="#">MIA</a>, <a href="#">Registration</a> and <a href="#">Enrolment</a></li> </ul> <p><b>Profile Management</b> (Admin UI)</p> <ul style="list-style-type: none"> <li>Change made to <b>2-factor authentication</b> login option in <a href="#">User Profile</a>.</li> </ul> <p><b>Remote Messaging</b> (Specifications)</p> <ul style="list-style-type: none"> <li>Change made to <b>Description</b> and <b>Sample Value</b> of <b>AuthType</b> in <a href="#">Pre Authentication Response</a>.</li> </ul> <p><b>Local Messaging</b> (Specifications)</p> <ul style="list-style-type: none"> <li>Changes made to <b>Request</b> and <b>Response</b> of <b>Cardholder Registration</b></li> <li>Changes made to <b>Request</b> and <b>Response</b> of <b>Notification</b></li> <li>Changes made to <b>Critical Card Data Encryption and Decryption</b></li> <li>Changes made to <b>Cardholder Registration</b></li> <li>Changes made to <b>Notification</b>.</li> </ul> |
| 06/12/2019 | 8.1.1  | 8.1.1:1 | <p><b>Installation</b> (Installation Guide)</p> <ul style="list-style-type: none"> <li>Added monitoring of the availability of <a href="#">ACS</a>, <a href="#">MIA</a>, <a href="#">Registration</a> and <a href="#">Enrolment</a></li> </ul> <p><b>Device Management</b> (Admin UI)</p> <ul style="list-style-type: none"> <li>Added <b>Plus (+) prefix</b> in <a href="#">SMS Center</a>.</li> </ul> <p><b>Issuers</b> (Admin UI)</p> <ul style="list-style-type: none"> <li>Change made to <a href="#">Language selection during authentication</a>: add <i>authentication process of 3-D Secure 1</i></li> <li>Change made to <a href="#">Provider Settings</a>: add JSON format examples.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Date       | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------|--------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |        |         | <p><b>Local Messaging (Specifications)</b></p> <ul style="list-style-type: none"> <li>Change made to <b>Request</b>: Update EncVectorIV</li> <li>Update Sample final registration request for <b>traditional 3-D Secure</b></li> <li>Change made to <b>Cancel Registration Request</b>: Make name attribute of ca optional</li> <li>Change made to <b>Critical Card Data Encryption and Decryption</b>: Change ke algorithm to AES</li> <li>Change made to <b>Cardholder Registration DTD</b>: Change <b>Name CDATA</b> to <b>I</b></li> </ul> |
|            |        |         | <p><b>Out of Band (OOB) Authentication Adapter (Specifications)</b></p> <ul style="list-style-type: none"> <li>Added <b>Swagger API URL</b> to <b>Restful API version of OOB Adapter</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                           |
|            |        |         | <p><b>Risk Engine Adapter (Specifications)</b></p> <ul style="list-style-type: none"> <li>Added <b>Swagger API URL</b> to <b>RESTful API Risk Adapter</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          |
|            |        |         | <p><b>Codes (Error Codes)</b></p> <ul style="list-style-type: none"> <li>Added Error codes to <b>Server Error Codes</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                            |
| 15/11/2019 | 8.1.0  | 8.1.0:1 | <p><b>Installation (Installation Guide)</b></p> <ul style="list-style-type: none"> <li>Removed <b>HSM_LIB_DIR</b> parameter from <b>Upgrades to v8.x.x</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                         |
|            |        |         | <p><b>System Management (Admin UI)</b></p> <ul style="list-style-type: none"> <li>Change made to <b>New Issuer Group</b>, <b>Issuer Group Details</b>, and <b>Issuer Data</b>. Changes <b>MAC Algorithm</b> to <b>3DS1 only</b> and changed <b>Use parent certificate public and encryption keys</b>.</li> <li>Change made to <b>Public &amp; Encryption Key Management</b>: Change key algorithm to <b>AES</b>.</li> </ul>                                                                                                                    |
|            |        |         | <p><b>Security (Admin UI)</b></p> <ul style="list-style-type: none"> <li>Added new section: <b>SDK certificate</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |
|            |        |         | <p><b>Cards (Admin UI)</b></p> <ul style="list-style-type: none"> <li>Change made to <b>New Card</b>: The card Expiry date is mandatory for Mastercard.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                             |
|            |        |         | <p><b>Risk Engine Adapter (Specifications)</b></p> <ul style="list-style-type: none"> <li>Removed one method of <b>TxCallback</b> from <b>Parameter Data Elements</b>.</li> <li>Removed <b>resultWhenTransmissionError</b> from <b>RemoteCondition Data Elements</b></li> <li>Added <b>range</b> field into <b>ConditionValue Data Elements</b></li> </ul>                                                                                                                                                                                     |

| Date       | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------|--------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 06/11/2019 | 8.0.3  | 8.0.3:1 | <p><b>Risk Engine Adapter</b> (Specifications)</p> <p>△ Change made to <b>AdapterInfo Data Elements</b>: Removed round brackets from <b>Token</b> Sample Value.</p> <p>△ Change made to <b>AssessmentResult Data Elements</b>: Change the description of <b>whatToDoNext</b></p> <p>+ <b>range</b> field added into <b>ConditionValue Data Elements</b></p>                                                                                                                                                                                                                                   |
| 09/10/2019 | 8.0.2  | 8.0.2:2 | <p><b>Remote Messaging</b> (Specifications)</p> <p>△ Change made to <b>Table 16 - VerifyAuthReq</b>: Removed round brackets from <b>Token</b> Sample Value.</p> <p><b>Out of Band (OOB) Authentication Adapter</b> (Specifications)</p> <p>+ Change made to <b>oobAuthenticationResult</b>: Add <b>PENDING</b> as a valid value</p> <p><b>Risk Engine Adapter</b> (Specifications)</p> <p>△ Updated <b>Risk chain setup diagram</b>.</p>                                                                                                                                                      |
| 02/10/2019 | 8.0.2  | 8.0.2:1 | <p><b>Installation</b> (Installation Guide)</p> <p>△ Changes made to <b>Upgrades to v8.x.x</b>: Addition of <b>HSM_LIB_DIR</b> parameter updates to JAR files which must be removed.</p> <p>+ Addition of <b>HSM_LIB_DIR</b>, <b>HSM_SLOT</b>, <b>TESTING_MODE</b>, <b>PROVIDER_TEST_AUTH_SERVER</b>, and <b>ACS_REFERENCE_NUMBER_TEST</b> to <b>Common configuration parameters</b>.</p> <p><b>Remote Messaging</b> (Specifications)</p> <p>+ Added <b>Response code = 3</b>.</p> <p><b>Codes</b> (Transaction Status Codes)</p> <p>+ Added a new page: <b>Transaction Status Codes</b>.</p> |
| 05/09/2019 | 8.0.1  | 8.0.1:1 | <p><b>Product Architecture</b> (Installation Guide)</p> <p>△ Added <b>Disaster Recovery</b> and <b>Clustering</b> diagrams.</p> <p><b>Installation</b> (Installation Guide)</p> <p>△ Changes made to <b>Upgrades to v8.0.x</b> and <b>New installations</b>.</p> <p><b>Security</b> (Admin UI)</p> <p>+ Added new <b>Key type</b> field to <b>Create Certificate Request</b>.</p>                                                                                                                                                                                                             |

| Date       | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|--------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |        |         | <p><b>Risk Engine Adapter (Specifications)</b></p> <ul style="list-style-type: none"> <li>Updated <b>Validator</b> field description in <b>ParameterDataElements</b></li> <li>Updated <b>PreviousData</b> field format in <b>RemoteAssessmentRequest Data Elements</b></li> <li>Added <b>AReqWithTransStatusDataElements</b></li> <li>Updated <b>ThreeDSComplInd</b> and <b>ThreeDSRequestorAuthenticationInd</b> field in <b>AReq Data Elements</b>.</li> </ul>                                        |
|            |        |         | <p><b>Remote Messaging (Specifications)</b></p> <ul style="list-style-type: none"> <li><b>InitAuthReq</b> table: Usage of <b>oobInfo</b> changed.</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
|            |        |         | <p><b>Out of Band (OOB) Authentication Adapter (Specifications)</b></p> <ul style="list-style-type: none"> <li>Change the URL in <b>Restful API version of OOB Adapter</b></li> <li>Change <b>NOT__AUTHENTICATED</b> to <b>NOT_AUTHENTICATED</b></li> <li>Update <b>MobilePhone Data Elements</b>, <b>HomePhone Data Elements</b>, and <b>W</b> <b>Data Elements</b>.</li> </ul>                                                                                                                        |
| 15/08/2019 | 8.0.0  | 8.0.0:1 | <p><b>Product Architecture (Installation Guide)</b></p> <ul style="list-style-type: none"> <li>Components labelled with (3DS1) or (3DS2) as relevant</li> <li>Added <b>Challenge Server (3DS2)</b>.</li> <li>Added <b>Risk Engine Adapter</b></li> <li>Added <b>Out of Band (OOB) Authentication Adapter</b></li> <li>Updated <b>Logical view of ActiveAccess</b> diagram</li> <li>Updated <b>Hardware and Software Requirements</b></li> <li>Removed references to <b>RuPay</b> components.</li> </ul> |
|            |        |         | <p><b>External Components (Installation Guide)</b></p> <ul style="list-style-type: none"> <li><b>Application Server</b> dependency removed, supports compatible Java Appl Servers.</li> </ul>                                                                                                                                                                                                                                                                                                           |
|            |        |         | <p><b>Installation (Installation Guide)</b></p> <ul style="list-style-type: none"> <li>ActiveAccess installation and setup process simplified.</li> </ul>                                                                                                                                                                                                                                                                                                                                               |
|            |        |         | <p><b>System Management (Admin UI)</b></p> <ul style="list-style-type: none"> <li><b>Authentication Management</b> section added with tabs for: <ul style="list-style-type: none"> <li><b>Device Management</b> previously under <b>System Management</b></li> <li><b>Risk Management</b> for 3DS2 risk management</li> <li><b>OOB Management</b> for OOB processing support.</li> </ul> </li> </ul>                                                                                                    |

