REF: 2008-25-INF-351 v1
Target: Public
Date: 28.04.2009

Created: CERT8
Reviewed: CALIDAD
Approved: JEFEAREA

Informe de mantenimiento de la garantía de la seguridad

Expediente:2008-25 Mantenimiento KeyOne 2.1

Referencias:

[INF-65] 2004-2 Certification Report, 20-01-2006
[EXT-233] 2006-3 Declaración de Seguridad, 13-11-2006

[AC] Assurance Continuity: CCRA Requirements, v1.0, Febrero 04

Common Criteria Arrangement

De acuerdo a los requisitos del CCRA (Common Criteria Recognition Arrangement) para continuidad de las garantías de seguridad [AC] y considerando el Informe de Análisis de Impacto (IAR, Impact Análisis Report) proporcionado por la empresa SAFELAYER SECURE COMMUNICATIONS, S.A., los parches siguientes se incluyen como parte del proceso de mantenimiento del certificado del producto "KeyOne 2.1.04S1R2 (parche 2.1.04S1R2_B25)":

2.1.04S1R2_B04
2.1.04S1R2_B06
2.1.04S1R2_B14
2.1.04S1R2_B15
2.1.04S1R2_B16
2.1.04S1R2_B17
2.1.04S1R2_B19
2.1.04S1R2_B20
2.1.04S1R2_B21
2.1.04S1R2_TN_A06

El punto de partida para esta valoración ha sido el Informe de Certificación, la Declaración de Seguridad y el Informe Técnico de Evaluación del producto KeyOne 2.1.04S1R2 certificado por el Centro Criptológico Nacional (CCN) como Organismo de Certificación del Esquema Español de Evaluación y Certificación de las TI, con número de expediente 2004-01, así

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

como la Declaración de Seguridad modificada con motivo del mantenimiento realizado con número de expediente 2006-03 y su correspondiente Informe de Mantenimiento.

Considerando la naturaleza de los cambios, la conclusión es clasificar éstos como cambios menores y por tanto se lleva a cabo el mantenimiento del certificado como garantía de continuidad de la seguridad del producto.

De este modo las garantías de seguridad descritas en el Informe de Certificación INF-65 y su apéndice, el Informe de Mantenimiento INF-101 se mantienen en esta nueva versión del producto. Los detalles se pueden encontrar en las páginas siguientes.

Este informe se considera un apéndice a los informes de certificación INF-65 e INF-101.

Introducción

Esta sección describe la información relativa a la identificación del Informe de Análisis de Impacto, del OE certificado y modificado y de los correspondientes Declaraciones de Seguridad como se describe en [AC].

Identificación del análisis de impacto

Identificación del documento: 555A330C v1.0

Título: Parches de Ampliación de Alcance para EAL2 – 2007 – Informe de Análisis de Impacto

Fecha de emisión: 11 de Julio de 2007

Autores: Safelayer Secure Communications S.A..

Estado: Emitido

Identificación del TOE certificado

KeyOne 2.1.04S1R2: KeyOne CA, KeyOne LRA, KeyOne VA y KeyOne TSA.

Parches: 2.1.04S1R2_B25.

Identificación del TOE modificado

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

KeyOne 2.1.04S1R2: KeyOne CA, KeyOne LRA, KeyOne VA y KeyOne TSA.

Parches: 2.1.04S1R2_B25.
Parches: 2.1.04S1R2_B04.
Parches: 2.1.04S1R2_TN_A06.
Parches: 2.1.04S1R2_B14.
Parches: 2.1.04S1R2_B15.
Parches: 2.1.04S1R2_B06.
Parches: 2.1.04S1R2_B16.
Parches: 2.1.04S1R2_B17.
Parches: 2.1.04S1R2_B19.
Parches: 2.1.04S1R2_B20.
Parches: 2.1.04S1R2_B21.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Identificación de la Declaración de Seguridad asociada al TOE certificado

Identificación del documento 0C53A113 v2.1

Título Security Target KeyOne 2.1

Autores Safelayer Secure Communications S.A.

