REF:	2009-26-INF-660 v1	Creado:	CERT8
Difusión:	Público	Revisado:	TECNICO
Fecha:	13.07.2011	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2009-26 PSTmail
Datos del solicitante: B82015181 AUTEK INGENIERÍA

Referencias: EXT-842 Solicitud de Certificación de PSTMail
EXT-1261 ETR de PSTMail v2.0, de 08/02/2011
EXT-1324 IAR PSTmail v3.0.4

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

Informe de certificación del producto PSTmail, versión 3.0.5, según la solicitud de referencia [EXT-842], de fecha 28/10/2009, y evaluado por el laboratorio Epoche & Espri, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1261] recibido el pasado 10/02/2011 y ampliado con las modificaciones detalladas en el Informe de Análisis de Impacto [EXT-1324] de acuerdo a [CCRA] y recibido el pasado 06/07/2011.

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

INDICE

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

Resumen

Este documento constituye el Informe de Certificación para el expediente de la certificación del producto PSTmail, versión 3.0.5.

PSTmail es una pasarela de correo electrónico, software que permite el intercambio de correo electrónico entre dos redes separadas conforme a unas políticas configurables de flujo de mensajes.

Fabricante: Autek.

Patrocinador: Autek.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: Epoche & Espri.

Perfil de Protección: Ninguno.

Nivel de Evaluación: EAL 4+(ALC_FLR.1).

Fortaleza de las Funciones: no aplica en CC v3.1

Fecha de término de la evaluación: 08/02/2011.
Fecha de entrega de las modificaciones: 13/07/2011

Todos los componentes de garantía requeridos por el nivel de evaluación EAL4 (aumentado con ALC_FLR.1) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Epoche & Espri asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto PSTmail, se propone la resolución estimatoria de la misma.

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

Resumen del TOE

PSTmail es un sistema que permite el intercambio de correo electrónico entre dos redes TCP/IP con diferentes grados de clasificación o políticas de seguridad lo que impediría su conexión por cualquier otro medio. Las dos redes no son equivalentes: una se considera que tiene un grado de clasificación o un nivel de seguridad mayor. PSTmail garantiza la imposibilidad de cualquier tipo de tráfico entre las dos redes excepto el correo transmitido por el propio sistema.

El sistema se administra exclusivamente desde la red más segura.

Los protocolos de correo soportados son los estándar de Internet: POP3 e IMAP4 para la recepción y SMTP para el envío. La pasarela no sustituye a los servidores de correo electrónico de las dos redes sino que los usa como elementos intermedios para el envío y recepción de mensajes.

El correo entra a la red segura de manera transparente para los usuarios, aunque se le pueden aplicar políticas de filtrado, desvíos condicionales y se puede redirigir a varias cuentas internas.

La salida de correo de la red segura requiere la autorización mediante firma electrónica de cada uno de los mensajes.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para el componente adicional, ALC_FLR.1, según la parte 3 de CC v3.1 r3.

Assurance Class	**Assurance Components**
Security Target	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.2, ASE_ECD.1, ASE_REQ.2, ASE_TSS.1
Development	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3
Guidance	AGD_OPE.1, AGD_PRE.1
Life Cycle	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_FLR.1
Tests	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
Vulnerability Analysis	AVA_VAN.3

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

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la parte 2 de CC v3.1 r3, siguientes:

FMT_SMR.2	Restrictions on security roles
FMT_SMF.1	Specification of Management Functions
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FMT_MSA.1/ IFF	Management of security attributes
FMT_MSA.1 / ACC	Management of security attributes
FMT_MSA.3 / IFF	Static attribute initialisation
FMT_MSA.3 / ACC	Static attribute initialisation
FDP_ACF.1	Security attribute based access control
FDP_ACC.2	Complete access control
FDP_IFC.2 / ENT	Complete information flow control
FDP_IFF.1 / ENT	Simple security attributes
FDP_IFC.2 / SAL	Complete information flow control
FDP_IFF.1 / SAL	Simple security attributes
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review

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

Identificación

Producto: PSTmail v3.0.5.

Declaración de Seguridad: Declaración de seguridad PSTmail v1.2, de 12/07/2011
Declaración de Seguridad (lite): Declaración de seguridad PSTmail v1.2 (versión pública), de 12/07/2011

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r3 EAL4+ (ALC_FLR.1).