| Date | AA Ver | Doc Ver | Change Details                                                                                                                                                                                                                                                                                                                                                                                 |
|------|--------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |        |         | <p><b>System Management (Admin UI) - Issuer Management</b></p> <p>⚠ <b>Device Settings:</b> Added <b>OOB</b> as a supported device.</p>                                                                                                                                                                                                                                                        |
|      |        |         | <p><b>Security (Admin UI)</b></p> <p>+ Added <b>Directory Server Certificate</b> section</p> <p>+ Added <b>OOB Certificate</b> section</p> <p>+ Added <b>Risk Certificate</b> section.</p>                                                                                                                                                                                                     |
|      |        |         | <p><b>Issuers (Admin UI)</b></p> <p>⚠ <b>Providers</b> parameters moved to a new page, and linked, from the <b>Settings</b> page. New fields added.</p>                                                                                                                                                                                                                                        |
|      |        |         | <p><b>Rules (Admin UI)</b></p> <p>⚠ <b>Rule Management</b> section replaces previous <b>Authentication Exemption</b> and <b>Registration</b> sections</p> <p>Tabs for:</p> <p>+ <b>Registration</b> previously <b>Force Registration</b> tab under <b>Rules</b></p> <p>⚠ <b>Authentication</b> previously <b>Authentication Exemption</b> tab under <b>Rules</b></p> <p>■ <b>Settings</b>.</p> |
|      |        |         | <p><b>Cards (Admin UI)</b></p> <p>⚠ <b>Users</b> tab renamed to <b>Cards</b>.</p>                                                                                                                                                                                                                                                                                                              |
|      |        |         | <p><b>Reports (Admin UI)</b></p> <p>⚠ Reports support reporting by 3-D Secure version.</p>                                                                                                                                                                                                                                                                                                     |
|      |        |         | <p><b>Transactions (Admin UI)</b></p> <p>⚠ <b>Find 3-D Secure:</b> supports search by 3-D Secure version. New fields added.</p>                                                                                                                                                                                                                                                                |
|      |        |         | <p><b>Admins (Admin UI)</b></p> <p>⚠ <b>Admin User Details</b> and <b>User Profile:</b> added <b>2-factor authentication</b> login</p>                                                                                                                                                                                                                                                         |
|      |        |         | <p><b>Local Messaging (Specifications)</b></p> <p>⚠ Updated <b>Final Registration Request</b> with OOB device registration request</p>                                                                                                                                                                                                                                                         |

| Date | AA Ver | Doc Ver | Change Details |
|------|--------|---------|----------------|
|------|--------|---------|----------------|

## Remote Messaging (Specifications)

-  Added **issuerName** and **theeDSPProtocolVersion** in **Transaction** table
-  Added **HeaderParams** table
-  Added **AdditionalParams** table
-  Added **AuthType** in **PreAuthResp** table
-  Added new OTP types for **AuthType** and **oobInfo** in **InitAuthReq** table
-  [Sample Request Response](#): changed **CVD** to NULL.

## CHANGES TO DOCUMENTATION STRUCTURE

-  All documentation moved online with the ability to print to PDF

**To print the entire ActiveAccess documentation:** click the  button on the [Introduction](#) page.

**To print a section:** click the  button on that section.

**Tip:** hovering your mouse over the  button will let you see which section will be printed.

-  See [Documentation change details](#) for full details of the changes in the documentation moving from PDF to online format.

|            |       |         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------|-------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 26/02/2019 | 7.4.6 | 7.4.6.1 | <h2>Remote Messaging</h2> <ul style="list-style-type: none"> <li> Added <b>AuthType</b> in <b>initAuthReq</b> table</li> <li> Updated RegToken definition in <b>CardInfo</b> table.</li> </ul>                                                                                                                                                                                                                        |
| 06/07/2018 | 7.4.0 | 7.4.0:1 | <ul style="list-style-type: none"> <li> Addition of options in <b>System Management &gt; Settings</b> to allow administrators to specify access levels to view Card Number (plaintext) and AAV/CAVV/AEV</li> <li> Updated description of Soft Launch List</li> <li> Addition of ActiveAccess Error Codes in Appendix A.</li> </ul> |



# Documentation change details

| Online Main Menu                        | Sub Menus                                              | Previous PDF Document / Latest Changes                                                    |
|-----------------------------------------|--------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#">Introduction</a>            |                                                        |                                                                                           |
| <a href="#">Installation Guide &gt;</a> |                                                        | A11-Install_Maint_TechRef.pdf                                                             |
|                                         | <a href="#">Product Architecture</a>                   |                                                                                           |
|                                         | <a href="#">External Components</a>                    |                                                                                           |
|                                         | <a href="#">Installation</a>                           |                                                                                           |
| <a href="#">Administration UI &gt;</a>  |                                                        | AA12-ActiveAccess Administration.pdf                                                      |
|                                         | <a href="#">About the Issuer Administration Server</a> | AA12 / Added support for two-factor authentication for logging into the Administration UI |
|                                         | <a href="#">System Management &gt;</a>                 | AA12                                                                                      |
|                                         | <a href="#">About System Management</a>                | AA12                                                                                      |
|                                         | <a href="#">Settings</a>                               | AA12                                                                                      |
|                                         | <a href="#">ACS Settings</a>                           | AA12                                                                                      |
|                                         | <a href="#">Issuer Management</a>                      | AA12                                                                                      |
|                                         | <a href="#">- Group Management</a>                     | AA12                                                                                      |
|                                         | <a href="#">- Authentication Mgmt &gt;</a>             | <b>New Subsection</b>                                                                     |
|                                         | <a href="#">- About Authentication Management</a>      | <b>New</b>                                                                                |

| Online Main Menu | Sub Menus                              | Previous PDF Document / Latest Changes |
|------------------|----------------------------------------|----------------------------------------|
|                  | - Devices                              | AA12, previously Device Management     |
|                  | - Risk                                 | <b>New</b>                             |
|                  | - OOB                                  | <b>New</b>                             |
|                  | Public & Encryption Key Management     | AA12                                   |
|                  | Exchange Configuration                 | AA12                                   |
|                  | Archive Management                     | AA12                                   |
|                  | <b>Security</b>                        | AA12                                   |
|                  | - Issuer Certificate                   | AA12                                   |
|                  | - AHS Certificate                      | AA12                                   |
|                  | - CAAS Certificate                     | AA12                                   |
|                  | - Directory Server Certificate         | <b>New</b>                             |
|                  | - OOB Certificate                      | <b>New</b>                             |
|                  | - Risk Certificate                     | <b>New</b>                             |
|                  | - CA Certificate                       | AA12                                   |
|                  | <b>Servers</b>                         | AA12                                   |
|                  | - MIA Servers                          | AA12                                   |
|                  | - Access Control Servers (ACS)         | AA12                                   |
|                  | - Authentication History Servers (AHS) | AA12                                   |

| Online Main Menu | Sub Menus                                                                     | Previous PDF Document / Latest Changes |
|------------------|-------------------------------------------------------------------------------|----------------------------------------|
|                  | - <a href="#">Centralised Authentication and Authorisation Servers (CAAS)</a> | AA12                                   |
|                  | - <a href="#">Out of Band Authentication Servers (OOB)</a>                    | AA12                                   |
|                  | - <a href="#">Risk Servers</a>                                                | AA12                                   |
|                  | <b>Utilities &gt;</b>                                                         |                                        |
|                  | <a href="#">Utilities</a>                                                     | AA12                                   |
|                  | <a href="#">Key Retiring Utility</a>                                          | AA12                                   |
|                  | <b>Issuers</b>                                                                | AA12                                   |
|                  | - <a href="#">Settings</a>                                                    | AA12                                   |
|                  | - <a href="#">Upload Registration Files</a>                                   | AA12                                   |
|                  | - <a href="#">Custom Pages</a>                                                | AA12                                   |
|                  | - <a href="#">Key Management</a>                                              | AA12                                   |
|                  | <b>Rules</b>                                                                  |                                        |
|                  | - <a href="#">Registration</a>                                                | AA12                                   |
|                  | -- Amount Threshold                                                           |                                        |
|                  | -- Merchant Blacklist                                                         |                                        |
|                  | - <a href="#">Authentication</a>                                              | AA12                                   |
|                  | -- Soft Launch List Rule                                                      |                                        |
|                  | -- Merchant Whitelist Rule                                                    |                                        |
|                  | -- Merchant Watchlist                                                         |                                        |
|                  | -- Location Watchlist                                                         |                                        |
|                  | - Location Watchlist Search Results                                           |                                        |
|                  | -- Domestic & International Transaction Amount Threshold                      |                                        |
|                  | -- Stand-In Transaction Threshold                                             |                                        |

