Sistema de distribución electrónica de claves en el ámbito de Defensa

Autor: Fernández-Amigo Aguado, Pablo

Directores: Ares Tarrio, Miguel Angel ; Álvarez Sabucedo, Luis Modesto

Contacto: pferagu@fn.mde.es

Resumen: En este trabajo se pretende identificar la aplicabilidad del desarrollo y posterior implantación de un Sistema de Distribución Electrónica de Claves (EKMS ESP) en el ámbito de Defensa, con el propósito de distribuir claves de ámbito OTAN desde la Agencia Nacional de Distribución (NDA ESP en adelante) a las cuatro Cuentas Principales de los Ejércitos, Armada y Estado Mayor de la Defensa, aprovechando la actual Infraestructura Integral de Información para la Defensa (I3D) para establecer la red de transporte.

El sistema EKMS ESP debe poder distribuir claves electrónicas de una manera segura y rápida a las Cuentas Principales, con una gestión centralizada desde NDA ESP, y que además sea escalable en función de la disponibilidad de nodos que puedan añadirse a las Subcuentas de los distintos ámbitos o incluso a los usuarios finales. Asimismo, dicho sistema debe poder ser acreditable por la Oficina Nacional de Seguridad (ONS). Para ello los equipos cripto y electrónica de red que se empleen en la misma deben estar certificados [1] o en disposición de estarlo.

Esta arquitectura de red permite resolver tres problemas actuales asociadas a la estructura de la cadena cripto en el Ministerio de Defensa: El coste logístico de desplazarse con un dispositivo de carga de claves desde las Cuentas Principales hasta NDA ESP, la disponibilidad del material criptográfico lo antes posible para su distribución posterior a unidades (especialmente a aquellas que van a ser desplegadas en zonas de operaciones o participan en ejercicios internacionales), y la seguridad en la protección de las mismas al no depender de uno o varios mensajeros .

Palabras clave: Claves criptográficas, ámbito, redes, cifradores, distribución.

---

1. Introducción

1.1. El cifrado de la información clasificada en el ámbito de Defensa

El éxito de cualquier operación militar radica en un adecuado empleo del "Mando y Control" (C2) por parte del mando de la operación, entendido el "Mando y Control" como el ejercicio de la autoridad y la conducción y seguimiento por parte de un "comandante" o "Mando Operativo" expresamente designado, sobre las fuerzas asignadas para el cumplimiento de una misión.

Para el adecuado ejercicio del C2, es imprescindible contar con medios que aseguren la adecuada protección de la información clasificada que se emplea en las redes militares. Desde hace varias décadas se han empleado los cifradores como dispositivos fundamentales para cifrar las comunicaciones, tanto en el ámbito de la OTAN como en el nacional.

Hasta hace unos años, los cifradores empleaban claves físicas (cinta perforada) que los operadores debían cargar manualmente en el equipo para que éste pudiera operar. Hoy día todas las claves que produce y distribuye DACAN en el ámbito de la OTAN son de formato electrónico. Además, la doctrina OTAN (2) establece que la distribución de este material criptográfico se hará por medios electrónicos siempre que sea posible para evitar posibles compromisos de seguridad.

1.2. Distribución de claves en el Ministerio de Defensa y la modernización cripto

En lo relativo a la distribución de claves de ámbito OTAN, el organismo responsable de distribuirlas a los países de la Alianza es la Agencia de Distribución y Contabilidad (DACAN, en adelante). Cada país dispone de un organismo llamado Agencia Nacional de Distribución (NDA por sus iniciales en inglés, en caso de España, NDA ESP) que recibe las claves en formato electrónico por un sistema de gestión electrónica llamado NEKMS. Después, cada NDA es responsable de distribuir este material a sus Cuentas Criptográficas subordinadas. En el ámbito de Defensa, estas Cuentas son las pertenecientes al Ejército de Tierra, la Armada, el Ejército del Aire y el Estado Mayor de la Defensa (EMAD). Cada ámbito es responsable, una vez recibidas las claves criptográficas, de realizar la distribución a sus subcuentas criptográficas, y de éstas a las unidades.

