Release Notes
RSA Authentication Agent API 8.6 for C

June 2016

Introduction

The RSA Authentication Agent Application Programming Interface (API) 8.6 for C enables developers to integrate RSA SecurID into custom or third-party applications. Use the RSA Authentication API 8.6 to integrate with Authentication Manager 8.1 Service Pack 1 or later.

This document lists what's new and changed in RSA Authentication Agent API 8.6 for C, as well as workarounds (wherever application) for known issues. Read this document before installing the software. This document contains the following sections:

What's New in This Release

This section describes the major changes introduced in this release. For detailed information on each change, refer to the *RSA Authentication Agent API 8.6 for C Developer's Guide*.

FIPS Support

RSA Authentication Agent API 8.6 for C incorporates FIPS-compliant cryptographic library module RSA BSAFE® Micro Edition Suite (MES) 4.1.5.0 that inherits its FIPS 140-2 status from RSA BSAFE® Crypto-C Micro Edition (ME) 4.1.2.0 (NIST Certificate # 2294). For more information, see the *RSA BSAFE Crypto-C Micro Edition Security Policy Level 1* document at **https://community.rsa.com/docs/DOC-41885**.

Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules (FIPS 140-2) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website: **http://www.nist.gov/**.

RSA Authentication Agent API 8.6 incorporates libraries that were independently audited by the NIST certified laboratory Gossamer laboratories Inc., an independent accredited lab under the National Voluntary Laboratory Accreditation Program (NVLAP Lab Code 200997-0). The base version of the cryptographic library incorporated into Authentication Manager was certified as FIPS compliant. This covers all algorithms that were required to be tested at the time of the certification.

RSA Authentication API 8.6 supports the Federal Information Processing Standards (FIPS). Dynamically linked BSAFE libraries are included in the kit.

The **lib** folder in the kit contains the following BSAFE libraries:

- For Windows: **ccme_asym.dll**, **ccme_base.dll**, **cryptocme.dll**, **cryptocme.sig**
- For Linux: **libccme_asym.so**, **libccme_base.so**, **libcryptocme.sig**, **libcryptocme.so**

You must specify the location of the BSAFE libraries with the RSA_BSAFE_LIBRARY_PATH tag in the **rsa_api.properties** file. The **rsa_api.properties** file is required in the SDK 8.6.

Note: Only FIPS mode is supported. You cannot use the SDK 8.6 without FIPS support.

New APIs for TCP Support

These APIs are only supported with the TCP protocol and SDK 8.6:

- **AceAgentStatusDisplayEx** obtains the last known status and configuration information for the realm. This function assists in writing customized utility applications, to check the configuration and connection status, and to perform test authentication.

  This API is similar to AceAgentStatusDislay, but AceAgentStatusDisplayEx supports showing both IPv4 and IPv6 addresses configured to the RSA Authentication Manager server. You can still use AceAgentStatusDisplay if you only have IPv4 addresses.

- **GetAuthSDKVersion** gets a copy of the string value containing the SDK version. This value can be retrieved at any time before or after a call to AceInitialize because the API does not depend on the value retrieved from RSA Authentication Manager.

Support for Additional Windows and Linux Platforms

Windows Server 2012 R2 and Red Hat Enterprise Linux 7.1 are now qualified and supported. Only Windows and Linux platforms are supported in this release. For the complete list, see the *Developer's Guide*.

Direct Migration from the SDK 8.1 and SDK 8.5

You can migrate to SDK 8.6 from either SDK 8.1 or SDK 8.5. For instructions, see the *Developer's Guide*.

Backward Compatibility

After migrating from SDK 8.1, the SDK 8.6 will not communicate with RSA Authentication Manager 6.1 and 7.1. However, if required, code that integrates with both the 8.1 SDK and the 8.6 SDK can be written to preserve backward compatibility.

For information about backward compatibility with older versions of the APIs, see the *Developer's Guide*.

IPv6 Support

RSA Authentication SDK 8.6 implements the TCP protocol, instead of the traditional UDP protocol. RSA Authentication SDK 8.6 allows agent hosts to be on an IPv4, IPv6, or a dual-stack machine.

You can verify the status of the Authentication Manager by running the code given in the sample code file **acestatusEx**. This returns the status of each Authentication Manager on which the agent is registered as an agent host, and provides details including server name and server IP address. The sample displays both the IPv4 and IPv6 addresses of each server. T

For information on the differences between the TCP protocol implemented in the SDK 8.6 and SDK 8.5, and the UDP protocol implemented in SDK 8.1, see the *Developer's Guide*.