| Online Main Menu      | Sub Menus                           | Previous PDF Document / Latest Changes                       |
|-----------------------|-------------------------------------|--------------------------------------------------------------|
|                       | <a href="#">- Settings</a>          | AA12                                                         |
|                       | <a href="#">Admin Users</a>         | AA12                                                         |
|                       | <a href="#">Cards</a>               | AA12 <b>Users</b> renamed to <b>Cards</b>                    |
|                       | <a href="#">Transactions</a>        | AA12                                                         |
|                       | <a href="#">Reporting</a>           | AA12                                                         |
|                       | <a href="#">Audit Log</a>           | AA12                                                         |
|                       | <a href="#">Profile Management_</a> | AA12                                                         |
| <b>Specifications</b> |                                     |                                                              |
|                       | <b>Local Messaging &gt;</b>         |                                                              |
|                       | Local Messaging                     | AA61-Messaging Specification.pdf                             |
|                       | Card Loader                         | AA32-GPayments Card Loader.pdf                               |
|                       | <b>Remote Messaging &gt;</b>        |                                                              |
|                       | Remote Messaging                    | AA71-Remote System Messaging Specification.pdf               |
|                       | Country and Currency Codes          | AA71-Remote System Messaging Specification.pdf<br>Appendix A |
|                       | Sample Card                         | AA71-Remote System Messaging Specification.pdf<br>Appendix B |
|                       | Sample Request Response             | AA71-Remote System Messaging Specification.pdf<br>Appendix C |
|                       | SMS via JMS                         | AA83-ActiveAccess - SMS via JMS Library.pdf                  |
|                       | Out of Band Authentication Adapter  | <b>New</b>                                                   |

| Online Main Menu            | Sub Menus                                  | Previous PDF Document / Latest Changes          |
|-----------------------------|--------------------------------------------|-------------------------------------------------|
|                             | Risk Engine Adapter                        | <b>New</b>                                      |
| <b>Error Codes</b>          |                                            | AA12 - Appendix A                               |
| <b>Glossary</b>             |                                            | AA12                                            |
| <b>Document Control&gt;</b> |                                            |                                                 |
|                             | Document Control                           | AA12                                            |
|                             | Documentation Changes ( <i>this page</i> ) | <b>New</b>                                      |
| <b>Release Notes</b>        |                                            | Previously included in the ActiveAccess package |
| <b>Legal Notices</b>        |                                            | AA12                                            |

# Release Notes

## ActiveAccess v8.4.4

[25/11/2020]

[EOL: Two years after the subsequent version's release date]

| Type        | Issue Number | Description                                  | Components                                   |
|-------------|--------------|----------------------------------------------|----------------------------------------------|
| ENHANCEMENT | #550         | Update Risk Engine Integrated in CAAS        | Access Control Server                        |
| FIX         | #572         | SDK issue for remote issuer                  | Access Control Server                        |
| FIX         | #574         | HMAC256 key creation error for Luna Provider | Access Control Server, Issuer Administration |

## ActiveAccess v8.4.3

[13/11/2020]

[EOL: 25/11/2022]

| Type | Issue Number | Description                                                                                                     | Components            |
|------|--------------|-----------------------------------------------------------------------------------------------------------------|-----------------------|
| FIX  | 560          | Fixed 3DS1 remote authentication issue when authType = 10                                                       | Access Control Server |
| FIX  | 563          | Fixed issue of formatting purchase date in CAAS API logs                                                        | Access Control Server |
| FIX  | 564          | Fixed acs.war issue of formatting purchase date displaying in Remote/Local issuer authentication challenge page | Access Control Server |

## ActiveAccess v8.4.2

[27/10/2020]

[EOL: 13/11/2022]

| Type        | Issue Number | Description                                                                                                             | Components            |
|-------------|--------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------|
| ENHANCEMENT |              | Enhancement on the remote issuer custom pages: both 3DS1 and 3DS2 remote authentication custom pages should be uploaded | Access Control Server |
| FIX         | 549          | Added version in schema.xsd at acs.war/WEB-INF/lib/caas.client-*.jar                                                    | Access Control Server |
| FIX         | 552          | Restore authType compatibility: authType can be used for authentication methods 1-15                                    | Access Control Server |

## ActiveAccess v8.4.1

[16/10/2020]

[EOL: 27/10/2022]

| Type        | Issue Number | Description                                                                 | Components            |
|-------------|--------------|-----------------------------------------------------------------------------|-----------------------|
| ENHANCEMENT | #528         | Support multi-instance for OOB Notifier                                     | Access Control Server |
| FIX         | #485         | Update authentication methods                                               | Access Control Server |
| FIX         | #514         | Mastercard 3DS2.1: generation of authentication method dropdown on the page | Access Control Server |
| FIX         | #525         | PAReq - invalid session                                                     | Access Control Server |
| FIX         | #530         | Issue with adding sms-centers to issuers on MIA                             | Issuer Administration |

| Type | Issue Number | Description                                          | Components                                                               |
|------|--------------|------------------------------------------------------|--------------------------------------------------------------------------|
| FIX  | #533         | Issue retrieving the wsUrl (Remote Issuer)           | Access Control Server                                                    |
| FIX  |              | General fixes, performance and security enhancements | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.4.0

[02/10/2020]

[EOL: 16/10/2022]

| Type        | Issue Number | Description                                                                                  | Components                                   |
|-------------|--------------|----------------------------------------------------------------------------------------------|----------------------------------------------|
| ENHANCEMENT | #348         | Support new Visa Secure CAVV Usage 3, Version 7 and add an option to select the algorithm    | Access Control Server, Issuer Administration |
| ENHANCEMENT | #383         | Separate SDK html pages from BRW html pages                                                  | Access Control Server                        |
| ENHANCEMENT | #387         | Remove Continue button & add support for auto-submission of OOB page - Remote Authentication | Access Control Server, Issuer Administration |
| ENHANCEMENT | #455         | Display IAV generation algorithm in Transaction Details                                      | Access Control Server, Issuer Administration |
| ENHANCEMENT | #457         | Extend OOB Adapter Challenge Request API with purchase date and time element                 | Access Control Server                        |
| ENHANCEMENT | #467         | Assign multiple SMS devices to cards that have different SMSC                                | Registration Server                          |
| ENHANCEMENT | #482         | Configurable log for number of DB connections                                                | Access Control Server                        |



| Type        | Issue Number | Description                                                                                                            | Components                                   |
|-------------|--------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| ENHANCEMENT | #498         | Compatibility with Visa authentication page requirements                                                               | Access Control Server                        |
| FIX         | #437         | Pages do not stretch to the entire height of the device - AnyBank_Remote Custompages_3DS2 - incorrect page display     | Access Control Server                        |
| FIX         | #440         | Error during decryption in CardDeviceUpdate                                                                            | CardLoader, Registration Server              |
| FIX         | #454         | Failed 3DS2 transaction details in MIA                                                                                 | Access Control Server, Issuer Administration |
| FIX         | #460         | Error during retrieving messageExtension from session                                                                  | Access Control Server                        |
| FIX         | #462         | Actions for when OobAuthenticationResult indicates cardholder did not perform OOB auth or there was a connection issue | Access Control Server                        |
| FIX         | #483         | SessionID logging                                                                                                      | Access Control Server                        |
| FIX         | #486         | CAVV issue - PAN length must be 16                                                                                     | Access Control Server                        |
| FIX         | #492         | Amount without separator                                                                                               | Access Control Server                        |
| FIX         | #493         | Fix \$PurchaseDateTime format in SMS messages                                                                          | Access Control Server                        |
| FIX         | #494         | The xslTransform not finished                                                                                          | Access Control Server                        |
| FIX         | #495         | 3DS2 Challenge errors flow                                                                                             | Access Control Server                        |
| FIX         | #499         | Incorrect data in MIA Reports                                                                                          | Issuer Administration                        |
| FIX         | #503         | Error during parsing sessionInfo when cardId is UUID for Remote Issuers                                                | Access Control Server                        |
| FIX         | #504         | Remote page issue - OOB initAuth error                                                                                 | Access Control Server                        |

| Type | Issue Number | Description                                          | Components                                                               |
|------|--------------|------------------------------------------------------|--------------------------------------------------------------------------|
| FIX  | #509         | SDK sessionKey should be saved in DB                 | Access Control Server                                                    |
| FIX  |              | General fixes, performance and security enhancements | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.3.6

[07/08/2022]

