DigiCert® PKI Platform

Release Notes

Version 8.20.6

October 29, 2020

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 8.20.6 Release Notes

DigiCert PKI Platform is a cloud-hosted service provided by DigiCert, Inc.

This document includes the following topics:

- What's New in 8.20.6
- Component Support Updates
- Platform Support Updates
- Documentation
- Issues Addressed
- Known Issues

What's New in 8.20.6

This release notes accompany the delivery of the DigiCert PKI Platform 8.20.6 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 8.20.6

New to 8.20.6	Description
Wider DigiCert Desktop Client support	DigiCert Desktop Client support for the “Active Directory” authentication method, using supported certificate templates: Client Authentication and S/MIME (Digital Signature only).
Multiple Key Sizes	Support for selecting multiple RSA or ECDSA key sizes when configuring a certificate profile. Note: If multiple key sizes are configured within the profile, DigiCert will pick the largest key from those set by the administrator or the key size submitted in the CSR.
Dual Admin Manual Approval	Support for Dual Admin approval flow for certificate profiles configured with the “Manual approval” authentication method and the new "Enable Dual Admin Approval flow" option, for certificate requests enrolled via non-API enrollment methods.
TN Auth List extension	Support for the “Telephone Number Authorization List” extension (1.3.6.1.5.5.7.1.26), using a custom "Generic Device Authentication (TN Auth List extension)" template. The value for such extension is submitted via API making use of the OID as a parameter and the extension value as an ANS.1 structure that is Base64 encoded. Contact your DigiCert representative to request access to such custom template.
UAA User Portal enhancements	Enhancements to the UAA User portal to support CSRs with both BEGIN-END tags or without and stop delivering a P7 file when issuing a certificate for profiles configured with the “DigiCert Desktop Client” enrollment method.

New to 8.20.6	Description
PKI Client	Various PKI Client bug fixes: • Fixed issue with PKI Client Outlook Email signer configuration after successful enrolment of S/MIME Certificate not working with Microsoft Office 365. • Fixed issue with PKI Client Post Processing script for Outlook (64-bit) not applying the correct default hashing/signing algorithms.
Compliance	From the 2nd of November 2020, certificates that are issued by a public issuing CA without an Enhanced Key Usage (EKU) value will be blocked and yield an a608 error with the below error message for all enrollment flows: "*You are attempting to issue a certificate from a legacy CA chain. Please contact your administrator to configure a profile using an Issuing CA that chains up to a DigiCert trusted Root CA*".

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 8.20.6 supports

Components	Version Supported
PKI Client	2.20.6
PKI Enterprise Gateway, including Autoenrollment Server	1.20.4
PKI Web Services	8.19
PKI Client-Android	2.0.1

[a] PKI Platform 8.20.6 supports previous versions of PKI Client. However, you must run v2.20.2 or higher to benefit from the features that are described in this release notes.

Platform Support Updates

PKI Platform 8.20.6 supports the platforms and operating systems detailed in the below sections.

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. In order to access PKI Manager portal, you need an administrator certificate hosted on the PKI Client agent.

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 79 Chrome 84
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 79 Chrome 84
Windows 10 Enterprise edition (32-bit and 64-bit)	Internet Explorer 11[a] Firefox 79 Chrome 84
Mac (Catalina, Mojave, and High Sierra)	Firefox 79

[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, b] Firefox 79

Operating systems	Browsers
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11[a, b] Firefox 79
Windows 10 (32-bit and 64-bit)	Internet Explorer 11[a, b, c] Firefox 79
macOS Sierra (10.12)	Safari 11.1.2 Firefox 79
macOS High Sierra (10.13)	Safari 11.1.2 Firefox 79
macOS Mojave (10.14)	Firefox 79
macOS Catalina (10.15)	Firefox 79

[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] Renewal of OS browser certificates supported only for Internet Explorer.

[c] Edge mode is not supported.

PKI Client

PKI Client is a middleware software for digital signing, authentication, and data protection for desktop-based applications. It supports auto-renewal of certificates under management and auto-configuration of third-party applications via Post Processing scripts configured by a PKI Administrator. It uses digital certificates on smart cards, Intel TPM chips, security devices, or users' workstations using its own secure virtual keystore (vToken).

