MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF:	2006-4-INF-98 v2	Created:	CERT2
Target:	Public	Reviewed:	CALIDAD
Date:	18.12.2006	Approved:	JEFEAREA

Assurance Continuity Maintenance Report

File: 2006-4 PATCH B08 of KeyOne 3.0

References:

EXT-18	2004-2 Security Target, 09-07-2004
EXT-125	2004-2 Evaluation Technical Report, 29-12-2005
INF-65	2004-2 Certification Report, 20-01-2006
AC	Assurance Continuity: CCRA Requirements, v1.0, February 2004

Common Criteria

Common Criteria Arrangement

According to the ***Assurance Continuity: CCRA Requirements***, version 1.0, February 2004, and considering the IAR (Impact Analysis Report) provided by the company SAFELAYER SECURE COMMUNICATIONS, the patch B08 is been included as part of the maintenance process of the IT product KeyOne v3.0. The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product KeyOne v3.0 certified by the National Cryptologic Centre (CCN) as Certification Body of the IT Security Evaluation & Certification National Scheme of Spain, under the file 2004-2 of this CB.

The change to the certified product is at Source Code level where a data type was adapted lightly to be compliant to an internal development standard of the company, a change that has no effect on assurance. The identification of the maintained product is indicated by a new patch number (B08) appended to the list of patches previously included with the version of the baseline certification.

Considering the nature of the change, the conclusion is to classify it as a minor change and that maintenance is the correct alternative to do the continuity of assurance.

Therefore, the assurance as described in the Certification Report INF-65 of the file 2004-2 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report INF-65.

Introduction

This section describes the information related to the identification of the IAR, certified and modified TOE, and the corresponding Security Targets as described by the *Assurance Continuity* [AC].

Impact Analysis Identification

IAR Document Identification D4718713 v1.3

Title Patch 3.0.04S2R1_B08 – Impact Analysis Report

Issued Date October 24, 2006

Authors Safelayer Secure Communications S.A..

Status Issued

Identification of the certified TOE

KeyOne 3.0 04S2R1: KeyOne CA, KeyOne LRA, KeyOne RA, KeyOne VA and KeyOne TSA.

Patches: 3.0_04S2R1_B01, 3.0_04S2R1_B02, 3.0_04S2R1_B03, 3.0_04S2R1_B04, 3.0_04S2R1_B05, 3.0_04S2R1_B06, 3.0_04S2R1_B07.

Identification of the modified TOE

KeyOne 3.0 04S2R1: KeyOne CA, KeyOne LRA, KeyOne RA, KeyOne VA and KeyOne TSA.

Patches: 3.0_04S2R1_B01, 3.0_04S2R1_B02, 3.0_04S2R1_B03, 3.0_04S2R1_B04, 3.0_04S2R1_B05, 3.0_04S2R1_B06, 3.0_04S2R1_B07, 3.0_04S2R1_B08.

Identification of the Security Target related to the certified TOE

Document Identifier B4E6DBC0 v1.38

Title Security Target KeyOne 3.0

Issued Date December 27, 2005

Authors Safelayer Secure Communications S.A..

Status Issued

Common Criteria version 2.2

Identification of the Security Target related to the modified TOE

Document Identifier B4E6DBC0 v1.39

Title Security Target KeyOne 3.0

Issued Date October 24, 2006

Authors Safelayer Secure Communications S.A..

Status Issued

Common Criteria version 2.2

Description of changes

Description of the 3.0.04S2R1 patch B08

The patch 3.0.04S2R1_B08 includes improvements in the internal management of the programming buffers to improve code robustness.

In the certified release 3.0.04S2R1 has been detected that some specific programming code that managed programming buffers, could be improved according to best practices adopted by the company’s development team. This improvement increases the security of some process related to verifications on the content and length of specific buffers.

Technical details and impact

The components included in the certified version 3.0.04S2R1are affected by a minor tiny modification. The scope of the described problem are uniquely those processes that make use of one specific method of an object involved cryptographic operations.

This method receives as parameter the content of a buffer related to the signature and the length of the content among other data. The function checks several properties of the content and length and returns TRUE if the content of the buffer is considered correct, or FALSE in other case.

The modification of the function on which the patch is based, consists of verifying also that the content of the buffer is not wrongly justified for other later functions. If the wrong justification is detected the function directly returns FALSE as output value.