Fortaleza de las Funciones: no aplica en CC v3.1.

Política de seguridad

El uso del producto PSTmail, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de las políticas como dispositivo de firma se encuentra en la declaración de seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

Política 01: P1.SEP

Las dos redes deben permanecer separadas. No debe ser posible el establecimiento de conexiones TCP/IP entre las dos redes.

Política 02: P2.SAL

Los mensajes de correo electrónico salientes (es decir, los dirigidos desde la Red Interna hacia la Red Externa) deben ser autorizados mediante firma electrónica.

Política 03: P3.CRYPT

La información (de configuración y la procesada por el sistema) que se guarde en disco en las unidades (PSTi, PSTe) debe estar cifrada*., al igual que as comunicaciones para administración remota y envío de datos de auditoría.*

Política 04: P4.ROLES

El PSTmail deberá implementar los siguiente roles, con las capacidades indicadas:

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

Administrador raíz:

1. Establece los CN de los certificados que se consideran válidos para la administración de la pasarela y sus permisos.

Administrador de Seguridad:

1. Establece la configuración de monitorización: parámetros que afectan a los eventos del sistema y al registro de transferencias.
2. Puede obtener una copia de los ficheros de registro de eventos de seguridad (que se almacenan localmente en la Unidad Interna de la pasarela).

Administrador de Servicios:

1. Establece toda la configuración de los servicios (entrada y salida de correo).
2. Puede arrancar y parar los servicios de entrada y salida de correo.
3. Puede obtener una copia de los ficheros de registro de eventos de funcionamiento (que se almacenan localmente en la Unidad Interna de la pasarela).

Administrador de Monitorización:

1. Supervisa el estado de funcionamiento de la pasarela.
2. Puede reiniciar las estadísticas de los servicios (entrada y salida de correo).

Administrador Local:

1. Establece la configuración local de las unidades internas.

Estos roles y sus capacidades se implementarán mediante las funcionalidades de autenticación que permitan establecer las políticas y funciones de control de acceso que regulen el ejercicio autorizado de las capacidades indicadas.

Política 05: P5.AUDITORIA

El PSTmail implementará un mecanismo de registro de su actividad.

Hipótesis y entorno de uso

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

Para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

Hipótesis 01: AS1

Nadie tiene acceso al hardware de ninguna de las dos unidades (salvo los administradores locales). Se supone que las maneras obvias de circunvalar el sistema (como por ejemplo conectar ambas unidades directamente mediante un

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

cable de red) quedan descartadas por medidas físicas u organizativas del entorno de explotación.

Hipótesis 02: AS2

La Red Interna es una red aislada y totalmente asegurada y confiable. La Red Externa es una red físicamente controlada (no se pueden conectar nuevas máquinas a la red) y con medidas de seguridad (cortafuegos en sus conexiones a otras redes, máquinas en la red securizadas y con las últimas actualizaciones y parches de seguridad, etc.) pero que sí está conectada mediante TCP/IP a otras redes.

Hipótesis 03: AS3

La plataforma (entorno del TOE) estará diseñada de tal modo y configurada de manera segura, de manera que no existan caminos de ataque a través de dicha plataforma.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto PSTmail v3.0.4, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “Enhanced Basic” de EAL4, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Amenazas cubiertas:

Amenaza 01: T1.IFF-ENT

Un atacante en la Red Interna recibe en su buzón, de manera no autorizada, mensajes destinados a otros usuarios.

Amenaza 02: T2.IFF-SAL

Un atacante en la Red Interna envía un mensaje no autorizado a través de la pasarela.

Amenaza 03: T3.IFF-EXT1

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

Un atacante en la Red Externa consigue introducir información en la Red Interna, a través del hardware de la pasarela pero, por un cauce distinto del correo electrónico de entrada.

Amenaza 04: T4.IFF-EXT2

Un atacante en la Red Externa consigue obtener información de la Red Interna por cualquier medio distinto de la salida autorizada de correo.

Funcionalidad del entorno.