[EOL: 02/10/2022]

| Type        | Issue Number | Description                                                                         | Components                                                               |
|-------------|--------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| ENHANCEMENT | #450         | Save valid messages with Invalid ISO codes                                          | Access Control Server                                                    |
| FIX         | #437         | Text displayed incorrectly when token is entered on Remote Authentication pages     | Access Control Server                                                    |
| FIX         | #446         | Display issue for 3DS1 Local Authentication when OOB + SMS was assigned to the card | Access Control Server                                                    |
| FIX         | #447         | Disabled the validation of cardholder name for 3DS2 authentication                  | Access Control Server                                                    |
| FIX         |              | General fixes, performance and security enhancements                                | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.3.5 (Patch)

[16/07/2020]

[EOL: 07/08/2022]

| Type | Issue Number | Description                                           | Components            |
|------|--------------|-------------------------------------------------------|-----------------------|
| FIX  | #441         | AAV generation issue for 3DS1 Mastercard transactions | Access Control Server |

## ActiveAccess v8.3.4 (Patch)

[09/07/2020]

[EOL: 16/07/2022]

| Type | Issue Number | Description                                              | Components            |
|------|--------------|----------------------------------------------------------|-----------------------|
| FIX  | #441         | Removing cancel button in XSL pages for SDK transactions | Access Control Server |

## ActiveAccess v8.3.3 (Patch)

[06/07/2020]

[EOL: 09/07/2022]

| Type        | Issue Number | Description                                            | Components            |
|-------------|--------------|--------------------------------------------------------|-----------------------|
| ENHANCEMENT | #441         | Additional logs added for 3DS1 Mastercard transactions | Access Control Server |

## ActiveAccess v8.3.2 (Patch)

[26/06/2020]

[EOL: 06/07/2022]

| Type | Issue Number | Description                                       | Components            |
|------|--------------|---------------------------------------------------|-----------------------|
| FIX  | #441         | Extending the Message Length for SDK transactions | Access Control Server |

## ActiveAccess v8.3.1 (Patch)

[12/06/2020]

[EOL: 26/06/2022]

| Type        | Issue Number | Description                                | Components            |
|-------------|--------------|--------------------------------------------|-----------------------|
| ENHANCEMENT | #441         | Additional logs added for SDK transactions | Access Control Server |

## ActiveAccess v8.3.0

[29/05/2020]

[EOL: 12/06/2022]

| Type        | Issue Number | Description                                             | Components                                          |
|-------------|--------------|---------------------------------------------------------|-----------------------------------------------------|
| ENHANCEMENT | #158         | OTP & password option for OOB                           | Issuer Administration, Access Control Server        |
| ENHANCEMENT | #274         | Encrypting critical data such as cardnumber in adapters | Issuer Administration, Access Control Server        |
| ENHANCEMENT | #325         | Encryption of card number in CardLoader logs            | CardLoader                                          |
| ENHANCEMENT | #343         | IAV method option for Mastercard PSD2 in Issuer groups  | Issuer Administration, Access Control Server        |
| ENHANCEMENT | #328         | RMI configuration option                                | Setup, Issuer Administration, Access Control Server |

| Type        | Issue Number | Description                                                                               | Components                                                               |
|-------------|--------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| ENHANCEMENT | #403         | Add 3DS2 transactional data into CAAS messages                                            | Access Control Server                                                    |
| ENHANCEMENT | #423         | MIA to notify user when device is removed from Issuer's Active Device list                | Issuer Administration                                                    |
| ENHANCEMENT | #429         | Remove case sensitivity of OobRequestChallengeResult.requestChallengeEnum accepted values | Access Control Server                                                    |
| FIX         | #370         | OOB deviceId length issue                                                                 | Registration Server                                                      |
| FIX         | #373         | FileNotFoundException during RBA and OOB startup                                          | Access Control Server                                                    |
| FIX         | #421         | 10-CR challenge authentication issue                                                      | Access Control Server                                                    |
| FIX         | #427         | Updated ECI values for AMEX, JCB and Diners                                               | Access Control Server                                                    |
| FIX         | #438         | Change SecureCode HMAC 256 key                                                            | Issuer Administration                                                    |
| FIX         |              | General fixes, performance and security enhancements                                      | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.2.6 (Patch)

[07/05/2020]

[EOL: 29/05/2022]

| Type | Issue Number | Description                                                 | Components                                                               |
|------|--------------|-------------------------------------------------------------|--------------------------------------------------------------------------|
| FIX  | #375         | Stop ACS from uploading CustomPages for AnyBank at start up | Issuer Administration                                                    |
| FIX  | #420         | NullPointerException during SMS device loading              | Access Control Server                                                    |
| FIX  | #426         | MIA Report error                                            | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.2.5 (Patch)

[04/05/2020]

[07/05/2022]

| Type | Issue Number | Description                                    | Components            |
|------|--------------|------------------------------------------------|-----------------------|
| FIX  | #420         | NullPointerException during SMS device loading | Access Control Server |

## ActiveAccess v8.2.4 (Patch)

[28/04/2020]

[04/05/2022]

| Type | Issue Number | Description                                    | Components            |
|------|--------------|------------------------------------------------|-----------------------|
| FIX  | #420         | NullPointerException during SMS device loading | Access Control Server |

## ActiveAccess v8.2.3 (Patch)

[24/04/2020]

[28/04/2022]

| Type | Issue Number | Description                                                                   | Components            |
|------|--------------|-------------------------------------------------------------------------------|-----------------------|
| FIX  | #419         | Issue with ACS authentication pages and authentication results cannot be seen | Access Control Server |

## ActiveAccess v8.2.2

[17/04/2020]

[24/04/2022]

| Type | Issue Number | Description                                                    | Components                   |
|------|--------------|----------------------------------------------------------------|------------------------------|
| FIX  | #371         | Fixes to Frictionless Flow, Browser, PA (Result = N)           | Access Control Server        |
| FIX  | #412         | Luna HSM KeyStore loading issue                                | Access Control Server, Setup |
| FIX  | #413         | RSA key size for new issuers and issuer groups changed to 2048 | Access Control Server, Setup |
| FIX  | #416         | Fixes to Frictionless Flow, 3RI, and NPA (Result = Y)          | Access Control Server        |

## ActiveAccess v8.2.1

[09/04/2020]

[EOL: 17/04/2022]

| Type        | Issue Number | Description                                                          | Components            |
|-------------|--------------|----------------------------------------------------------------------|-----------------------|
| ENHANCEMENT | #331         | Addition of cancel link to 3DS2 authentication pages                 | Access Control Server |
| ENHANCEMENT | #369         | Addition of "store name", "date" and "amount" to authentication page | Access Control Server |

| Type | Issue Number | Description                                                                 | Components                                             |
|------|--------------|-----------------------------------------------------------------------------|--------------------------------------------------------|
| FIX  | #349         | null cardName in verifyRegResp produces an error                            | Access Control Server                                  |
| FIX  | #371         | Changes to the validation date of cardLoader generated certificate          | CardLoader                                             |
| FIX  | #393         | Misplacement of elements in responsive view of custom pages                 | Access Control Server                                  |
| FIX  | #394         | NullPointerException error while processing regStatus=1 in CAAS             | Access Control Server                                  |
| FIX  | #395, 400    | ClientID=null not to be included in Notification Reports, OOB & RBA APIs    | Access Control Server, CardLoader, Registration Server |
| FIX  | #396         | Exception during initializing LunaProvider in gpcomp.updater                | Setup                                                  |
| FIX  | #397, #399   | Archive database schema upgrade from ActiveAccess v7.3 to ActiveAccess v8.2 | Issuer Administration, Setup                           |
| FIX  | #407         | Configuration of "ACS challenge URL" for issuers                            | Access Control Server                                  |

## ActiveAccess v8.2.0

[27/03/2020]

[EOL: 09/04/2022]

| Type        | Issue Number | Description                                          | Components                                   |
|-------------|--------------|------------------------------------------------------|----------------------------------------------|
| ENHANCEMENT | #151         | Support push notifications during OOB authentication | Access Control Server, Registration Server   |
| ENHANCEMENT | #174         | IAV method option for Mastercard PSD2                | Access Control Server, Issuer Administration |



| Type        | Issue Number | Description                                                                         | Components                                                                    |
|-------------|--------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| ENHANCEMENT | #192         | Displaying OTP+StaticPassword for CAAS                                              | Access Control Server                                                         |
| ENHANCEMENT | #221         | Displaying risk decision in Transaction Details page                                | Issuer Administration                                                         |
| ENHANCEMENT | #307         | Addition of a new card attribute: ClientID                                          | Access Control Server, CardLoader, Issuer Administration, Registration Server |
| ENHANCEMENT | #316         | Card and Transaction search performance improvement                                 | Issuer Administration                                                         |
| ENHANCEMENT | #319         | "Score range for device" in RBA allows for selection from all devices including OOB | Access Control Server                                                         |
| ENHANCEMENT | #323         | Addition of "Maximum interaction" limit for Remote Issuers                          | Access Control Server, Issuer Administration                                  |
| FIX         | #234         | Fix for CAASSESSION table lock issue                                                | Access Control Server                                                         |
| FIX         | #315         | Fix for archive and purge features                                                  | Issuer Administration                                                         |
| FIX         | #353         | Reverting Card Expiry Date to optional                                              | Issuer Administration, Registration Server                                    |
| FIX         |              | General fixes, performance and security enhancements                                | Setup, Issuer Administration, Access Control Server, Registration Server      |