Un factor que se debe tener en cuenta es la profunda modernización criptográfica que se está llevando en el seno de la Alianza, y que en su documento [2] incluye como elemento clave el desarrollo de sistemas de distribución electrónica de claves. Se pretende desarrollar una infraestructura de gestión electrónica de claves (NKMI) que permita a cada país desarrollar su propio sistema nacional y pueda incorporarse a esta infraestructura con las debidas condiciones de seguridad e interoperabilidad.

1.3. El sistema de distribución electrónica de claves del Ministerio de Defensa

Con los condicionantes vistos hasta ahora, el objetivo por lo tanto es desarrollar un sistema de distribución de claves que cumpla las siguientes características:

- El sistema debe poder ser acreditable por la Oficina Nacional de Seguridad (ONS). Para ello los equipos cripto y electrónica de red que se empleen en la misma deben estar certificados o en disposición de estarlo.

- El sistema debe de emplear una red de transporte que sea común a los ámbitos que van a emplearlo: Ejército de Tierra, Armada, Ejército del Aire, EMAD y la Agencia Española de Distribución (NDA ESP).
- El sistema debe ser escalable, para que pueda ajustarse fácilmente a posibles cambios en la estructura de la organización.
- El sistema debe disponer de una configuración dinámica para necesidades temporales, como por ejemplo la distribución de claves criptográficas en un área de operaciones.
- El sistema debe permitir una gestión centralizada que permita una distribución desde NDA ESP a los usuarios de la red.

Además, el sistema debe de incorporar las siguientes funcionalidades:

- Almacenamiento seguro de claves.
- Importación y exportación de claves electrónicas en el sistema.
- Gestión y distribución electrónica de claves.
- Contabilidad y registro de claves y equipos criptográficos.

2. Desarrollo

2.1 Estado del arte

Como ya se ha comentado, la OTAN está en un proceso de modernización criptográfica profundo, puesto que hay una gran variedad de productos criptográficos cuya obsolescencia hace que estén descertificados o próximos a descertificar. En algunos casos existen productos ya identificados como sustitutos de cifradores antiguos, pero en otros no, y sólo los países criptoproductores (fundamentalmente EE. UU. y Reino Unido, y en menor medida Alemania, Francia, Italia y España) tienen capacidad de desarrollar dispositivos que puedan cumplir los requisitos necesarios.

Una de las áreas que se quiere potenciar con el desarrollo de la NATO Key Management Infraestructure (NKMI) es precisamente, la distribución electrónica de claves. El objetivo es desarrollar un estándar que permita una interoperabilidad entre los sistemas nacionales de distribución de claves y los dispositivos criptográficos para el usuario final (ECU[1]). Teniendo en cuenta que algunos de los ECUs pueden haber sido a proveedores extranjeros, la integración de éstos con el sistema nacional de distribución de claves que tenga dicho país puede simplificarse con la adopción de una especificación de interoperabilidad de claves.

Conviene mencionar también el hecho de que los equipos criptográficos que actualmente se emplean en la distribución vía OTAT/OTAD[2] también se ven afectados por la descertificación del algoritmo criptográfico que emplean. Esté método de distribución de claves electrónicas, muy empleado en las marinas de la OTAN, aunque sólo sirve para casos puntuales (no se pueden transmitir grandes volúmenes de datos) es una de las áreas que deben ser renovadas.

Por último, hay que mencionar que en el ámbito nacional también se están modernizando los cifradores bajo la supervisión del Centro Criptológico Nacional, debido a que aún se emplean modelos

[1] End Cryptographic Unit.
[2] OTAD: Over the air distribution /OTAT: Over the air transmission.

antiguos de la familia EPICOM en algunos casos, pero la telegestión de estos equipos no se ve afectada, y no es objeto de este trabajo.

2.2 Arquitectura objetivo

En el modelo planteado, se pretende implantar una red de nodos con funcionalidad EKMS[3] desarrollados por la empresa TECNOBIT, utilizando las capacidades de transporte de la red I3D[4] del Ministerio de Defensa. El desarrollo de este sistema en el ámbito de Defensa está contemplado en el documento [3] como uno de los servicios de Infraestructura tecnológica.

La jerarquía del sistema es a modo de árbol, donde el nodo principal de NDA ESP tiene como nodos dependientes de él a los nodos del Ejército de Tierra, Armada, Ejército del Aire y EMAD. Al ser un sistema distribuido los nodos no tienen porqué estar en la misma sala o zona geográfica, pueden estar localizados en distintos puntos del país siempre y cuando estén conectados a la misma red.