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del producto son los siguientes:

Objetivo entorno 01: O.ENV.AS1

Nadie tendrá acceso al hardware de ninguna de las dos unidades (salvo el administrador Local). Se supone que las maneras obvias de circunvalar el sistema (como por ejemplo conectar ambas unidades directamente mediante un cable de red) quedan descartadas por medidas físicas u organizativas del entorno de explotación.

Objetivo entorno 02: O.ENV.AS2

La Red Interna es una red aislada y totalmente asegurada y confiable. La Red Externa es una red físicamente controlada (no se pueden conectar nuevas máquinas a la red) y con medidas de seguridad (cortafuegos en sus conexiones a otras redes, IDS, máquinas en la red securizadas y con las últimas actualizaciones y parches de seguridad, etc.) pero que sí está conectada mediante TCP/IP a otras redes no seguras.

Objetivo entorno 03: O.ENV.AS3

La plataforma (entorno del TOE) estará diseñada de tal modo y configurada de manera segura, de manera que no existan caminos de ataque a través de dicha plataforma.

Objetivo entorno 04: O.ENV.AS4

Las operaciones criptográficas utilizan la criptografía de Windows para lo siguiente:

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

- Cifrado de disco de las unidades internas (PSTi). El cifrado en las unidades internas se realiza con una clave que se guarda en un dispositivo externo y se recupera en cada arranque para descifrar.
- Cifrado de disco de las unidades externas (PSTe). El cifrado en las unidades Externas se realiza con una clave de sesión lo que garantiza que no haya persistencia entre sesiones.
- Verificación de firma de los mensajes de salida
- Establecimiento de conexiones TLS de administración y envío de datos de auditoría.

Objetivo entorno 05: O.ENV.AS5

Separación de redes. La arquitectura hardware debe ser tal que exista un host distinto en cada una de las redes. La comunicación entre ambos hosts debe realizarse mediante un dispositivo pasivo de intercambio de información.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del OE se encuentran en la correspondiente Declaración de Seguridad.

Arquitectura

Arquitectura Física:

El componente fundamental de PSTmail lo constituyen dos equipos que se denominarán 'unidades'. Cada uno de ellos se conecta a una de las redes y se denomina PSTi al de la Red Interna y PSTe al de la Externa. Se trata de equipos dedicados, es decir, no se ejecuta en ellos ninguna aplicación software aparte de las propias de PSTmail.

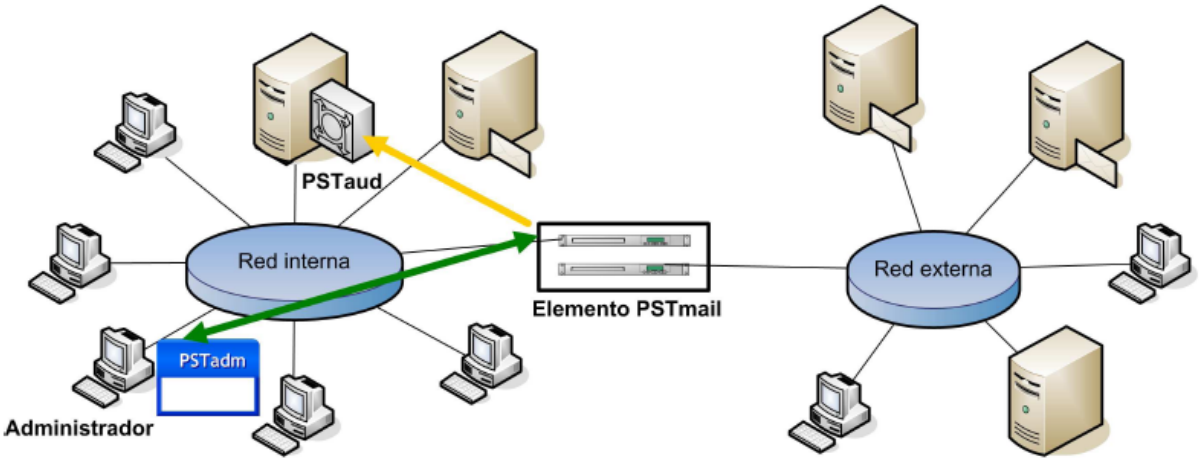
- Elemento PSTmail
  Cada pareja de unidades PSTi y PSTe, forma un elemento. El elemento incluye también el dispositivo hardware necesario para la comunicación entre las unidades. Existen dos posibles configuraciones: individual -formada por un elemento- y redundante -formada por dos elementos en un esquema de redundancia activopasivo-.

