REF: 2010-29-INF-582 v2
Difusión: Expediente
Fecha: 29.03.2011

Creado: CERT2
Revisado: TECNICO
Aprobado: JEFEAREA

INFORME DE MANTENIMIENTO

Expediente: 2010-29
Datos del solicitante: FABRICA NACIONAL DE MONEDA Y TIMBRE

Referencias: [EXT-1147] Solicitud de mantenimiento de la FNMT-RCM
[EXT-1145] Análisis de Impacto del cambio de PIN en certificados
[EXT-1202] Actualización del IAR y solicitud de FNMT-RCM
[EXT-1146] Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE v1.4
[EXT-374] 2004-4 Security Target lite DNIe v1.13
[EXT-343] 2004-4 Evaluation Technical Report DNIe v1.13
[INF-148] 2004-4 Informe Certificación DNIe v1.13
[AC] Assurance Continuity: CCRA Requirements, v1.0, Feb 2004

Common Criteria Arrangement

Conforme al documento "***Assurance Continuity: CCRA Requirements***, version 1.0, February 2004", y considerando el IAR (Impact Analysis Report) proporcionado por la FNMT-RCM, el cambio propuesto en la solicitud de mantenimiento del expediente 2010-29 del Organismo de Certificación, ha sido incluido como parte del proceso de mantenimiento del producto DNIe v1.13 previamente certificado según el expediente 2004-4.

La base para esta decisión está en la revisión del informe de certificación del producto DNIe v.1.13, certificado por el Centro Criptológico Nacional (CCN) como Organismo de Certificación del Esquema Nacional bajo el expediente 2004-4, así como de su Declaración de Seguridad y el Evaluation Technical Report del producto.

El cambio al producto certificado es de configuración en algunos de sus ficheros de datos, no afectando al código fuente, y solo viéndose modificado el documento de

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

instalación, generación y puesta en marcha. Este cambio se considera que no tiene efectos en las garantías de seguridad del certificado del producto.

El cambio se identifica por la inclusión de una nueva versión 1.4 del documento "Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE", que se incluiría como adenda al contenido del certificado previo.

Considerando la naturaleza del cambio, la conclusión es clasificarlo como "minor change" según [AC] y por tanto incluirlo en este esquema de mantenimiento es la alternativa correcta para continuar extendiendo las garantías de seguridad del certificado emitido previamente.

Por este motivo, las garantías de seguridad descritas en el Informe de Mantenimiento INF-148 del expediente 2004-4 se mantienen para esta versión del producto. Los detalles pueden encontrarse en las páginas siguientes.

Este informe es una adenda al Informe de Certificación INF-148.

Introducción

Esta sección describe la información relative a la identificación del IAR, TOE certificado y modificado, y las correspondientes STs según lo descrito por el documento *Assurance Continuity* [AC].

Identificación del IAR

Informe de Análisis de Impacto (IAR) DNIe 1.13 Cambios de Personalización.

Referencia CCC/IAR/CPDNIE0100/2011. Versión 1.1, 02/03/2011.

Autor: Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda.

Identificación del TOE certificado

DNIe, versión 1.13, configuraciones DNIe 1.13 A11 H4C34 EXP 1-1 y DNIe 1.13 B11 H4C34 EXP 1-1.

"Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE" v1.3.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Identificación del TOE modificado

DNIe, versión 1.13, configuraciones DNIe 1.13 A11 H4C34 **EXP 1-4.5-0** y DNIe 1.13 B11 H4C34 **EXP 1-4.5-0**.

"Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE" **v1.4**.

Identificación de la ST del TOE certificado

"Declaración de Seguridad Tarjeta DNIe" de versión 1.0 y revisión 6.

Autor: Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda

Common Criteria version 2.2

Identificación de la ST del TOE modificado

No cambia.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Descripción de los cambios

Los cambios efectuados se han limitado al procedimiento de generación, y por tanto no afectan a la tarjeta DNIe como tal sino a uno de sus documentos de operación asociados.

Este documento es el “Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE” v1.4, que en esta nueva versión especifica que los permisos o condiciones de acceso a los certificados públicos del usuario en el chip NO requieren ya el presentar el PIN, a diferencia de lo que ocurría anteriormente.

Detalles técnicos e impacto

El impacto del cambio en cómo se genera la tarjeta es menor y sin ser un problema para la seguridad del producto se espera que aumente su usabilidad.

Actualmente este tipo de certificados por su naturaleza son públicos de manera que se presentan a los navegadores web para establecer el canal SSL de comunicaciones seguras en las aplicaciones.

Por su propia naturaleza de certificado “público” la información criptográfica contenida en el mismo no tiene problemas que sea conocida. De hecho es necesario para el proceso de autenticación basado en clave asimétrica.

Se reduce así el número de veces que el navegador pide este PIN a los usuarios finales (ya que por motivos de seguridad los drivers DNIe no cachean este PIN).

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Evidencias del desarrollador afectadas

Son todas de tipo documental y se limitan a un documento de la actividad CC ADO.

El documento “Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE” v1.3 del certificado previo.

Ahora pasa a ser la versión “Procedimiento de instalación, generación y puesta en marcha de la Tarjeta DNIE” v1.4 del mantenimiento.

ENAC
CERTIFICACIÓN
Nº 45/C-PR110

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