## ActiveAccess v8.1.2

[10/01/2020]

[EOL: 28/02/2022]

| Type        | Issue Number | Description                                                                          | Components                                                                          |
|-------------|--------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| ENHANCEMENT | #228         | Adding forgot password link for browser device channel                               | Access Control Server                                                               |
| ENHANCEMENT | #251         | Send tokens only when the Resend OTP link is clicked                                 | Access Control Server                                                               |
| ENHANCEMENT | #268         | Changes to PreAuth in Remote Authentication model                                    | Access Control Server                                                               |
| ENHANCEMENT | #299         | Improvements to enabling 2FA for admin users                                         | Issuer Administration                                                               |
| ENHANCEMENT | #300         | Device selection when two OOB devices are assigned to a card                         | Access Control Server                                                               |
| ENHANCEMENT | #312         | Addition of DESede support to CardLoader and Registration for backward compatibility | Registration Server, CardLoader                                                     |
| FIX         | #271         | Fixing Ping Command connection issue                                                 | Issuer Administration, Access Control Server, Registration Server, Enrolment Server |
| FIX         |              | General fixes, performance and security enhancements                                 | Setup, Issuer Administration, Access Control Server, Registration Server            |

## ActiveAccess v8.1.1

[06/12/2019]

[EOL: 10/01/2022]

| Type        | Issue Number | Description                                             | Components                      |
|-------------|--------------|---------------------------------------------------------|---------------------------------|
| ENHANCEMENT | #267         | Add new CancelReg request with optional cardholder name | Registration Server, CardLoader |

| Type        | Issue Number | Description                                             | Components                                                                          |
|-------------|--------------|---------------------------------------------------------|-------------------------------------------------------------------------------------|
| ENHANCEMENT | #271         | ActiveAccess Ping command improvement                   | Issuer Administration, Access Control Server, Registration Server, Enrolment Server |
| FIX         | #303         | Invalidate empty cardholder name in PreReg and FinalReg | Registration Server, CardLoader                                                     |

## ActiveAccess v8.1.0

[15/11/2019]

[EOL: 06/12/2021]

| Type        | Issue Number | Description                                                                    | Components                                   |
|-------------|--------------|--------------------------------------------------------------------------------|----------------------------------------------|
| ENHANCEMENT | #92          | Acceptable values for <b>App unsupported devices</b> updated                   | Access Control Server, Issuer Administration |
| ENHANCEMENT | #131         | Supporting two-factor authentication for local authentication                  | Access Control Server, Issuer Administration |
| ENHANCEMENT | #142         | Changing the risk/rule decision process                                        | Access Control Server                        |
| ENHANCEMENT | #143         | Provide a mechanism to test OOB and RBA restful adapters connect/read timeouts | Access Control Server, Issuer Administration |
| ENHANCEMENT | #179         | Including more data in RBA call back                                           | Access Control Server                        |
| ENHANCEMENT | #198         | Updating the approach of populating the historical transaction for RBA         | Access Control Server                        |
| ENHANCEMENT | #201         | Create a swagger for OOB and Risk restful adapters                             | Access Control Server                        |
| ENHANCEMENT | #246         | Enabling language selection during authentication for 3DS1                     | Access Control Server, Issuer Administration |

| Type        | Issue Number | Description                                                          | Components            |
|-------------|--------------|----------------------------------------------------------------------|-----------------------|
| ENHANCEMENT | #273         | Http protocol version for external connections                       | Access Control Server |
| FIX         | #53          | 3DS method notification post data                                    | Access Control Server |
| FIX         | #95          | ACS decision based on risk chain score in remote authentication      | Access Control Server |
| FIX         | #260         | HSM installation issues                                              | Setup                 |
| FIX         | #266         | Detach SDK certificates from Issuer Certificates                     | Setup                 |
| FIX         | #278         | CAAS Server throws NullPointerException when message category is NPA | Access Control Server |

## ActiveAccess v8.0.4

[06/11/2019]

[EOL: 15/11/2021]

| Type | Issue Number | Description                      | Components            |
|------|--------------|----------------------------------|-----------------------|
| FIX  | #281         | Invalid Request to Remote Server | Access Control Server |

## ActiveAccess v8.0.3

[25/10/2019]

[EOL: 06/11/2021]

| Type | Issue Number | Description                                   | Components   |
|------|--------------|-----------------------------------------------|--------------|
| FIX  | #277         | Deployment of registration.war during startup | Registration |

| Type | Issue Number | Description                                                     | Components            |
|------|--------------|-----------------------------------------------------------------|-----------------------|
| FIX  | #278         | CAAS throws a NullPointerException when message category is NPA | Access Control Server |

## ActiveAccess v8.0.2

[09/10/2019]

[EOL: 25/10/2021]

| Type        | Issue Number | Description                                                                                     | Components                                   |
|-------------|--------------|-------------------------------------------------------------------------------------------------|----------------------------------------------|
| ENHANCEMENT | #51          | Support 3DS2 purchase amount 0 for Mastercard IDC                                               | Access Control Server                        |
| ENHANCEMENT | #98          | Update ECI for Message Category NPA for Mastercard IDC                                          | Access Control Server                        |
| ENHANCEMENT | #219         | Making acsReferenceNumber configurable for testing purposes                                     | Issuer Administration, Access Control Server |
| ENHANCEMENT | #223         | Addition of decline code to preAuthResp of CAAS                                                 | Access Control Server                        |
| ENHANCEMENT | #229         | Addition of KeyStore and TrustStore for RBA Server                                              | Access Control Server                        |
| ENHANCEMENT | #233         | Addition of KeyStore and TrustStore for OOB Server                                              | Access Control Server                        |
| FIX         | #132         | Updates to Mastercard IDC status codes                                                          | Access Control Server                        |
| FIX         | #148         | Remote CAAS PreAuth changes                                                                     | Access Control Server                        |
| FIX         | #226         | Setup could not generate RSA2048 keys for the MAP error during Luna PKCS11 installation/upgrade | Setup                                        |

| Type | Issue Number | Description                                                                               | Components                                                               |
|------|--------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| FIX  | #242         | Verified by Visa references changed to Visa Secure in the content of authentication pages | Access Control Server                                                    |
| FIX  |              | General fixes, performance and security enhancements                                      | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.0.1

[05/09/2019]

[EOL: 02/10/2021]

| Type        | Issue Number | Description                                                  | Components                                          |
|-------------|--------------|--------------------------------------------------------------|-----------------------------------------------------|
| ENHANCEMENT | #169         | EULA update                                                  | Issuer Administration                               |
| ENHANCEMENT | #208         | Grant scripts run automatically during setup                 | Setup                                               |
| FIX         | #172         | Device selection page isn't being shown                      | Access Control Server                               |
| FIX         | #182         | Device registration fails when issuer has OOB device enabled | Access Control Server                               |
| FIX         | #186         | Exception raised during Diners Club remote authentication    | Access Control Server                               |
| FIX         | #188         | ChallengeResponse failure in remote authentication           | Access Control Server                               |
| FIX         | #189         | Risk adapter configuration page issue                        | Issuer Administration                               |
| FIX         | #193         | Generate RSA 2048 when the EC key generation fails           | Setup, Issuer Administration, Access Control Server |

| Type | Issue Number | Description                                                   | Components                                                               |
|------|--------------|---------------------------------------------------------------|--------------------------------------------------------------------------|
| FIX  | #196         | CardLoader setup.sh doesn't work                              | CardLoader                                                               |
| FIX  | #203         | Upgrade issue from 7.4.2 to 8.0.0 with currency exchange rate | Setup                                                                    |
| FIX  |              | General fixes, performance and security enhancements          | Setup, Issuer Administration, Access Control Server, Registration Server |

## ActiveAccess v8.0.0

[15/08/2019]

[EOL: 05/09/2021]

| Type        | Issue Number | Description                                          | Components                                                               |
|-------------|--------------|------------------------------------------------------|--------------------------------------------------------------------------|
| ENHANCEMENT | #93          | Enhancements to the Administration interface (MIA)   | Issuer Administration                                                    |
| ENHANCEMENT | #5468        | Support incremental database schema changes in Setup | Setup                                                                    |
| ENHANCEMENT | #5801        | Web Container Neutralization                         | Setup                                                                    |
| ENHANCEMENT | #6659        | Support for 3-D Secure 2.1                           | Setup, Issuer Administration, Access Control Server, Registration Server |
| ENHANCEMENT | #6661        | 3DS2 Transaction search based on 3DS version         | Issuer Administration                                                    |
| ENHANCEMENT | #6663        | Support for 3DS2 Risk Management                     | Issuer Administration, Access Control Server                             |
| ENHANCEMENT | #6664        | Support 3DS2 Reporting                               | Issuer Administration                                                    |

| Type        | Issue Number | Description                                                                                                 | Components                                          |
|-------------|--------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| ENHANCEMENT | #7207        | Support for OOB Processing                                                                                  | Issuer Administration, Access Control Server        |
| ENHANCEMENT | #7383        | Substitute Triple DES encryption in ActiveAccess with stronger cryptography                                 | Issuer Administration, Access Control Server        |
| ENHANCEMENT | #7845        | Removal of RuPay component                                                                                  | Setup, Issuer Administration                        |
| ENHANCEMENT | #7880        | Two-factor authentication for MIA login                                                                     | Issuer Administration                               |
| ENHANCEMENT | #8082        | Simplify the setup process                                                                                  | Setup                                               |
| ENHANCEMENT | #8310        | SPA2 algorithm for AAV generation                                                                           | Setup, Issuer Administration, Access Control Server |
| FIX         | #5425        | MIA allows exceeded password length and updates it successfully                                             | Access Control Server                               |
| FIX         | #7297        | Adminlog and AuditlogCollectorErrors have been updated to fix the errors that occurred during scheduler job | Access Control Server                               |
| FIX         | #8160        | Authentication Exemption Rules for CAAS server                                                              | Access Control Server                               |

