THALES

gemalto
a Thales company

Gemalto Customer Documentation 2.0

RELEASE NOTES

Issue Date: 18 April 2019
Document Part Number: <PartNumber> Rev. A

Contents

Release Overview

This section describes what's new in this release and flags any product advisories.

Product Description

Provide a brief description of the product.

Release Description

Provide a brief description of the release.

New Features and Enhancements

Provide a brief description of the features and enhancements introduced in this release.

Feature

the new feature.

Enhancement

Provide a brief description of the enhancement to an existing feature.

Advisory Notes

This section highlights important issues you should be aware of before deploying this release.

Customer Advisory

Provide a brief description of the customer advisory.

Known and Resolved Issues

This section lists the issues that are known to exist in this release, and that have been resolved in this release. The following table defines the severity of the issues listed in this section.

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

Known Issues

The following issues are known to exist in the product at the time of release.

Issue	Severity	Synopsis
(Jira_Issue) Issue summary	H	**Problem:** Description of the problem. **Workaround:** Problem workaround.
(LHSM-12345) 32-bit JVM Java on 64-bits CentOS does not run if SELinux is enabled.	M	**Problem:** If SELinux is enabled, you cannot run a 32-bit JVM on a 64-bit OS. **Workaround:** Disable SELinux.

Resolved Issues

The following issues are fixed in this release.

Issue	Severity	Synopsis
(Jira_Issue) Issue summary	H	**Problem:** Description of the problem. **Resolution:** What was does to resolve the issue.
(181030) LunaProvider: RSA-PSS should use non-zero default salt length	M	**Problem:** The Luna provider's RSA-PSS implementation uses a 0-byte salt if no parameters are given. This is a security hazard, since without a salt the PSS algorithm loses the randomness that makes it effective. RFC 4055 recommends using a salt no shorter than the hash length used in the signature. **Resolution:** The default hash used in the signature is SHA-1. The default salt has therefore been set to 20 bytes.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> 📝 **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.