tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

145

LA IDENTIDAD DIGITAL EN EL MINISTERIO DE DEFENSA

Miguel Ángel Rego Fernández
Comandante de la Armada
Área de Seguridad
Inspección General CIS
Secretaría de Estado de Defensa
Ministerio de Defensa

Miguel Ángel Rego Fernández

Palabras clave

Seguridad de la Información, Seguridad
Identidad Digital
PKI (Public Key Infrastructure), Infraestructura de Clave Pública
Certificados Digitales, Certificación
Prestadores de Servicios de Certificación (PSCs)
Cifrado
Firma electrónica
Tarjeta electrónica
Tarjeta chip
Autoridad de Certificación, CA
Autenticación
Control de acceso

Resumen de su Comunicación

La comunicación trata sobre los siguientes aspectos:

- Implantación de una Infraestructura de Clave Pública (PKI) como herramienta fundamental para la implementación de servicios de seguridad en los sistemas de información y en las aplicaciones (autenticación, firma digital, cifrado, no repudio y sellado de tiempo).

- Implantación de la Tarjeta Electrónica de Defensa (TEDEF) como elemento seguro de identificación ante sistemas electrónicos y soporte de certificados y claves emitidos por la PKI (control de acceso físico, control de acceso lógico, soporte seguro de información, etc.).

- Proyecto de Real Decreto de Firma Electrónica que desarrolla el artículo 4.4 de la Ley 59/2003 de Firma Electrónica.

Mediante la gestión de claves y certificados a través de una PKI en una organización se facilita la posibilidad de utilización de los servicios de firma electrónica y cifrado en una amplia variedad de aplicaciones, estableciendo y manteniendo un entorno de red seguro.

La implantación de una PKI proporciona a una organización, entre otras, las siguientes funcionalidades:

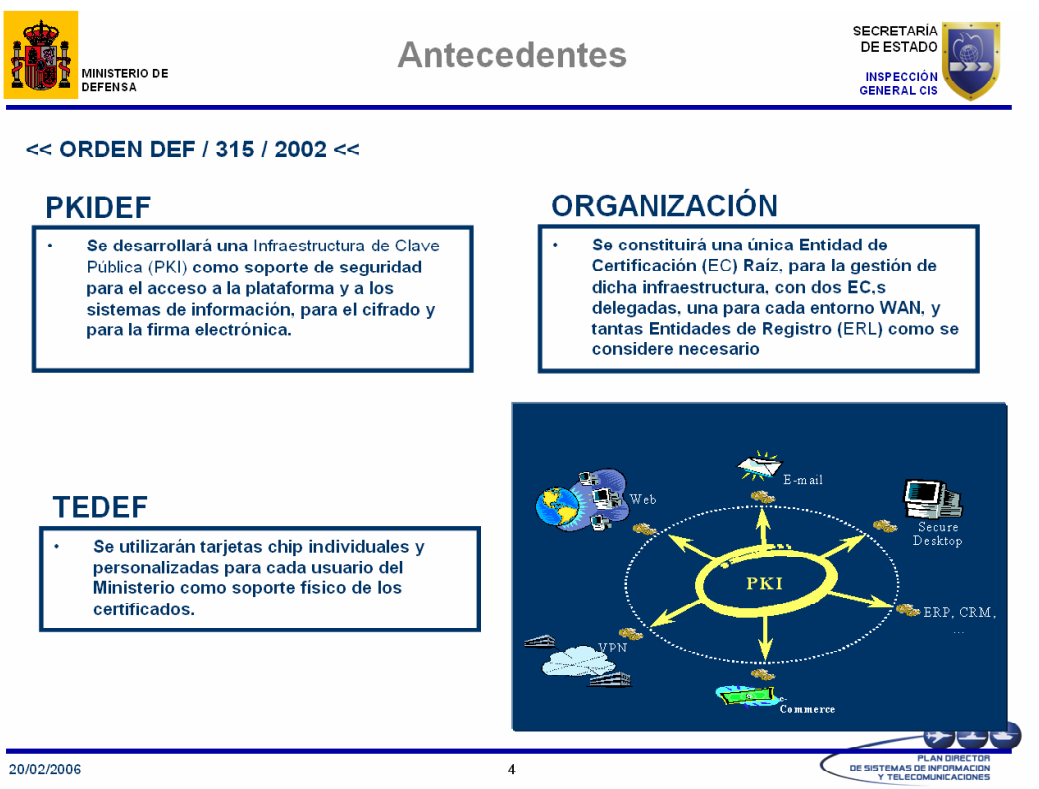
- Autenticación y cifrado de redes de comunicación.
- Acceso Remoto Seguro.
- Identificación de usuarios.
- Firma electrónica de documentos.
- Cifrado de documentos.
- No repudio de mensajes.