## ActiveAccess v7.4.7 (Patch)

[23/03/2019]

[EOL: 15/08/2021]

| Access Control Server |       |                                                                                    |
|-----------------------|-------|------------------------------------------------------------------------------------|
| FIX                   | #8147 | Fixed the purchAmount field to avoid the mismatch of value between PAREs and PAREq |



## ActiveAccess v7.4.6 (Patch)

[05/03/2019]

[EOL: 23/03/2021]

|                       |  |  |
|-----------------------|--|--|
| Issuer Administration |  |  |
|-----------------------|--|--|

|     |       |                                                 |
|-----|-------|-------------------------------------------------|
| FIX | #8022 | Removing "+" sign when sending message via JMS. |
|-----|-------|-------------------------------------------------|

|                       |  |  |
|-----------------------|--|--|
| Access Control Server |  |  |
|-----------------------|--|--|

|     |       |                                                 |
|-----|-------|-------------------------------------------------|
| FIX | #8022 | Removing "+" sign when sending message via JMS. |
|-----|-------|-------------------------------------------------|

## ActiveAccess v7.4.5 (Patch)

[01/02/2019]

[EOL: 05/03/2021]

|                       |  |  |
|-----------------------|--|--|
| Access Control Server |  |  |
|-----------------------|--|--|

|             |       |                                                              |
|-------------|-------|--------------------------------------------------------------|
| ENHANCEMENT | #7843 | Displaying the Mobile Number on Remote Authentication pages. |
|-------------|-------|--------------------------------------------------------------|

|             |       |                                                                                 |
|-------------|-------|---------------------------------------------------------------------------------|
| ENHANCEMENT | #7893 | Adding PurchaseExponent attribute to the transaction table of requests to CAAS. |
|-------------|-------|---------------------------------------------------------------------------------|

## ActiveAccess v7.4.4 (Patch)

[27/09/2018]

[EOL: 01/02/2021]

|                       |  |  |
|-----------------------|--|--|
| Issuer Administration |  |  |
|-----------------------|--|--|

|     |       |                                                                                                                                     |
|-----|-------|-------------------------------------------------------------------------------------------------------------------------------------|
| FIX | #7748 | SMS delivery fails as ACS sends the phone number without the '+' sign to SMPP client. ACS now includes the + sign when sending SMS. |
|-----|-------|-------------------------------------------------------------------------------------------------------------------------------------|

| Access Control Server |  |  |
|-----------------------|--|--|
|-----------------------|--|--|

|     |       |                                                                                                                                     |
|-----|-------|-------------------------------------------------------------------------------------------------------------------------------------|
| FIX | #7748 | SMS delivery fails as ACS sends the phone number without the '+' sign to SMPP client. ACS now includes the + sign when sending SMS. |
|-----|-------|-------------------------------------------------------------------------------------------------------------------------------------|

## ActiveAccess v7.4.3 (Patch)

[18/09/2018]

[EOL: 27/09/2020]

| Issuer Administration |  |  |
|-----------------------|--|--|
|-----------------------|--|--|

|     |       |                                                                                                                                                   |
|-----|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| FIX | #7718 | Card Registration File Upload Errorcard file. Clearing the timer to prevent "java.lang.IllegalStateException: Timer already canceled" exceptions. |
|-----|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|

## ActiveAccess v7.4.2

[20/08/2018]

[EOL: 07/06/2020]

| Issuer Administration |  |  |
|-----------------------|--|--|
|-----------------------|--|--|

|             |       |                                              |
|-------------|-------|----------------------------------------------|
| ENHANCEMENT | #7543 | ISO 3166 Update country details for Eswatini |
|-------------|-------|----------------------------------------------|

|             |       |                               |
|-------------|-------|-------------------------------|
| ENHANCEMENT | #7654 | ISO 4217 Amendment Number 169 |
|-------------|-------|-------------------------------|

| Active Control Server |  |  |
|-----------------------|--|--|
|-----------------------|--|--|

|             |       |                                              |
|-------------|-------|----------------------------------------------|
| ENHANCEMENT | #7543 | ISO 3166 Update country details for Eswatini |
|-------------|-------|----------------------------------------------|

|             |       |                               |
|-------------|-------|-------------------------------|
| ENHANCEMENT | #7654 | ISO 4217 Amendment Number 169 |
|-------------|-------|-------------------------------|

|     |       |                                                |
|-----|-------|------------------------------------------------|
| FIX | #7677 | CurrencyExchange error in ActiveAccess startup |
|-----|-------|------------------------------------------------|

**Registration Server**

|     |       |                               |
|-----|-------|-------------------------------|
| FIX | #7639 | Card Registration File Upload |
|-----|-------|-------------------------------|

## ActiveAccess v7.4.1 (Patch)

[08/08/2018]

[EOL: 20/08/2020]

**Issuer Administration**

|     |       |                                                      |
|-----|-------|------------------------------------------------------|
| FIX | #7557 | Verification code not received for Email device type |
|-----|-------|------------------------------------------------------|

**Active Control Server**

|     |       |                             |
|-----|-------|-----------------------------|
| FIX | #7482 | Custom Pages layout updates |
|-----|-------|-----------------------------|

|     |       |                                                      |
|-----|-------|------------------------------------------------------|
| FIX | #7557 | Verification code not received for Email device type |
|-----|-------|------------------------------------------------------|

## ActiveAccess v7.4.0

[06/07/2018]

[EOL: 08/08/2020]

**Setup**

|             |       |                                       |
|-------------|-------|---------------------------------------|
| ENHANCEMENT | #6479 | External HSM setup - PKCS #11 Support |
|-------------|-------|---------------------------------------|

|             |       |                                  |
|-------------|-------|----------------------------------|
| ENHANCEMENT | #7470 | Update key type for CVC2 process |
|-------------|-------|----------------------------------|

|             |       |                               |
|-------------|-------|-------------------------------|
| ENHANCEMENT | #7471 | HMAC key length update for MC |
|-------------|-------|-------------------------------|

|             |       |                                            |
|-------------|-------|--------------------------------------------|
| ENHANCEMENT | #7477 | Support HSMs in which DES is not available |
|-------------|-------|--------------------------------------------|

|             |       |                                                  |
|-------------|-------|--------------------------------------------------|
| ENHANCEMENT | #7519 | Upgraded log4j from 1.2.13 to the 1.2.17 version |
|-------------|-------|--------------------------------------------------|

|     |       |                                                                  |
|-----|-------|------------------------------------------------------------------|
| FIX | #7380 | Visa 3-D Secure Security Program - Encryption of CAVV/AAV values |
|-----|-------|------------------------------------------------------------------|

| Setup |  |  |
|-------|--|--|
|-------|--|--|

FIX #7518 Updated GET\_CARDS procedure

| Issuer Administration |  |  |
|-----------------------|--|--|
|-----------------------|--|--|

ENHANCEMENT #6479 External HSM setup - PKCS #11 Support

ENHANCEMENT #7359 ISO 4217 Amendment Number 166

ENHANCEMENT #7470 Update key type for CVC2 process

ENHANCEMENT #7471 HMAC key length update for MC

ENHANCEMENT #7477 Support HSMs in which DES is not available

ENHANCEMENT #7519 Upgraded log4j from 1.2.13 to the 1.2.17 version

FIX #7329 Public key for the Issuer Group

FIX #7380 Visa 3-D Secure Security Program - Encryption of CAVV/AAV values

FIX #7520 Purge processor is already running error

| Access Control Server |  |  |
|-----------------------|--|--|
|-----------------------|--|--|

ENHANCEMENT #6479 External HSM setup - PKCS #11 Support

ENHANCEMENT #7359 ISO 4217 Amendment Number 166

ENHANCEMENT #7482 Combining two device registration custom pages into one

ENHANCEMENT #7519 Upgraded log4j from 1.2.13 to the 1.2.17 version

FIX #7047 Updating the path of caaswarning.properties to keep it unchanged during the upgrade process

FIX #7380 Visa 3-D Secure Security Program - Encryption of CAVV/AAV values

**Access Control  
Server**

|     |       |                             |
|-----|-------|-----------------------------|
| FIX | #7518 | Updated GET_CARDS procedure |
|-----|-------|-----------------------------|

