

Verifying XML Signatures

Technical Note

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **4**

1.1 Document Purpose 4

1.2 Intended Audience 4

2 Kemp Digital Signatures **5**

3 XML Signature Validation **7**

3.1 SHA-256 Checksum Comparison 7

3.2 Verifying the XML Digital Signature 8

3.2.1 XML 7.2.50 and Below 8

3.2.2 XML 7.2.57 and 7.2.48.8 LTS and Above 8

Last Updated Date **10**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

1.1 Document Purpose

The purpose of this document is to outline how to manually validate the digital signatures of resources provided by Kemp. Resources such as firmware, patches, and add-ons have associated XML files which contain the MD5 and SHA-256 checksums of the resource and are digitally signed by Kemp.

XML checksum files are currently not provided for LoadMaster templates.

You can automatically validate digital signatures easily using the LoadMaster Web User Interface (WUI). Simply enable the **Display Verify Update Option** check box in **System Configuration > Miscellaneous Options > WUI Settings**. This provides an option to upload the XML verification file when updating the LoadMaster software or installing an add-on file on the **System Configuration > System Administration > Update Software** page.

1.2 Intended Audience

This document is intended to guide any LoadMaster administrator or corporate security officer through the options to validate the integrity and authenticity of downloaded Kemp resources.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 Kemp Digital Signatures

All LoadMaster releases and associated add-on packages are digitally signed using XML-format signature files (also known as 'detached signatures') that conform to the best practices defined by the World Wide Web Consortium (W3C) for XML Signature Syntax and Processing. The XML signature filenames include the filename of the downloaded installation package as a prefix with the extension **.checksum.xml**.

The digital signing process employs an SSL certificate that has an expiration date. When the certificate reaches its expiration date, signature validation using this certificate will fail. Therefore, vendors need to update this certificate occasionally so that verification of digital signatures continues to work.

> On May 27th 2022, the SSL certificate used to sign LoadMaster release artifacts for LoadMaster Operating System (LMOS) version 7.2.56.x and prior releases expires.

All LoadMaster releases that occur after the above date (for example, LMOS 7.2.57.0) will be digitally signed using a newly obtained certificate.

What Does This Mean To You?

After 27th May 2022, verifying digital signatures for LMOS images and add-on packages will work only if the image or add-on package was signed with the new certificate. So, for example, you will be able to verify the XML signature in these scenarios:

- Updating LMOS 7.2.55.0 to LMOS 7.2.57.0 (or a later version).
- Installing an add-on package released with LMOS 7.2.57.0 (or a later version).

Verifying XML signatures will not work if you attempt to update the system with any LMOS update image or add-on package signed with the earlier, expired certificate. So, for example, XML signature verification will fail in these scenarios:

- Updating any LMOS release using an LMOS 7.2.56.0 image.
- Updating any LMOS release with the 7.2.55.0 Network Telemetry add-on package.

In these cases, you will need to skip XML signature verification when installing the LMOS image or add-on package. This can be done by navigating to **System Configuration > Miscellaneous Options > WUI Settings** and setting the **Update Verification Options** field to **Optional**. This allows you to

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

skip XML verification when you install the image. Once the update is complete, XML verification for future upgrades can once again be set to **Required** (if desired).

> If you have FIPS mode enabled, you will not be able to change the **Update Verification Options** field, which is set to **Required** in FIPS mode. If you need to update a FIPS system to an LMOS version signed with an expired certificate after 27th May 2022, please contact Support for assistance.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 XML Signature Validation

