



ASSURANCE CONTINUITY MAINTENANCE REPORT FOR CertAgent, Version 7.0 patch level 8

CertAgent, Version 7.0 patch level 8

Maintenance Report Number: CCEVS-VR-VID10815-2020

Date of Activity: 13 August 2020

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- CertAgent Impact Analysis Report (IAR), Information Security Corporation, Version 1.0.2, 13 August 2020
- Protection Profile for Certification Authorities Version 2.1 (PP_CA_21)

Documentation reported as being updated:

- **Security Target:**
 - CertAgent Security Target for Common Criteria Evaluation, version 4.1.4, May 11, 2020
- **Guidance:**
 - CertAgent Guidance for Common Criteria Evaluation, version 2.54.0, February 24, 2020
 - CertAgent Installation, Configuration and Management Guide, version 7.0, January 29, 2020
 - CertAgent Administrator Guide, version 7.0, January 22, 2020
 - CertAgent Certificate Authority Guide, version 7.0, January 22, 2020
 - CertAgent Public Site Guide, version 7.0, January 22, 2020
- Update descriptions can be found in the product Release Notes:
 - CertAgent Release Notes, version 7.0.8, January 31, 2020

Assurance Continuity Maintenance Report:

The Information Security Corporation (ISC) has prepared and submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 13 August 2020. An IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0.

The purpose of this Assurance Continuity Maintenance Report (ACMR) is to summarize and present the findings of CCEVS' analysis of the IAR and associated evidence submitted in support

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

of the changes to the original evaluation, and to make a determination regarding the appropriateness of Assurance Maintenance Continuity for the evaluation.

Introduction:

The evaluation, VID10815, was conducted by DXC.technology. The product met the security requirements specified by the NIAP approved protection profiles:

- Protection Profile for Certification Authorities Version 2.1

Information Security Corporation (ISC) has requested an assurance maintenance activity for the product to update the original evaluation and changes to the original product are detailed in the IAR.

Summary Description:

The vendor made software changes that addressed three areas: new features, changes to existing functionality and defect fixes. None of the changes were to any of the security functions, TSF interfaces or security objectives. The documentation has been updated to reflect the software version, the Security Target and Common Criteria Configuration Guide.

TOE new features:

Feature	Description
Added support for partially unattended installation and a post-install script	ISC rates the impact on assurance to be minor because we have simply automated existing installation procedures. These changes do not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.

TOE changes to existing functionality:

Feature	Description
Changed the Certificates and Certificate Requests pages to allow multiple profile selection	ISC rates the impact on assurance to be minor because we have only changed the filtering of displayed requests and simplified the issuance process for the CA Operations Staff role. These changes do not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.
Changed dNSName validation to allow comma and underscore characters	ISC rates the impact on assurance as minor because we simply allowed new characters in the extension values for which no PP guidance exists

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

<p>Changed the RA Management Interface (RAMI) certificate enrollment response</p>	<p>ISC rates the impact on assurance as minor because the change simply provided an additional way to obtain the issued certificate through RAMI. This change does not affect any TSF interfaces, SFRs, or security functions.</p>
<p>Added hyperlinks to display certificates and certificate chains in base64 format</p>	<p>ISC rates the impact on assurance as minor because the change simplified the process to obtain the certificate in base64-encoded format. This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.</p>
<p>Automated update of CRLs used for path validation and enhanced status checking</p>	<p>ISC rates the impact on assurance to be minor because we have automated the CRL update process for the administrators and the TOE always checks the CRL when doing status checking as part of the authentication process. These changes do not affect any TSF interfaces, SFRs, or security functions.</p>
<p>Increased the maximum number of characters allowed in an account ID and display name</p>	<p>ISC rates the impact on assurance as minor because using a longer account/profile ID and display name are only cosmetic changes. These changes do not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.</p>
<p>Added an option to the CACLI export function to control the filenames of output files</p>	<p>ISC rates the impact on assurance as minor because the change only affects the output filename. This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.</p>
<p>Updated the Admin and CA Account sites user interface</p>	<p>ISC rates the impact on assurance as minor because they are cosmetic changes. These changes do not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with them.</p>
<p>Simplified the process to reconfigure the TOE after a Java update</p>	<p>ISC rates the impact on assurance as minor because Java is not part of the TOE and the change simplified the manual update process required after a Java update. This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.</p>
<p>Removed the option to view the Tomcat logs from the admin site</p>	<p>ISC rates the impact on assurance as minor because we simply removed unnecessary option. The Tomcat logs were never part of the TOE's official audit system nor were they used during validation testing to meet any requirements.</p>

