DigiCert® PKI Platform

Release Notes

Version 8.19

May 29, 2019

digicert®

Legal Notice

The product described in this document is provided by DigiCert, Inc. and distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of DigiCert, Inc. and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DIGICERT, INC. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The licensed software and documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the licensed software and documentation by the U.S. Government shall be solely in accordance with the terms of this documentation.

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com/

DigiCert® PKI Platform 8.19 Release Notes

DigiCert PKI Platform is a cloud-hosted service provided by DigiCert, Inc., which acquired Symantec's Website Security and related PKI solutions business on October 31, 2017.

This document includes the following topics:

- What's New in 8.19
- Component Support Updates
- Platform Support Updates
- Documentation
- Issues Addressed and Known Issues

What's New in 8.19

This release notes accompany the delivery of the DigiCert PKI Platform 8.19 release, henceforth referred to as PKI Platform.

PKI Platform is a cloud-hosted service, so your enterprise receives the latest releases as soon as the service is live.

Table 1 New in 8.19

New to 8.19	Description
DigiCert brand for all portals and solution components	Re-branding the Symantec Portals and Components to DigiCert.
Implementation of Email Domain Validation for S/MIME certificates	As per new Mozilla policy requirements, we support various methods of validation, which includes Email Validation, File Auth, or DNS TXT. For more details, refer to: KB article.
Integration with Microsoft Intune-SCEP workflow	Integration of DigiCert PKI Platform system and Microsoft Intune to issue certificates through SCEP enrollment flow. For more details, refer to: KB article.
Support for SafeNet Network HSM 7	DigiCert PKI Enterprise Gateway and Autoenrollment Server supports SafeNet Network HSM 7, both in FIPS and non-FIPS Mode, Cloning and Export Mode. For more details, refer to: KB article.
Support for nShield Connect	DigiCert PKI Enterprise Gateway and Autoenrollment Server support for nCipher's nShiled HSM.
Support for Windows Server 2016	DigiCert PKI Enterprise Gateway, Autoenrollment Server and LKMS support for Windows Server 2016.
PKI Client support for Android devices	Addition of an updated play store application (DigiCert PKI Client for Android) to support certificate enrollment from Android devices
Removal of Adobe certificate templates	Removal of Adobe Individual, Adobe Organization and Adobe CDS certificate templates from accounts that have either not deployed the template or have issued certificates from such template(s) which have now expired. For more details, refer to: KB article.

Component Support Updates

All software components are available from the **Resources** page within the PKI Manager web portal.

Table 2 Optional components that PKI Platform 8.19 supports

Components	Version Supported
PKI Client	2.17.9
PKI Enterprise Gateway, including Autoenrollment Server	1.19
PKI Web Services	8.19

[a] PKI Platform 8.19 supports previous versions of PKI Client. However, you must run v2.17.9 or higher to benefit from the features that are described in this release notes.

Platform Support Updates

PKI Platform 8.19 supports the following platforms and operating systems.

NOTE: In addition to the supported platforms and operating systems, PKI Platform and its components may work on other platforms or operating systems. However, DigiCert does not guarantee technical support related to issues that may arise on platforms or operating systems that are not listed here.

PKI Manager

PKI Manager is a web portal hosted in DigiCert's data center. It allows PKI Platform administrators to perform account, user, certificate, and key management tasks.

Table 3 - PKI Manager operating system and browser support

Operating systems	Browsers
Windows 7 Enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 66
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 66
Windows 10 Enterprise edition (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 66

[a] Edge Mode on Internet Explorer is supported.

PKI Certificate Services

PKI Certificate Services are webpages hosted in DigiCert's data center that enable users to request, install, renew and recover encryption certificates.

Table 4 - PKI Certificate Services operating system and browser support

Operating systems	Browsers
Windows 7 enterprise edition SP1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 66
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 66
Windows 10 (32-bit and 64-bit)	Internet Explorer 11[a, b] Firefox 66
macOS Sierra (10.12)	Safari 11.1.2 Firefox 66
macOS High Sierra (10.13)	Safari 11.1.2 Firefox 66

[a] The renewal plug-in is not supported in Internet Explorer 11 if Enhanced Protection Mode (EPM) is enabled. EPM is disabled by default in Internet Explorer 11.

[b] Edge mode is not supported.

PKI Client

PKI Client is middleware software for digital signing, authentication, and data protection for desktop-based applications. It uses digital certificates on smart cards, security devices, or users' workstations.

Table 5 - PKI Client operating systems and browser support

Operating systems	Browsers
Windows 7 SP1 (64-bit)	Internet Explorer 11 Firefox 66 Chrome 76
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 Firefox 66 Chrome 76
Windows 10 (32-bit and 64-bit)	Internet Explorer 11 Firefox 66 Chrome 76
macOS Sierra (10.12)[a]	Safari 11.1.2 Firefox 66 Chrome 76
macOS High Sierra (10.13)[a]	Safari 11.1.2 Firefox 66 Chrome 76

[a] PKI Platform does not support Government Edition CAC and PIV smart cards on the Mac OS Sierra and macOS High Sierra operating systems.

PKI Client for Android

Table 6 - PKI Client Android version support

Type	Version
Android Pie	9.0
Android Oreo	8.1

Mobile Device

PKI Platform supports issuing digital certificates on all devices running on Android, iOS 11 and 12.

Documentation

The following documents have been revised to incorporate PKI Platform 8.19 specific material:

- *DigiCert PKI Platform 8.19 Release Notes* (this document)

Unless otherwise noted, all PKI Platform documents are available from the **Resources** page within the PKI Manager portal.

Issues Addressed and Known Issues

For information about fixed issues and other workarounds, see the DigiCert Knowledge Center for PKI Platform at the following URL:

https://knowledge.digicert.com/

- Enter **8.19** as the Knowledge Center Search text to find known issues and workarounds.
- Enter **Issues addressed in DigiCert PKI Platform 8.19** as the Knowledge Center Search text to obtain a list of the issues addressed.

Known Issues

The following are the known issues in this version:

- The DigiCert PKI Client for Android application is built using API version 26 best suited for Android Oreo (8.1) and below.

  The application functionality has been verified on Android 9 (Pie) and Android Q. In some cases, for Android Pie and Q, while opening the application for the first time, you might get an alert stating, “Detected Problems with API”. Click “OK” and proceed as the functionality has been successfully verified on both these Android versions.
- On iOS, certificate renewal after its expiry may not happen as expected. There is no workaround to this issue.
- iOS renewals will not work if user kicks off the process from the renewal link which is sent in the renewal e-mail. User must renew the iOS certificate from iPhone’s/iPad’s settings by updating the profile.
- PKI Client is not officially supported on mac Mojave