Estado Emitido

Versión de CC 2.2

Identificación de la Declaración de Seguridad asociada al TOE modificado

Identificación del documento 0C53A113 v2.2

Título Security Target KeyOne 2.1

Autores Safelayer Secure Communications S.A.

Estado Emitido

Versión de CC 2.2

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción de los cambios

Descripción del parche 2.1.04S1R2_B04

El parche 2.1.04S1R2_B04 soluciona un error en las aplicaciones KeyOne que utilizan un HSM nCipher. El error se produce en el caso de que se haya realizado anteriormente un proceso de migración (se ha usado un PSS generado con una versión anterior).

Impacto y detalles técnicos

Todos los productos incluidos en la versión certificada 2.1.04S1R2 están afectados, siendo el ámbito de la aplicación únicamente aquellas aplicaciones que arranquen con un HSM nCipher.

El objetivo de la mejora se produjo por lograr la compatibilidad con el HSM Chrysalis, y el contexto por tanto de este cambio está definido en el uso de este HSM. Este HSM no forma parte del entorno de certificación EAL2, y en consecuencia la funcionalidad modificada por la mejora no es ejecutada en un sistema instalado y configurado según los parámetros de seguridad de la certificación EAL2.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B04:
• KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
• Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
• Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
• Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
• Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
• MPIs:
• Release: 2.1.04S1R2_B04, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
• Release: 2.1.04S1R2_B04, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
• Release: 2.1.04S1R2_B04, Product: keyone-va, Version: $Revision: 1.5.2.2 $
• Release: 2.1.04S1R2_B04, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
• Código de programación:
    • Fichero cache.cpp.
    • Fichero jpkcs11.cpp.
• Parche 2.1.04S1R2_B04.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_TN_A06

El parche 2.1.04S1R2_TN_A06 soluciona un error en la visualización y desinstalación de los parches instalados en una distribución. El problema corresponde al bug interno de KeyOne 1710 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

Todos los productos incluidos en la versión certificada 2.1.04S1R2 están afectados, puesto que el error afecta a la aplicación de instalación de la distribución.

El error era provocado porque algunos parches, una vez instalados no se podían desinstalar con la aplicación de instalación de parches. Concretamente:

- La opción “Desinstalar parche” no desinstalaba el parche.
- La opción “Mostrar información de la instalación” mostraban el parche como instalado una vez se había procedido a la desinstalación.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_TN_A06:
- KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
- Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
- Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
- Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
- Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
- Código de programación:
- Fichero fixpatches.ws.
- Parche 2.1.04S1R2_TN_A06.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B14

El parche 2.1.04S1R2_B14 soluciona un error en la emisión de certificados cruzados en el caso de que se haya cambiado el puerto del programa de administración *offline* de KeyOne CA. El problema corresponde al bug interno de KeyOne 1727 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

El producto afectado por el parche 2.1.04S1R2_B14 es KeyOne CA.

El programa de administración *offline* de KeyOne CA tiene asignado el puerto 8081. Este programa administra varias páginas que están asociadas a un puerto. La página de emisión de certificados cruzados tiene *hardcodeado* el puerto 8081. En el caso de que se modifique el puerto por defecto 8081, la emisión de certificados cruzados fallará.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B14:

- KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
- Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
- Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer: 436EFD02.
- Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
- Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
- MPIs:
    - Release: 2.1.04S1R2_B14, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B14, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B14, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B14, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
- Código de programación:
    - Fichero config_ca_crosscert_pages.ws.
- Parche 2.1.04S1R2_B14.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B15

El parche 2.1.04S1R2_B15 soluciona un error en la aplicación KeyOne TSA. El error consiste en que no se genera un log de inicio ni un log de final de sesión (tal y como lo hacen el resto de aplicaciones KeyOne). El problema corresponde al bug interno de KeyOne 1740 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

El ámbito de aplicación es KeyOne TSA, y por tanto únicamente está afectado el producto KeyOne TSA. El error era provocado porque no se registraban los siguientes eventos:
• Inicio del servidor TSA (TSP_RESPONDER_STARTED)
• Parada del servidor TSA (TSP_RESPONDER_STOPPED)
• Inicio del programa de administración de TSA (TSP_ADMIN_STARTED)
• Parada del programa de administración de TSA (TSP_ADMIN_STOPPED)