Table 5 - PKI Client operating systems and browser support

Operating systems	Browsers
Windows 7 SP1 (64-bit)	Internet Explorer 11 Firefox 79 Chrome 84
Windows 8.1 (32-bit and 64-bit)	Internet Explorer 11 Firefox 79 Chrome 84

Operating systems	Browsers
Windows 10 (32-bit and 64-bit)	Internet Explorer 11 Firefox 79 Chrome 84
macOS Sierra (10.12)[a]	Safari 11.1.2 Firefox 79 Chrome 84
macOS High Sierra (10.13)[a]	Safari 11.1.2 Firefox 79 Chrome 84
macOS Mojave (10.14)[b]	Firefox 79
macOS Catalina (10.15)[c]	Firefox 79

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

[b] Safari Version 12 or higher and Client Authentication using eToken is not supported on Chrome & Firefox from macOS Mojave.

[c] On macOS Catalina, certificate pickup on Hardware token using Firefox (ONLY) will not work without TokenD enabled in the system. For workaround and details, please refer: KB article.

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, 12 and 13.

User Authorization Agent (UAA)

The User Authorization Agent (UAA) is a service hosted in DigiCert's data center. It allows PKI Platform administrators to provide details of idP and SAML configurations to perform authentication/authorization before allowing DigiCert to issue a certificate, based on the certificate profile requirements you have set.

The UAA service supports both SAML 2.0 IdP and SP-initiated flows.

The UAA service is composed of two web portals: UAA Admin and User portals.

Note: UAA service is not available for Test Drive accounts.

Supported Certificate Templates and Enrollment Methods

Certificate Template	Enrollment Method
All Templates in Device and Server Seat Pools	• CSR
Client Authentication S/MIME (Digital Signature only)	• Browser PKCS12 • DigiCert Desktop Client

UAA Admin Portal

A portal accessed by PKI Administrators using the same administrator certificate securely stored on DigiCert PKI Client used to access PKI Manager. It allows an administrator to configure SAML profiles detailing where certificate data is sourced from (e.g. Fixed values set by an administrator, from a CSR, from a SAML Assertion) and how users go about enrolling/provisioning certificates (e.g. via a Browser PKCS12 flow, or using the DigiCert Desktop Client to interact with browser keystores).

Table 7 – UAA Admin Portal operating systems and browser support

Operating System	Browser
Windows 10 Mac OS (10.14.6)	Chrome (84.0. or later) Firefox (79.0 or later) Microsoft Edge (84.0 Windows/Mac or later)

UAA User Portal

A portal accessed by end-users to enroll for certificates based on a profile configured by their administrator. Users can authenticate against their SAML IdP provider and land on a UAA User self-service portal, from where they can perform various operations against profile that been configured by their administrator: enroll, download, revoke a certificate.

Users can also be given a specific URL that is bound to a profile and upon clicking on it, they will be redirected to their SAML IdP provider to authenticate/authorize before returning to the UAA User portal from where they can initiate the enrollment process and get a certificate provisioned via the method set by the administrator within the profile.

Table 8 – UAA User Portal operating systems and browser support

Operating System	Browser
Windows 10 Mac OS (10.14.6) Linux (Ubuntu 18.04) iOS 13 Android 9 (Pie)	Chrome (84.0. or later) Firefox (79.0 or later) Microsoft Edge (84.0 Windows/Mac or later) Safari (13.1 or later on Mac) Safari (13 on iOS 13) Chrome (69.0 on Android 9)

DigiCert Desktop Client

DigiCert Desktop Client can be used to generate keys and install software certificates across various browsers and platforms (Windows and macOS), when configuring a profile with the “DigiCert Desktop Client” enrollment method using the below certificate templates:

- Client Authentication
- S/MIME (Digital Signature only)

Table 5 – DigiCert Desktop Client operating systems and browser support

Operating systems	Browsers
Windows 10 (32-bit and 64-bit)	Chrome (84.0. later) Firefox (79.0 later) Microsoft Edge (84.0 Windows/Mac or later)
macOS Mojave (10.14.6) macOS Catalina (10.15.2)	Chrome (84.0. later) Firefox (79.0 later) Microsoft Edge (84.0 Windows/Mac or later) Safari (13.1 later on Mac)