Software Development Kit Contents

When you download and extract the SDK (.zip or.tar file), the SDK creates the directory structure outlined in the following table.

Directory	Contents
\doc	Contains the RSA Authentication Agent API 8.6 for C Developer's Guide in PDF format (**auth_agent_API_C_dev_guide)**. This guide provides an overview of the RSA Authentication Agent API for C, and describes all the functions in detail.
\inc	Contains the header files required for integrating with the Authentication API.
\lib	Includes the libraries required for each of the supported operating systems.
\samples	Contains samples that illustrate the application of the API.
\src	Contains files used to modify the Message Catalog for windows and non-windows.
\util	Contains acestatus, acestatusEX, acetest, and the ns_load utility.

Product Documentation

The following documentation is in the *Auth SDK* in the ***doc*** directory.

Title	Filename
Developer's Guide	**\doc\auth_agent_API_C_dev_guide.pdf**

Fixed Issues

This section lists issues that have been fixed in this release.

AAC-585 — In the **rsa_api.properties** file, the RSA_LOG_FILE_LOC tag specifies a log file location that can include a complete log filename. If a log filename is not specified, the file **aceclnt.log** is created. If the directory is invalid, the SDK does not start.

AAC-599 — Fixed an issue in which an invalid log file location did not generate an error message. If the log file location specified with the RSA_LOG_FILE_LOC tag in **rsa_api.properties** is invalid, the SDK fails to initialize, but an "Invalid Path" error is logged through the Debugger on Windows and to stderr in Linux.

AAC-643 — In the **rsa_api.properties** file, you can choose to enter an entire directory path or only a drive location for tags such as SDNDSCRT_LOC and RSA_CONFIG_DATA_LOC.

AAC-680 — You can use **config.xml** to set the connection timeout value.

AAC-755 — Fixed a memory allocation issue in which stress testing with 100,000 simulated authentications increased memory usage from 2 MB to 12 MB.

Known Issues

This section describes issues that remain unresolved in this release.

IPv6 addresses are not supported for the RSA RADIUS Server

Tracking Number: AAC-431
Problem: RSA RADIUS does not support IPv6 addresses on the server. In RSA Authentication Manager 8.1 Service Pack 1 or later, only RSA RADIUS clients can use IPv6 addresses.
Workaround: There is no workaround for this issue.

AceStatus and AceStatusEX do not display server status

Tracking Number: AAC-756
Problem: Server status is not implemented in this release.
Workaround: There is no workaround for this issue.

Cross-realm authentication does not work with the TCP protocol

Tracking Number: AAC-584
Problem: Cross-realm authentication does not successfully complete using the TCP protocol.
Workaround: There is no workaround for this issue.

Error occurs when over 1000 authentications are attempted concurrently on a single instance

Tracking Number: AAC-611
Problem: Some authentications do not succeed when too many authentications are attempted concurrently.
Workaround:

1. Add a replica instance.

   OR

1. Login to the AM server using SSH and locate /opt/rsa/am/server/config/.
2. Increase the max-open-sock-count property value to 2000 for biztier in the **config.xml** file.
3. Restart the processes with **/opt/rsa/am/server/rsaserv restart all**.

The acestatus utility does not display accurate Server Release information

Tracking Number: AAC-630
Problem: The acestatus utility does not accurately display the Server Release information because Patch and Hotfix information is not displayed.
Workaround: To see accurate server version information, in the Authentication Manager Security Console, go to the Software Version Information page.

SDK message key on machine with daylight saving time expires one hour before configured time

Tracking Number: AAC-657
Problem: When SDK is deployed on a machine with a time zone that has daylight saving time (DST), the message key in SDK that is used to encrypt and decrypt AuthRequest and AuthResponse expires before the configured expiration time in Authentication Manager. The expiration time depends on the daylight savings for that particular time zone. For example, if the default message key expiration time is eight hours and the machine is in the central daylight time (CDT) time zone (which has one-hour daylight savings), then the key expires in seven hours, instead of eight hours. This issue occurs when DST is active on the machine. This issue does not cause authentication failures.
Workaround: The administrator should not configure the key expiration time in Authentication Manager to be less than the daylight saving time of the SDK machine. The default value of key expiration is eight hours.

Support and Service

You can access community and support information on RSA Link at **https://community.rsa.com**. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at **www.rsaready.com** provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Trademarks

Intellectual Property Notice