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B15:
• KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
• Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
• Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
• Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
• Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
• MPIs:
    • Release: 2.1.04S1R2_B15, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B15, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B15, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B15, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
• Código de programación:
    • Fichero config_tsa_server.ws
    • Fichero config_tsa_server_database_functions.ws
    • Fichero config_tsa_server_event_control.ws
    • Fichero config_tsa_server_login_callbacks.ws
    • Fichero config_tsa_server_server.ws
    • Fichero config_admin_tsa_server.ws
    • Fichero config_tsa_server_login_callbacks.ws.lang.txt
• Parche 2.1.04S1R2_B15.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B06

El parche 2.1.04S1R2_B06 soluciona un error en la generación de certificados y CRLs que usen el algoritmo RSA con hash SHA-256 bits, con hash SHA-384 bits y con hash SHA-512 bits. El problema corresponde al bug interno de KeyOne 1683 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

El producto afectado por el parche es KeyOne CA. Se genera un informe de error en la generación de firmas de certificados y CRLs, cuando se intenta firmar con claves RSA con hash SHA-256 bits (sha256withRSAEncryption), con hash SHA-384 bits (sha384withRSAEncryption) y con hash SHA-512 bits (sha512withRSAEncryption).

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B06:

- KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
- Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
- Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
- Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
- Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
- MPIs:
    - Release: 2.1.04S1R2_B06, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B06, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B06, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B06, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
- Código de programación:
    - Fichero rsacipher.cpp.
- Parche 2.1.04S1R2_B06.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B16

El parche 2.1.04S1R2_B16 soluciona errores en la documentación de instalación de los productos KeyOne. El problema corresponde a los bugs internos de KeyOne 1721 y 1722 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

Los bugs afectan a documentación genérica de todos los productos incluidos en la versión certificada 2.1.04S1R2.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B16:
• KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
• Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
• MPIs:
    • Release: 2.1.04S1R2_B16, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B16, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B16, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B16, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
• Manuales de administración, instalación y configuración
• Documento Installation and Uninstallation Tool Manual, código interno B84D4B36, versión 1.1.
• Documento Puesta en marcha de aplicaciones KeyOne con HSM, código interno B0E8748E, versión 1.4.
• Documento Starting Up KeyOne Applications with HSM, código interno C9FD2693, versión 1.2.
• Parche 2.1.04S1R2_B16.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B17

El parche 2.1.04S1R2_B17 soluciona un error en el filtrado de los certificados de las Autoridades de Certificación que se muestran en una conexión de un cliente con cualquier servidor KeyOne configurado con autenticación de cliente. El problema corresponde al bug interno de KeyOne 1726 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

Todos los productos incluidos en la versión certificada 2.1.04S1R2 están afectados. El error era provocado porque en diferentes localizaciones del código la lista de certificados de las Autoridades de Certificación que se debían mostrar en una conexión de un cliente (configurado con SSL con autenticación de cliente) con cualquier servidor KeyOne, se gestionaba en formatos diferentes: en formato string (ejempo: “cn=Pepe González, o=safelayer, c=es”) o en codificación DER.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B17:

- KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
- Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
- Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
- Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
- Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
- MPIs:
    - Release: 2.1.04S1R2_B17, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B17, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B17, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    - Release:2.1.04S1R2_B17, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
- Código de programación:
    - Fichero tlshandshaketypes.h.
    - Fichero tlsconfiguration.cpp.
- Parche 2.1.04S1R2_B17.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B19

El parche 2.1.04S1R2_B19 soluciona los siguientes errores:
• Modificación de los nombres alternativos de las peticiones de certificación.
• No se puede generar claves AES de tamaños 128, 192 y 256.
• No es posible crear/procesar peticiones y certificados con GeneralNames de tipo X.400.
• En el caso de que los certificados tengan nombres (campo subject) con caracteres especiales y no se use la codificación UTF-8, se incumple el estándar PKCS #11 ([PKCS#11]), ya que el atributo CKA_LABEL del PKCS #11 tampoco se codifica en UTF-8 cuando éste sí que debiera estar codificado en UTF-8.
• Los servidores KeyOne VA y KeyOne TSA dejan de funcionar correctamente y se paran en el caso de que se realicen pruebas de carga con estos servidores.