There are a number of different approaches to validation of detached XML signature files. The XML signature file is viewable in a text editor and looks something like the following:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<file name="LoadMaster-Patch-64bit.zip">
  <checksum>
    <sha256>ce7e1e92c1544061bb26ab0e14fc7dc512584ba37fd6c71e28e46e61ac2e41ba</sha256>
    <md5>79cf19cfa053f54e620c7d3de2cd690f</md5>
  </checksum>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
        <DigestValue>YukhB51PcSB3DsyMCtKaQsJuj9L4ca7qCS/ygBUNgLzkSH5+tCL+2TJHN7n7iIW2</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>KnRlanWC7dj9pG3/S/dh1FVVndTPmLMHDJzeyDkEzQ9tx5OLLG3J5p+YaX79UJW6
S1TbDUlx/QSuWhQtjhoq+piC66Yp5FlY3EmFQ0GpGhG0o0ShW7IwzwaaH4JGjrse</SignatureValue>
    <KeyInfo>
      <X509Data>
      <X509Certificate>MIICWzCCAeKgAwIBAgICEAAwCgYIKoZIzj0EAwMwYDELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgMAk5ZMR8wHQYDVQQKDBZLZW1wIFRlY2hub2xvZ2llcyBJbmMuMSMwIQYD
VQQDDBpLZW1wIENlcnRpZmljYXRlIEF1dGhvcml0eTAeFw0yMDA1MjcwODA4MzVa
Fw0yMjA1MjcwODA4MzVaMFcxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJOWTEfMB0G
A1UECgwWS2VtcCBUZWNobm9sb2dpZXMgSW5jLjEaMBgGA1UEAwwRS2VtcCBDb2Rl
IFNpZ25pbmcwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAARNGCQDbxI6sFZ5l7amUVLu
h+w4r+0l/a5YvsrqZzDf4l/ExgtQFdlMzqN0eObQC85eu5E5RdEtUqQFYgRuIIdH
vd0+ceN6kZuF283EV/oVLJ2v0wN+zjfahi6YacptxmGjeDB2MB0GA1UdDgQWBBSG
UYGDdfxIAMD/YDNDfdHvnwArDzAfBgNVHSMEGDAWgBSfmMgzNt3X/uMJ9yElYI/7
WnWxLjAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUBAf8EDDAK
BggrBgEFBQcDAzAKBggqhkjOPQQDAwNnADBkAjBkGsfjH5ESe0eTOKdK1/loSNp4
QuM6hXbUHeNTJnHeZhoxEwKCJM/Esm52SiZ6E9ICME8Cc01LkYk8tita3WGJYogW
slUNelBEuOihi8hcfxxJpKxwEhxFKSuKd5xWCNjAHw==</X509Certificate>
    <X509SubjectName>CN=Kemp Code Signing,O=Kemp Technologies Inc.,ST=NY,C=US</X509SubjectName>
    <X509IssuerSerial>
    <X509IssuerName>CN=Kemp Certificate Authority,O=Kemp Technologies Inc.,ST=NY,C=US</X509IssuerName>
    <X509SerialNumber>4096</X509SerialNumber>
    </X509IssuerSerial>
    </X509Data>
    </KeyInfo>
  </Signature>
</file>
```

3.1 SHA-256 Checksum Comparison

The basic process to validate the integrity of a Kemp resource is to do a checksum comparison:

1. Perform a local SHA-256 checksum on the downloaded Kemp resource.

    - On Windows: **certUtil -hashfile <PathToResource> SHA256**

    - On Unix: **sha256sum <PathToResource>**

2. Compare the locally generated SHA-256 checksum with the checksum contained in the XML signature file. To do this, open the XML signature file in a text editor and compare the SHA-256 checksum under <checksum><sha256> with the locally generated one. If these values do not match, then the original resource has been altered and should not be trusted.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. If the checksums match, validate the digital signature of the XML signature file.

3.2 Verifying the XML Digital Signature

A number of tools exist to validate detached XML signatures as provided by Kemp. Kemp recommends using the XMLSec Library (https://www.aleksey.com/xmlsec/) to verify the authenticity of XML signature files. This site provides sources and downloadable binaries for Windows platforms. This tool is available on many Linux environments as the xmlsec1 command.

3.2.1 XML 7.2.50 and Below

Verify the authenticity of the digital signature for XML files version 7.2.50 and below using the following xmlsec1 command.

xmlsec1 --verify <XMLSignatureFile>

If there are any errors in the output of the above command, the XML signature file has been altered and should not be trusted.

3.2.2 XML 7.2.57 and 7.2.48.8 LTS and Above

As of LoadMaster firmware versions 7.2.57 and 7.2.48.8 LTS there is a new certificate used to verify the authenticity of the XML digital signature. To verify the authenticity of the XML digital signature, you must first download the Kemp certificate bundle.

This downloads a zip archive with three certificates:

1. root.kemp.crt – Root Kemp CA certificate
2. ca.kemp.crt – Intermediate Kemp CA certificate
3. codesign.kemp.crt – Kemp code signing certificate

Unzip the archive into a desired location.

```
→  Downloads xmlsec1 --verify 7.2.49.1.18450.RELEASE.PATCH-64-MULTICORE.checksum.xml
OK
SignedInfo References (ok/all): 1/1
Manifests References (ok/all): 0/0
```


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

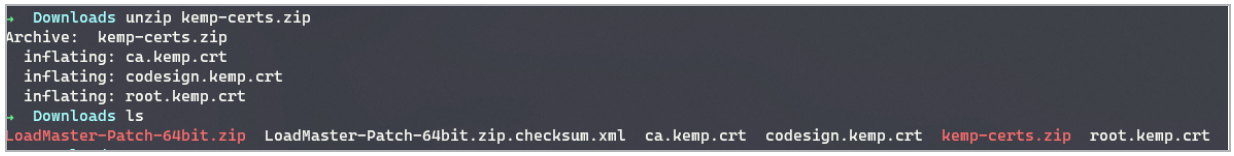
Verify the authenticity of the digital signature for XML files version 7.2.57/7.2.48.8 LTS and above using the following xmlsec1 command.

xmlsec1 --verify --enabled-key-data x509 --trusted-pem root.kemp.crt --trusted-pem ca.kemp.crt <XMLSignatureFile>

The expected output of successful verification is as follows:

```
OK
SignedInfo References (ok/all): 1/1
Manifests References (ok/all): 0/0
```

If there are any errors in the output of the above command, the XML signature file has been altered and should not be trusted.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 27 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.