**Enrolment Server**

|             |       |                                       |
|-------------|-------|---------------------------------------|
| ENHANCEMENT | #6479 | External HSM setup - PKCS #11 Support |
|-------------|-------|---------------------------------------|

|             |       |                                                  |
|-------------|-------|--------------------------------------------------|
| ENHANCEMENT | #7519 | Upgraded log4j from 1.2.13 to the 1.2.17 version |
|-------------|-------|--------------------------------------------------|

**Registration Server**

|             |       |                                       |
|-------------|-------|---------------------------------------|
| ENHANCEMENT | #6479 | External HSM setup - PKCS #11 Support |
|-------------|-------|---------------------------------------|

|             |       |                                                  |
|-------------|-------|--------------------------------------------------|
| ENHANCEMENT | #7519 | Upgraded log4j from 1.2.13 to the 1.2.17 version |
|-------------|-------|--------------------------------------------------|

## ActiveAccess v7.3.3 (Patch)

[25/05/2018]

[EOL: 06/07/2018]

**Access Control Server**

|     |       |                                                                  |
|-----|-------|------------------------------------------------------------------|
| FIX | #7402 | Incorrect JCB transaction status with 'Card Not Found' from CAAS |
|-----|-------|------------------------------------------------------------------|

## ActiveAccess v7.3.2 (Patch)

[29/03/2018]

[EOL: 25/05/2020]

**Access Control Server**

|     |       |                                  |
|-----|-------|----------------------------------|
| FIX | #7160 | Remove error on missing MD field |
|-----|-------|----------------------------------|

## ActiveAccess v7.3.1 (Patch)

[20/02/2018]

[EOL: 29/03/2020]

| Access Control Server |       |                                        |
|-----------------------|-------|----------------------------------------|
| FIX                   | #7116 | JCB VReq with Browser.deviceCategory=1 |

## ActiveAccess v7.3.0

[29/01/2018]

[EOL: 20/02/2020]

| Setup |       |                                                          |
|-------|-------|----------------------------------------------------------|
| FIX   | #6334 | Correction to the casing for SafeNet in setup/sample.ini |
| FIX   | #6338 | Remove WebSphere application server option from setup    |
| FIX   | #6986 | Decryption error during notification report process      |
| FIX   | #7052 | Notification reports - java.lang.NullPointerException    |

| Issuer Administration |       |                                                                                       |
|-----------------------|-------|---------------------------------------------------------------------------------------|
| FIX                   | #6406 | Exception thrown when clicking Back on Matched Rule Details page                      |
| FIX                   | #6244 | Update the default value for AMEX 'Maximum forgot password attempts                   |
| FIX                   | #6620 | MIA incorrectly searches the WEB-INF folder for cacerts, instead of the config folder |
| FIX                   | #6645 | Cards do not get assigned to the most detailed BIN                                    |
| FIX                   | #7052 | Notification reports - java.lang.NullPointerException                                 |

| Issuer Administration |       |                                                                                                    |
|-----------------------|-------|----------------------------------------------------------------------------------------------------|
| ENHANCEMENT           | #4131 | Authentication pages compatibility with mobile devices                                             |
| ENHANCEMENT           | #5935 | New authentication method Email OTP                                                                |
| ENHANCEMENT           | #6252 | ISO 3166 Update country details for Moldova and Gambia                                             |
| ENHANCEMENT           | #6308 | Addition of a message on MIA's blank screen for admin users of Issuers with an invalid license key |
| ENHANCEMENT           | #6377 | Option to defer application of Setting changes to next server restart                              |
| ENHANCEMENT           | #6463 | ISO 4217 Currency Code Service - Amendment number 163                                              |
| ENHANCEMENT           | #6527 | Mastercard Identity Check Support                                                                  |
| ENHANCEMENT           | #6688 | JCB Attempt process                                                                                |
| ENHANCEMENT           | #6727 | Security enhancements                                                                              |
| ENHANCEMENT           | #6765 | All PANs must now comply with the Luhn algorithm and pass a Mod-10 check                           |
| ENHANCEMENT           | #6773 | ISO 4217 Amendment Number 164                                                                      |
| ENHANCEMENT           | #6823 | Rules Settings challenge option for 'not exempted authentications' as per IDC requirements         |
| ENHANCEMENT           | #6981 | ISO 4217 Amendment Number 165                                                                      |
| Access Control Server |       |                                                                                                    |
| FIX                   | #5686 | Proof of Attempt = Disabled still displays the opt-out link during ADS                             |
| FIX                   | #6244 | Update the default value for AMEX 'Maximum forgot password attempts                                |
| FIX                   | #6417 | PAReq is not logged by ACS when the Authentication Exemption Rules are used                        |

| Access Control Server |       |                                                                                                   |
|-----------------------|-------|---------------------------------------------------------------------------------------------------|
| FIX                   | #6687 | Updating error details wording to match 3DS v1.0.2 document                                       |
| FIX                   | #6693 | Errors related to JCB compliance test                                                             |
| FIX                   | #7037 | Authentication Exemption rules do not apply during transactions                                   |
| ENHANCEMENT           | #4131 | Authentication pages compatibility with mobile devices                                            |
| ENHANCEMENT           | #5935 | New authentication method Email OTP                                                               |
| ENHANCEMENT           | #6209 | Style applied to XML formatted error pages displayed during authentication                        |
| ENHANCEMENT           | #6252 | ISO 3166 Update country details for Moldova and Gambia                                            |
| ENHANCEMENT           | #6463 | ISO 4217 Currency Code Service - Amendment number 163                                             |
| ENHANCEMENT           | #6527 | Mastercard Identity Check Support                                                                 |
| ENHANCEMENT           | #6652 | Compliance with JCB J/Secure                                                                      |
| ENHANCEMENT           | #6688 | JCB Attempt process                                                                               |
| ENHANCEMENT           | #6689 | Addition of new data elements in JCB Authentication page and updates to the masking format of PAN |
| ENHANCEMENT           | #6691 | Remove AHS support for JCB                                                                        |
| ENHANCEMENT           | #6692 | Multi-language support of JCB pages                                                               |
| ENHANCEMENT           | #6727 | Security enhancements                                                                             |
| ENHANCEMENT           | #6765 | All PANs must now comply with the Luhn algorithm and pass a Mod-10 check                          |
| ENHANCEMENT           | #6773 | ISO 4217 Amendment Number 164                                                                     |
| ENHANCEMENT           | #6823 | Rules Settings challenge option for 'not exempted authentications' as per IDC requirements        |



**Access Control  
Server**

ENHANCEMENT      #6981      ISO 4217 Amendment Number 165

**Enrolment Server**

ENHANCEMENT      #6705      The effect of 'Uses confirmation' field in Enrolment

ENHANCEMENT      #6727      Security enhancements

**Registration Server**

FIX      #6396      CardLoader error message does not correspond with Registration logs

ENHANCEMENT      #5935      New authentication method Email OTP

ENHANCEMENT      #6527      Mastercard Identity Check Support

ENHANCEMENT      #6727      Security enhancements

## ActiveAccess v7.2.1

[20/04/2017]

[EOL: 29/01/2020]

Setup v7.2.1

Issuer Administration v7.2.1

Access Control Server v7.2.1

Enrolment Server v7.2.1

Registration Server v7.2.1

**Setup**

ENHANCEMENT      #6289      Encode hsmpassword parameter (Base64) in RuPay config file.

|                       |  |  |
|-----------------------|--|--|
| Issuer Administration |  |  |
|-----------------------|--|--|

|             |       |                                                             |
|-------------|-------|-------------------------------------------------------------|
| FIX         | #4584 | PCI Key Retiring utility performance issue.                 |
| FIX         | #6182 | Certificate creation failure.                               |
| ENHANCEMENT | #6289 | Encode hsmpassword parameter (Base64) in RuPay config file. |

|                       |  |  |
|-----------------------|--|--|
| Access Control Server |  |  |
|-----------------------|--|--|

|             |       |                                                              |
|-------------|-------|--------------------------------------------------------------|
| FIX         | #4584 | PCI Key Retiring utility performance issue.                  |
| FIX         | #6186 | Error while processing a custom page.                        |
| ENHANCEMENT | #4217 | Addition of JCB XSL pages into the standard release package. |
| ENHANCEMENT | #6289 | Encode hsmpassword parameter (Base64) in RuPay config file.  |

|                  |  |  |
|------------------|--|--|
| Enrolment Server |  |  |
|------------------|--|--|

|             |       |                                                             |
|-------------|-------|-------------------------------------------------------------|
| ENHANCEMENT | #6289 | Encode hsmpassword parameter (Base64) in RuPay config file. |
|-------------|-------|-------------------------------------------------------------|

|                     |  |  |
|---------------------|--|--|
| Registration Server |  |  |
|---------------------|--|--|

|             |       |                                                             |
|-------------|-------|-------------------------------------------------------------|
| ENHANCEMENT | #6289 | Encode hsmpassword parameter (Base64) in RuPay config file. |
|-------------|-------|-------------------------------------------------------------|

## ActiveAccess v7.2.0

[22/12/2016]

[EOL: 20/04/2019]