Estos problemas corresponden a los bugs internos de KeyOne 1739, 1777, 1900, 1906 y 1953 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

Todos los productos incluidos en la versión certificada 2.1.04S1R2 están afectados.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B19:
• KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
• Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
• Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
• Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
• Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
• MPIs:
    • Release: 2.1.04S1R2_B19, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B19, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B19, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B19, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
• Código de programación:
    • Fichero asn2str.cpp.
    • Fichero aescipher.cpp.
    • Fichero ctxsecretkey.cpp
    • Fichero cryptstate.h
    • Fichero alginfo.h
    • Fichero aescipher.h
    • Fichero jpkcs11.cpp

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Fichero crypt.cpp
- Fichero initlib.cpp

• Parche 2.1.04S1R2_B19.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B20

El parche 2.1.04S1R2_B20 soluciona los siguientes errores:
• Reporte de error en KeyOne TSA cuando el cliente utiliza un algoritmo de hash SHA1 en la petición TST.
• Error interno de KeyOne TSA cuando la petición TSP incluye una política no correcta.

El problema corresponde a los bugs internos de KeyOne 2029 y 1609 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

Únicamente el producto KeyOne TSA está afectado por el parche.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B20:
• KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
• Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
• Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
• Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
• Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
• MPIs:
    • Release: 2.1.04S1R2_B20, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B20, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B20, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    • Release: 2.1.04S1R2_B20, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
• Código de programación:
    • Fichero config_tsa_server_responder.ws.
• Parche 2.1.04S1R2_B20.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción del parche 2.1.04S1R2_B21

El parche 2.1.04S1R2_B21 añade nuevas zonas horarias a las aplicaciones KeyOne. El problema corresponde al bug interno de KeyOne 2074 de la versión certificada 2.1.04S1R2.

Impacto y detalles técnicos

Todos los productos incluidos en la versión certificada 2.1.04S1R2 están afectados. El error consiste en que Scryptor no permitía configurar el settimezone como UTC, soportando únicamente las zonas horarias de Europa CET y WET.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por el parche 2.1.04S1R2_B21:

- KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
- Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.
- Escenario de Pruebas. Departamento de Calidad, versión 1.8. Código interno de Safelayer : 436EFD02.
- Quality Assurance. Test Description, versión 1.9. Código interno de Safelayer: C4484186.
- Quality Assurance. Test Results, versión 1.7. Código interno de Safelayer: 47C18C40.
- MPIs:
    - Release: 2.1.04S1R2_B21, Product: keyone-ca, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B21, Product: keyone-lra, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B21, Product: keyone-va, Version: $Revision: 1.5.2.2 $
    - Release: 2.1.04S1R2_B21, Product: keyone-tsaserver, Version: $Revision: 1.5.2.2 $
- Código de programación:
    - Fichero jtime_africa.def.
    - Fichero jtime_asia.def.
    - Fichero jtime_australia.def.
    - Fichero jtime_centerandsouthamerica.def.
    - Fichero jtime_europe.def.
    - Fichero jtime_northamerica.def.
    - Fichero jtime_standards.def.
- Parche 2.1.04S1R2_B21.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción de la actualización de la gestión de configuración

Se ha actualizado el documento [CM] para modificar el mecanismo de identificación de MPIs en el caso de parches. En caso de MPIs de parches se incluía en el campo "release" la identificación de la distribución asociada. Sin embargo este campo, junto con el resto de campos para la identificación del MPI (product, version) no identificaban unívocamente el MPI en el caso de un parche. Se ha hecho el siguiente cambio en la sección "Identifying products and their components" del capítulo 3 "Configuration Identification": The "Release:" field identifies the distribution related to the MPI. cambiado por The "Release:" field identifies the distribution (or patch) related to the MPI.

Evidencias de la certificación afectadas

Las siguientes evidencias son las actualizadas por la modificación del documento [CM]:

• KeyOne 2.1 – Declaración de Seguridad, versión 2.2. Código interno de Safelayer: 040A5EBD.
• Security Target - KeyOne 2.1, versión 2.2. Código interno de Safelayer: 0C53A113.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es