Miguel Ángel Rego Fernández

LA IDENTIDAD DIGITAL EN EL MINISTERIO DE DEFENSA

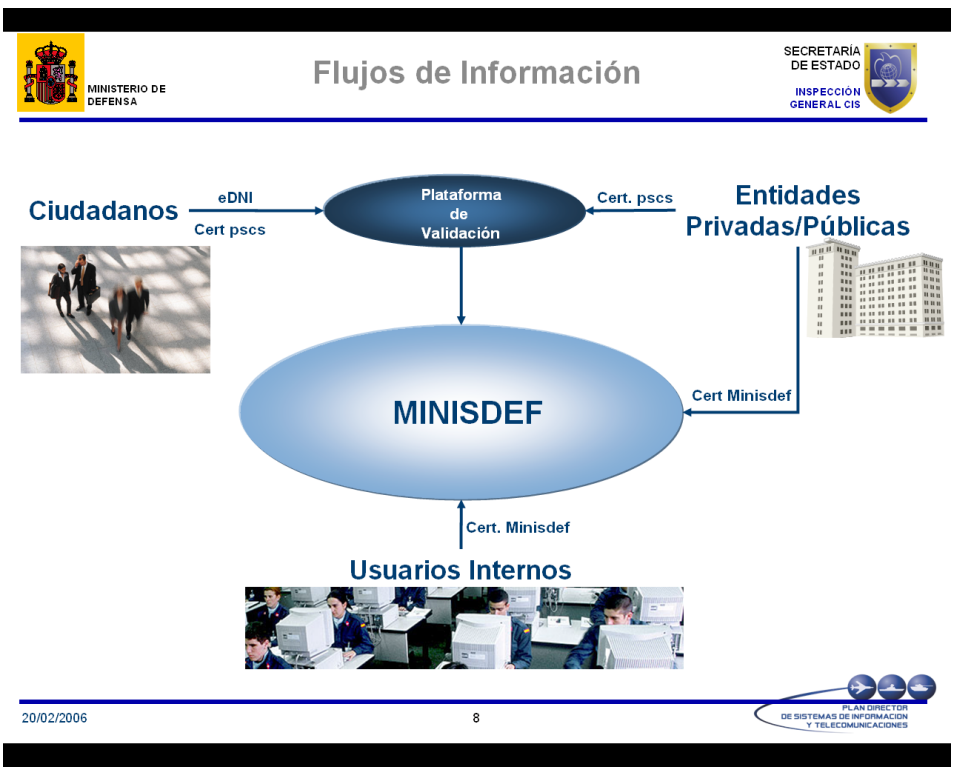
1. Antecedentes

Los Proyectos de Identidad Digital del Ministerio de Defensa se enmarcan dentro de las acciones previstas en el Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa (PDCIS), aprobado por OM 315/2002 de 14 de febrero.



2. Flujos de información

En los flujos de intercambio de información entre el Ministerio de Defensa y ciudadanos, entidades privadas y públicas se aceptarán los certificados emitidos por Prestadores de Servicios de Certificación (PSCs) reconocidos, entre ellos el eDNI.

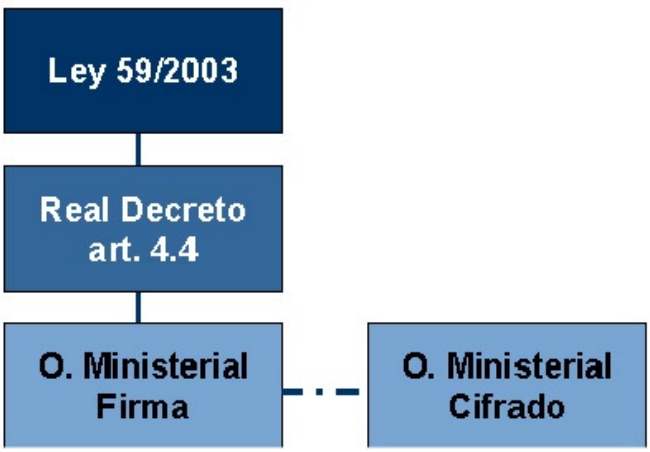


En aquellos casos en que las comunicaciones afecten a información clasificada o el ámbito de la Defensa Nacional, el Ministerio de Defensa utilizará sus propios certificados para realizar el intercambio de datos con entidades públicas, privadas y otras organizaciones. En este sentido, el Ministerio de Defensa ha acometido la elaboración de un Real Decreto que regule la utilización de firma electrónica en el ámbito de la defensa nacional o la información clasificada.