Setup v7.2.0

Issuer Administration v7.2.0

Access Control Server v7.2.0

Enrolment Server v7.2.0

## Registration Server v7.2.0

### Rupay v1.1.0

### Card Loader 1.1.41

| Setup        |       |                                                                     |
|--------------|-------|---------------------------------------------------------------------|
| SUPPORT:     | #5806 | nCipherKM.jar being removed in installation                         |
| ENHANCEMENT: | #5474 | Support silent mode installation                                    |
| ENHANCEMENT: | #5939 | Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files |
| ENHANCEMENT: | #5574 | Remove usage of deprecated JRE classes                              |
| FEATURE:     | #5546 | Supports Amex Safekey compliance (rev 2016)                         |

| Issuer Administration |       |                                                                                                                                                                |
|-----------------------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIX:                  | #5525 | Encrypt critical data in case of registration failure                                                                                                          |
| FIX:                  | #5899 | Archive history details page display error                                                                                                                     |
| SUPPORT:              | #5729 | Visa Intermediate SHA2 CA cert added for new installations                                                                                                     |
| ENHANCEMENT:          | #5574 | Remove usage of deprecated JRE classes                                                                                                                         |
| ENHANCEMENT:          | #5740 | Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries |
| ENHANCEMENT:          | #5829 | Remove restriction on using previous CAVV key                                                                                                                  |
| ENHANCEMENT:          | #5874 | Support p7 and der files when installing certificates                                                                                                          |
| ENHANCEMENT:          | #5939 | Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files                                                                                            |
| FEATURE:              | #5546 | Supports Amex Safekey compliance (rev 2016)                                                                                                                    |

| Access Control Server |       |                                                                                                                                                                |
|-----------------------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIX:                  | #4584 | Improve PCI Key Retiring utility performance*                                                                                                                  |
| FIX:                  | #5965 | CAAS Card Auth Data format not found error. The error message is logged in ACS logs during a remote transaction regardless of success of the transaction.      |
| FIX:                  |       | Various spelling corrections in application and XSL files                                                                                                      |
| SUPPORT:              | #5748 | Error in restarting Number of authentication exemptions and Sum of exempted authentications' amounts when empty cardholder name is received from CAAS server   |
| SUPPORT:              | #5785 | Unable to establish connection to CAAS                                                                                                                         |
| SUPPORT:              | #5903 | Optimise GET_CARDS procedure                                                                                                                                   |
| SUPPORT:              | #5952 | Update American Express SafeKey logo                                                                                                                           |
| ENHANCEMENT:          | #5054 | Support SafeNet Network HSM (Cloud HSM/Luna SA)                                                                                                                |
| ENHANCEMENT:          | #5546 | Compliance with American Express Safekey (revision 2016)                                                                                                       |
| ENHANCEMENT:          | #5574 | Remove usage of deprecated JRE classes                                                                                                                         |
| ENHANCEMENT:          | #5740 | Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries |
| ENHANCEMENT:          | #5939 | Encode HSM_PASSWORD parameter (Base64) in ActiveAccess config files                                                                                            |
| FEATURE:              | #5546 | Supports Amex Safekey compliance (rev 2016)                                                                                                                    |

| Enrolment Server |       |                                                           |
|------------------|-------|-----------------------------------------------------------|
| FIX:             |       | Various spelling corrections in application and XSL files |
| ENHANCEMENT:     | #5574 | Remove usage of deprecated JRE classes                    |

| Enrolment Server |  |  |
|------------------|--|--|
|------------------|--|--|

ENHANCEMENT: #5740 Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries

ENHANCEMENT: #5939 Encode HSM\_PASSWORD parameter (Base64) in ActiveAccess config files

| Registration Server |  |  |
|---------------------|--|--|
|---------------------|--|--|

SUPPORT: #5767 Changing request Id length in notification request to be at most 1024 characters

ENHANCEMENT: #5574 Remove usage of deprecated JRE classes

ENHANCEMENT: #5740 Exclusion of third party XML parser libraries (JAXP libraries),Third party XML parser libraries (JAXP libraries) excluded and replaced with JDK JAXP libraries

ENHANCEMENT: #5939 Encode HSM\_PASSWORD parameter (Base64) in ActiveAccess config files

| RuPay |  |  |
|-------|--|--|
|-------|--|--|

FIX: #5482 Search by Error Code field in Transaction screens

FIX: #6025 RuPay verifyRegistration did not forward contextBlob to initAuthentication. contextBlob now included

FIX: #6026 Support authType in addition to authTypeSupList in RuPay

| Card Loader |  |  |
|-------------|--|--|
|-------------|--|--|

FIX: #5779 CardLoader now supports Java 8

SUPPORT: #5767 Changing request Id length in notification request to be at most 1024 characters

ENHANCEMENT: #5574 Remove usage of deprecated JRE classes

## ActiveAccess v7.1.4

[03/10/2016]

[EOL: 22/12/2018]

### Setup v7.1.4

### Issuer Administration v7.1.4

### Access Control Server v7.1.4

### Enrolment Server v7.1.4

### Registration Server v7.1.4

| Issuer Administration |       |                                                                                       |
|-----------------------|-------|---------------------------------------------------------------------------------------|
| Support               | #5703 | Database connectivity issue                                                           |
| Bug                   | #5720 | ActiveAccess 7.1.4 beta 5 installation error: no record found                         |
| Enhancement           | #5715 | Version class in ActiveAccess should be filtered in Maven                             |
| Support               | #5664 | Login issue with remote issuers' business and helpdesk admins without access to rules |
| Support               | #5548 | FileNotFoundException: auditconfig.properties changed from an Error to a Warning      |
| Bug                   | #5745 | CSR Export Issue                                                                      |

| Access Control Server |       |                                    |
|-----------------------|-------|------------------------------------|
| Support               | #5703 | Database connectivity issue        |
| Bug                   | #5689 | CAAS: ISO currency & country codes |
| Enhancement           | #5523 | Risk Based Authentication          |
| Bug                   | #5674 | DB Warning Logger in ACS log file  |

| Access Control Server |       |                                                           |
|-----------------------|-------|-----------------------------------------------------------|
| Enhancement           | #5715 | Version class in ActiveAccess should be filtered in Maven |
| Enhancement           | #5688 | Copyright of XSL pages                                    |
| Bug                   | #5685 | AHS logging PATransReq twice in the acs log file          |
| Support               | #5646 | Merchant URL Must be URL pattern                          |
| Support               | #5634 | PARes with parameter SSID to MPI                          |
| Support               | #5616 | A null priSec value results in NullPointerException       |
| Enhancement           | #5596 | Support for unmasked CH.fullIPAN in PATRANSReq messages   |

| Enrolment Server |  |  |
|------------------|--|--|
|------------------|--|--|

Enhancement #5715 Version class in ActiveAccess should be filtered in Maven

| Registration Server |  |  |
|---------------------|--|--|
|---------------------|--|--|

Enhancement #5715 Version class in ActiveAccess should be filtered in Maven

| Setup |  |  |
|-------|--|--|
|-------|--|--|

Bug #5735 RuPay tables missing in database after installation

Enhancement #5715 Version class in ActiveAccess should be filtered in Maven

Bug #5678 RuPay module being installed without being selected (Centos 6.x)

Bug #5562 No rupay WAR files found in tomcat/webapps when installing AA with Rupay option

## ActiveAccess v7.1.3

[03/09/2016]

[EOL: 03/10/2018]

Setup v7.1.3

Issuer Administration v7.1.3

Access Control Server v7.1.3

Enrolment Server v7.1.3

Registration Server v7.1.3

|                       |  |  |
|-----------------------|--|--|
| Access Control Server |  |  |
|-----------------------|--|--|

Bug

#5619

SignatureMethod must be SHA1

No changes in other components



# Legal Notices

## Confidentiality Statement

GPayments reserves all rights to the confidential information and intellectual property contained in this document. This document may contain information relating to the business, commercial, financial or technical activities of GPayments. This information is intended for the sole use of the recipient, as the disclosure of this information to a third party would expose GPayments to considerable disadvantage. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any process without prior written permission. This information is provided under an existing non-disclosure agreement with the recipient.

## Copyright Statement

This work is Copyright © 2003-2019 by GPayments Pty Ltd. All Rights Reserved. No permission to reproduce or use GPayments Pty Ltd copyright material is to be implied by the availability of that material in this or any other document.

All third party product and service names and logos used in this document are trade names, service marks, trademarks, or registered trademarks of their respective owners.

The example companies, organizations, products, people and events used in screenshots in this document are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

## Disclaimer

GPayments Pty Ltd makes no, and does not intend to make any, representations regarding any of the products, protocols or standards contained in this document. GPayments Pty Ltd does not guarantee the content, completeness, accuracy or suitability of this information for any purpose. The information is provided "as is" without express or implied warranty and is subject to change without notice. GPayments Pty Ltd disclaims all warranties with regard to this information, including all implied warranties of merchantability and fitness for a particular purpose and any warranty against infringement. Any determinations and/or statements made by GPayments Pty

Ltd with respect to any products, protocols or standards contained in this document are not to be relied upon.

## Liability

In no event shall GPayments Pty Ltd be liable for any special, incidental, indirect or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) whether in an action of contract, negligence or other tortious action, rising out of or in connection with the use or inability to use this information or the products, protocols or standards described herein, even if GPayments has been advised of the possibilities of such damages.

# GPayments