Arquitectura Lógica:

Adicionalmente el sistema está formado por los siguientes componentes software que se ejecutarán en puestos de propósito general o servidores situados en la Red Interna:

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

- PSTadm - Aplicación de administración (No forma parte del TOE) La administración del sistema completo se realiza desde un puesto de la Red Interna. La unidad situada en la Red Externa (PSTe) no necesita ser administrada.
- PSTaud - Servicio de recepción de registros de auditoríaLos datos de actividad (datos de los mensajes transferidos por la pasarela) se registran en una base de datos ajena a PSTmail. La misión de PSTaud es insertar los datos que recibe de la unidad interna, en una base de datos.



Documentos

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- Declaración de seguridad de PSTmail v1.2, de julio 2011
- Manual de operación Revisión 16, de febrero 2011
- Manual de instalación y puesta en servicio Revisión 17, de febrero 2011

Pruebas del producto

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante en sus instalaciones con resultado satisfactorio.

El proceso ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la declaración de seguridad.

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

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de los las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido entorno a un 25 % de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados así obtenidos son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado el evaluador ha constatado que dicha variación no representaba un problema para la seguridad, ni suponía una merma en la capacidad funcional del producto.

Configuración evaluada

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto PSTmail v3.0.5 es necesario disponer de los siguientes componentes:

La parte central del TOE se ejecuta en dos servidores específicos suministrados por el fabricante que ejecutan Windows Embedded Standard. Se soportan las series S1 y S2.

Para instalación y ejecución del servicio de registro de transferencias PSTaud es necesario un PC estándar con un procesador de 1GHz o superior y mínimo 1GB de memoria ejecutando el Sistema Operativo Windows XP SP3 o superior.

El entorno donde se ejecuta PSTmail debe incluir:

- Para la instalación y ejecución de la aplicación de administración PSTadm es necesario un PC estándar con un procesador de 1GHz o superior y mínimo 1GB de memoria ejecutando el Sistema Operativo Windows XP SP3 o superior.
- Infraestructura de clave pública
- Servidor(es) de syslog (Red Interna)

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

- Servidor de base de datos para el registro de transferencias accesible mediante ODBC (Red Interna)
- Servidores de correo electrónico
- Clientes de correo electrónico con soporte S/MIME (Red Interna)

Resultados de la Evaluación

El producto PSTmail ha sido evaluado frente a la declaración de seguridad "Declaración de seguridad de PSTmail v3.0.5" v1.2 de julio de 2011.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL4+** (aumentado con ALC_FLR.1) presentan el veredicto de "PASA". Por consiguiente, el laboratorio Epoche & Espri asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL4, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r3.

Recomendaciones y comentarios de los evaluadores

A continuación se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

1. Es imprescindible confiar en la(s) infraestructura(s) de clave pública sobre la(s) que descansa el producto.
2. La autenticación se realiza a través del Common Name, con independencia de la CA utilizada (siempre y cuando esté almacenada en el TOE), por lo tanto, esta deben ser confiables.
3. Por diseño del producto es necesario que las contraseñas de los buzones de los usuarios sean conocidos por los administradores de la pasarela. Los usuarios del TOE deberán de ser conscientes de este hecho.
4. La comunicación con los servidores de correo puede realizarse en texto en claro. Se recomienda la securización de dichas comunicaciones en el entorno operacional.
5. Es necesario destacar que un supervisor posee potestad para crear y modificar correos electrónicos en nombre de cualquiera de sus supervisados. Se recomienda que los usuarios supervisores sean confiables.
6. Existen vulnerabilidades que han sido cerradas mediante advertencias en la declaración de seguridad y advertencias de uso seguro en los manuales. Es importante por lo tanto que estas sean muy tenidas en cuenta.

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

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto PSTmail, se propone la resolución estimatoria de la misma.

Glosario de términos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ETR	Evaluation Technical Report
OC	Organismo de Certificación

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

Bibliografía

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, Julio 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, Julio 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, Julio 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, Julio 2009.

Declaración de seguridad

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: "**Declaración de Seguridad de PSTmail v3.0.5", v1.2 de julio 2011**.

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