Este Real Decreto desarrolla el artículo 4.4 de la ley 59/2003 de Firma Electrónica, siendo de utilidad para cualquier organismo de la Administración General del Estado cuyas comunicaciones puedan afectar a la información clasificada, a la seguridad pública o a la defensa nacional.

3. Normativa

"La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica. (Art. 4-4 Ley 59/2003)":

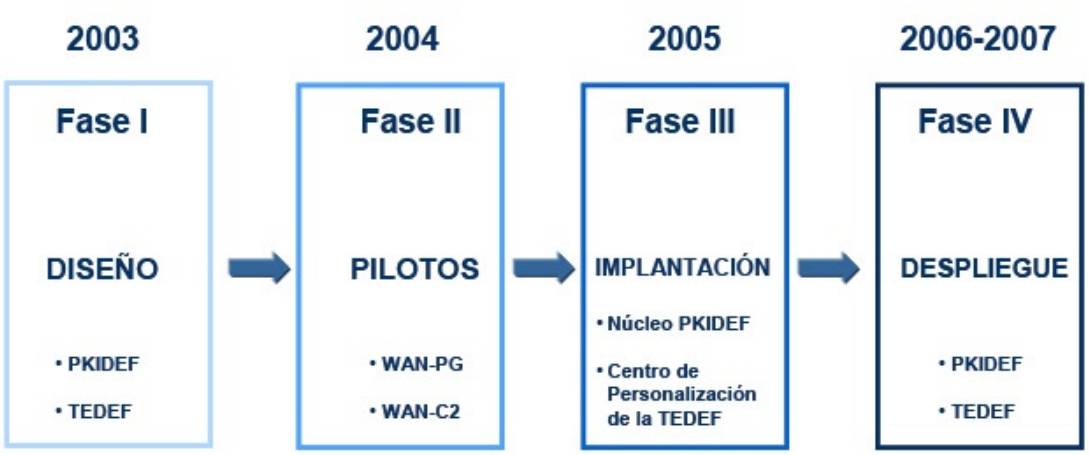


Una vez aprobado el Real Decreto que ha sido desarrollado por el Ministerio de Defensa (todavía no aprobado oficialmente), cada Departamento de la Administración General del Estado podrá desarrollar la normativa específica que regule internamente la utilización de la firma electrónica.

En el caso del Ministerio de Defensa, se desarrollará la normativa relativa al cifrado de la información y las comunicaciones.

4. Fases del proyecto de implantación de la PKI y TEDEF

Las fases de implantación de la PKI y la Tarjeta Electrónica del Ministerio de Defensa son las siguientes:

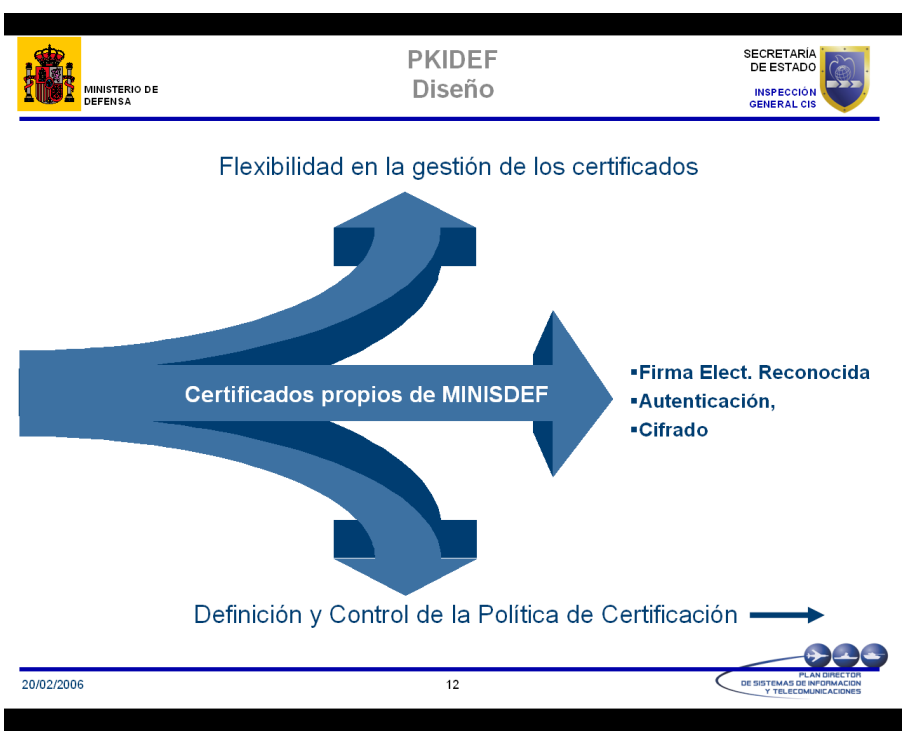


Fase I: Diseño

PKIDEF

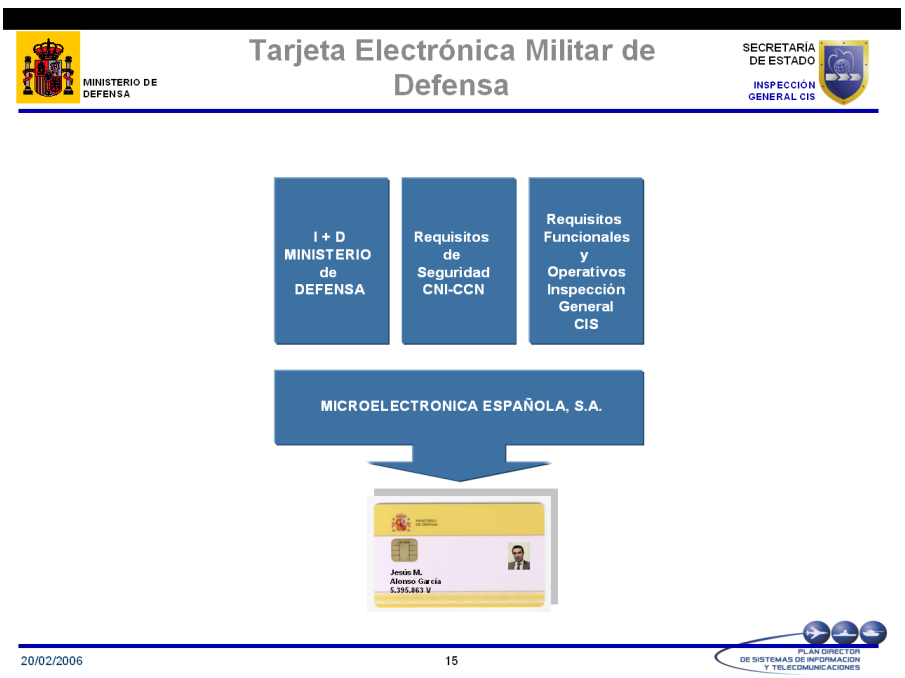
El diseño de la PKIDEF se realizó partiendo de las siguientes premisas:

- Flexibilidad en la gestión de certificados.
- Certificados propios del Ministerio de Defensa:
  - Firma electrónica reconocida.
  - Autenticación.
  - Cifrado.
- Definición y Control de la Política de Certificación, acorde a los requisitos de Defensa:
  - Adaptación de la PKI a las necesidades de Defensa (Internas y Externas).
  - Integración con PKIs externas (OTAN, UE, etc.).
  - Requisitos de Seguridad para el manejo de INFORMACIÓN CLASIFICADA.
  - Interoperabilidad con los propios Sistemas de Defensa.
  - Mayor Control, Rapidez, Operatividad, Eficacia, Seguridad e Interoperabilidad.