Note: Other browsers may work, but have not been formally qualified by DigiCert

Table 6 Supported DigiCert Desktop Client version

Components	Version Supported
DigiCert Desktop Client	3.1.4

Table 7 Supported Certificate Templates and Authentication Methods for DigiCert Desktop Client

Certificate Template	Authentication Method
Client Authentication S/MIME (Digital Signature only)	• Manual approval • Enrollment code • Active Directory • Federated auth

Note:

- DigiCert Desktop Client is not available for Test Drive accounts.
- DigiCert Desktop Client support for the “Active Directory” authentication method is verified only on Windows 10 Operating system.

Documentation

Unless otherwise noted, all PKI Platform documents are available from the **Resources** page within the PKI Manager portal. Alternatively, you can also download a history of Release Notes from this KB article.

Issues Addressed

Issues addressed within this release include:

- [DPPC-1985] Invalid Enrollment Link error for Secure Email profiles configured with Enrollment Code and various codes generated against the same Seat ID.
- [DPPC-1857] dnsName extension appears duplicated for Domain Controller profiles.
- [DPPC-1980] Extended the backend database field size to support SAN extensions with values up to 4000 chars.
- [DPPC-1992] Performance improvements for PKI Web Services search operations.

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.

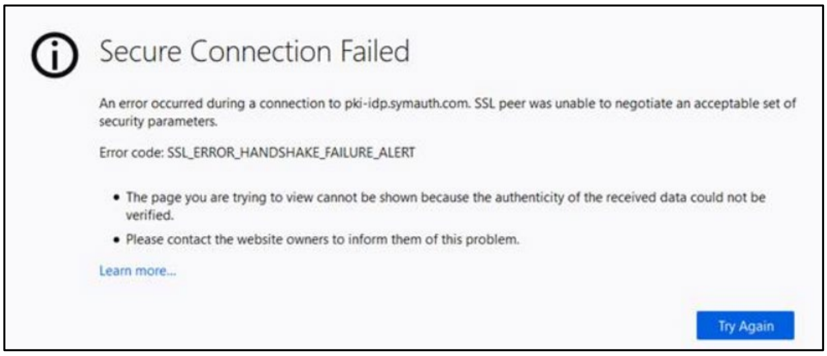
- While installing certificate on iOS for iPhones, although the certificate profile gets downloaded, the DigiCert UI displays a message showing “Your Certificate is not installed”.

- User/Admin enrollment on any Browser, any Operating System, may result into a Blank Page without any progress if the Symantec branded Browser extension is not removed from the Browser from where enrollment is attempted. Please manually remove the Symantec branded browser extension and install the DigiCert branded browser extension as provided on our instructions page and then restart the browser. Certificate enrollment should work fine after this procedure.

- Safari version 12 or higher is not supported on any macOS, due to an Apple API change affecting the PKI Client Safari extension.

- Client Authentication using eToken is currently not supported on Chrome & Firefox from macOS.

- For Mac and Windows OS, while accessing the PKI Manager portal using the PKI Client in Firefox browser, an error message may be displayed with the error code: **SSL_ERROR_HANDSHAKE_FAILURE_ALERT.**



Secure Connection Failed

An error occurred during a connection to pki-idp.symauth.com. SSL peer was unable to negotiate an acceptable set of security parameters.

Error code: SSL_ERROR_HANDSHAKE_FAILURE_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

This can be resolved by navigating to the settings of the Security Devices for PKI Client. From the **Open Menu** panel select -> **Options** -> type “Certificate” in **Find in Options** text field -> click on **Security Devices** button, and

1. Click the **Load** button and select the **PKCS 11** module.
2. Browse to the path where the PKCS 11 module is located:

   For Mac: /usr/local/lib/tblive-4/PKCS11.so

   For Windows: C:\Program Files\DigiCert\PKI Client\PKCS11.dll
3. Click **OK**.

   You will be able to access the PKI Manager portal successfully. For more details on the steps, please refer: KB article

- Certificate information report will not include **Other Name (GUID)** information for historic certificate data.