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

	This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.
Removed the browser-based enrollment option from the Public Site when using Firefox	ISC rates the impact on assurance as minor because browser-based enrollment is not a requirement of the PP, the functionality is still supported when Internet Explorer is used, and guidance was added to provide an alternate way to generate enrollment requests where Firefox was previously specified. This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.
Updated Apache Tomcat	ISC rates the impact on assurance as minor because after a review of the Apache Tomcat Changelog and source code we concluded that there were only minor changes in functionality used by the TOE. This change does not affect any TSF interfaces, SFRs, or security functions.
Added support for Amazon Corretto 8 as a supported Java Implementation	ISC rates the impact on assurance as minor because Java is not part of the TOE. This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.

TOE defect fixes:

Feature	Description
Corrected the Enrollment over Secure Transport (EST) URL	ISC rates the impact on assurance as minor because only the URL format and content-type changed. Neither change is covered by tests in the PP. The URL change doesn't change how the TOE authenticates the clients or processes the requests. The content-type change now complies with the RFC and EST clients that expect the content-type: "application/pkcs7-mime; smime-type=cert-only" now function properly. The above changes do not affect the TSF interface, SFRs, and security functions.
Restricted the "System" Credential to RSA only	ISC rates the impact on assurance as minor because the changes just ensure the sign and decrypt capabilities of the system credential and removed an optional feature (ECC key support for the system credential). This change does not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with this change.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

<p>Updated the order of the user authentication checks</p>	<p>ISC rates the impact on assurance as minor because the change only modified the order of the checks. These changes do not affect the TSF interface, SFRs, and security functions.</p>
<p>Corrected the error message displayed on the Admin site when an integrity check fails</p>	<p>ISC rates the impact on assurance as minor because the change only affects the error message displayed to the privileged user when integrity failure occurs. This change does not affect the TSF interface, SFRs, and security functions.</p>
<p>Updated some audit events</p>	<p>ISC rates the impact on assurance as minor because the changes only removed redundant information from, or provided additional details to, the existing audit events. The updated guidance document (<i>Guidance for Common Criteria Evaluation v2.54.0</i>) contains the current audit events. These changes do not affect the TSF interface, SFRs, and security functions.</p>
<p>Corrected the validity period calculations</p>	<p>ISC rates the impact on assurance as minor because the notAfter date is now calculated correctly regardless of the daylight-saving time status. This change does not affect any TSF interfaces, SFRs, or security functions.</p>
<p>Added input validation on the NIAP Conformance: Client Certificate DN Filter setting</p>	<p>ISC rates the impact on assurance as minor because only a validation check was added. This change does not affect any TSF interfaces, SFRs, or security functions.</p>
<p>Updated so that old CRLs are automatically removed when replaced</p>	<p>ISC rates the impact on assurance to be minor because we have simplified the administrator's task and improved the path validation performance. Both validated and changed TOEs return the path validation result properly. These changes do not affect any TSF interfaces, SFRs, or security functions.</p>
<p>Corrected issues with the user interfaces</p>	<p>ISC rates the impact on assurance to be minor because they corrected minor issues. These changes do not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with these changes.</p>
<p>Fixed CACLI bugs</p>	<p>ISC rates the impact on assurance to be minor because they corrected minor issues and added support for settings in the web interface that were missing in the CACLI. These changes do not affect any TSF interfaces, SFRs, or security functions and there are no assurance activities associated with these changes.</p>

Regression Testing:

Regression testing and new feature testing was performed to ensure that the validated claims continued to be satisfied. For all product releases, ISC ran a full suite of tests that cover the functionality of the product, including testing of common criteria functions. All tests were satisfied and passed.

Vulnerability Analysis:

An updated search for vulnerabilities was performed, on the updated TOE, August 13, 2020. The results of the vulnerability assessment were included in the IAR. No new vulnerabilities were detected.

The following search terms were used in the updated vulnerability analysis:

Acalashim

Apache Tomcat 8.5.50

CDK

jquery 1.11.0

log4j 1.2.16

org.json.json-rpc

Conclusion:

CCEVS reviewed the description of the changes, both security related and non-security related changes. There were no changes to the TSF interfaces, SFRs, or security functions introduced by the TOE changes and bug fixes. All of the changes were considered to be minor in impact. In addition, the existing NIST CAVP certifications were also not impacted by any of the changes.

The CCTL also reported that there were no vulnerabilities associated with any of the models. Therefore, CCEVS agrees that the original assurance is maintained for the product.