TEDEF

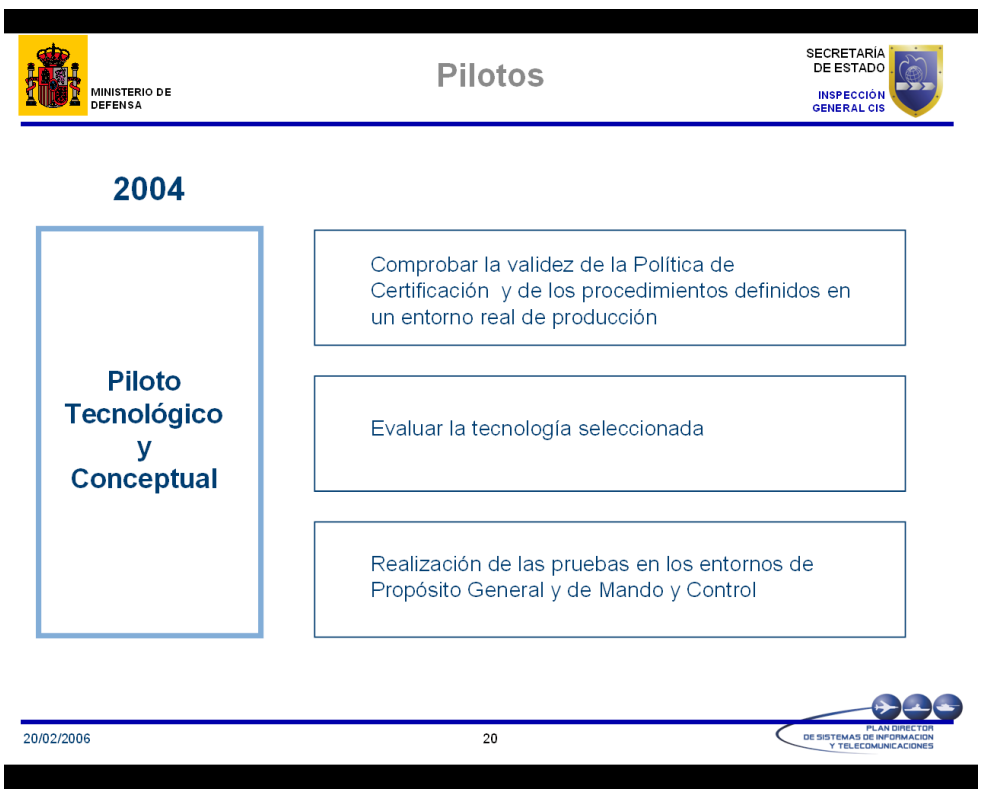
- Tarjeta Alta Seguridad (Criptográfica, Física, Imagen).
- Certificación Nacional SECRETO.
- Imagen Institucional.
- Alta funcionalidad (Firma, Integridad, Cifrado, Identificación, Control Acceso Lógico y Físico).
- Uso universal (WAN-PG [1], WAN-C2 [2] , TIM [3], Seguridad Instalaciones, etc.).
- Dual (Chip con contactos + chip sin contactos).



1 El Ministerio de Defensa dispone de dos redes de área extensa (WAN), físicamente aisladas, que dan soporte a todos los sistemas de información del Ministerio. Por una parte, una WAN para Mando y Control Militar (WAN-C2), y por otra parte, la WAN Corporativa de Propósito General (WAN-PG).
2 WAN-C2: Red de Área Extensa del entorno de Mando y Control Militar.
3 TIM: Tarjeta de Identidad Militar.

Fase II: Pilotos

En el Ministerio de Defensa se realizaron pilotos de implantación reducida de la PKI y TEDEF tanto en el entorno de la red administrativa (WAN-PG), como en la red táctica (WAN-C2).



Fase III: Implantación del Núcleo

En la tercera fase del proyecto, que finalizó en diciembre de 2005, se acometieron las siguientes actividades:

- Implantación de la Infraestructura Central de la PKI.

- Consolidación de los entornos pilotos.

- Integración con el Sistema de Gestión de Ordenes de Proceder.

- Despliegue inicial de servicios a unos 1500 usuarios.

- Implantación del Centro de Personalización de Tarjetas (CPTDEF).

Fase IV: Despliegue

En la última fase del proyecto, actualmente en curso, se están llevando a cabo las siguientes actividades:

- Despliegue de las Autoridades de Registro Local.
- Despliegue de los Puestos de Gestión de Tarjetas.
- Instalación y configuración de los puestos de usuario y despliegue de los servicios de la PKI al resto del Ministerio.

5. Conclusiones

El uso generalizado en el Ministerio de Defensa de Sistemas de Información y Telecomunicaciones (CIS), a través de los cuales se procesa, almacena o transmite información, exige la necesidad de dotarla de la necesaria protección en los sistemas. La implantación de la Infraestructura de Clave Pública y la Tarjeta Electrónica del Ministerio de Defensa permite la utilización de servicios de seguridad en los sistemas y aplicaciones, empleando certificados digitales sobre un soporte seguro.

El modelo de PKI desarrollado por el Ministerio de Defensa permite alcanzar altos niveles de servicio y seguridad, por la autonomía que proporciona la gestión interna que se hace de los certificados digitales y la utilización de productos certificados por el CCN [4]. Este modelo es exportable al resto de la Administración del Estado que habitualmente ha trabajado con arquitecturas de PKI gestionadas externamente.

Por otra parte, la Tarjeta Electrónica de Defensa (TEDEF), certificada por el CNI [5] con altas prestaciones de seguridad, tanto criptográficas como gráficas, es la única tarjeta con la posibilidad de manejar información clasificada SECRETO.

La utilización de estos servicios necesita, dados sus especiales requisitos de seguridad, de una normativa específica que se recoge en el Proyecto de Real Decreto de Firma Electrónica que desarrolla el artículo 4.4 de la Ley 59/2003 de Firma Electrónica.

4 CCN: Centro Criptológico Nacional.

5 CNI: Centro Nacional de Inteligencia