Al estar conectando dos sistemas (la red EKMS-ESP y la red I3D), deberemos cumplir con lo establecido en la Instrucción Técnica [4], e implementar un Sistema de Protección de Perímetro (SPP), que es una combinación de recursos hardware y/o software llamados Dispositivos de Protección de Perímetro, cuya finalidad es mediar entre el tráfico de salida y entrada. Para este caso se establece una Pasarela en una zoma desmilitarizada (DMZ) con un cifrador IP.

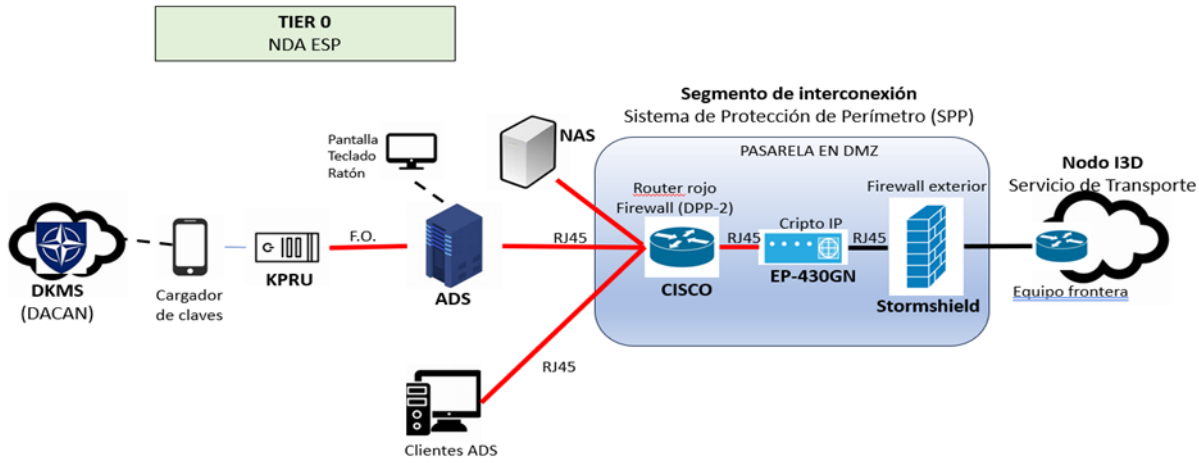

Figura 1. Ejemplo de interconexión entre nodo EKMS y red I3D

La información que se transporte por esta red irá cifrada con varias capas, una la que dan los propios nodos a las claves, más la de otorgan los cifradores IP que se colocarán en el segmento de interconexión. Esto significa que las claves viajan “en negro”, y sólo pueden ser utilizadas en destino una vez desencriptadas.

2.3 Gestión de los nodos EKMS-ESP

Para la gestión remota de los distintos equipos existirá un Nodo de Gestión de Servicios de Seguridad (NGSS), controlando y supervisando la actividad dentro de la red y asegurando la configuración del segmento de interconexión según los procedimientos que establece el CCN para la gestión de la información clasificada.

[3] Electronic Key Management System: Sistema de gestion electronica de claves.
[4] Infraestructura Integral de Información para la Defensa.

Existirán estaciones de gestión y control remoto de la seguridad que dispongan de acceso remoto a la LAN EKMS-ESP, así como a los cifradores IP y a los cortafuegos Stormshield. La responsabilidad del nodo NGSS sería de NDA ESP como Autoridad del Sistema, punto clave y cabeza en la jerarquía de la red.

La gestión remota de los cortafuegos se realizaría mediante la implementación de una Red Privada virtual (VPN) utilizando protocolo IPSEC, otorgando seguridad y la integridad en la gestión de los firewalls. En cuando a la gestión de los cifradores IP, debe de hacerse mediante un centro de gestión de cifradores IP semejante al que existe en la Cuenta de Cifra del EMAD o de la Armada. Por último, para la gestión remota de los router CISCO, se propone establecer un túnel GRE permitiendo las comunicaciones encaminamiento entre los router rojos de la EKMS-ESP.

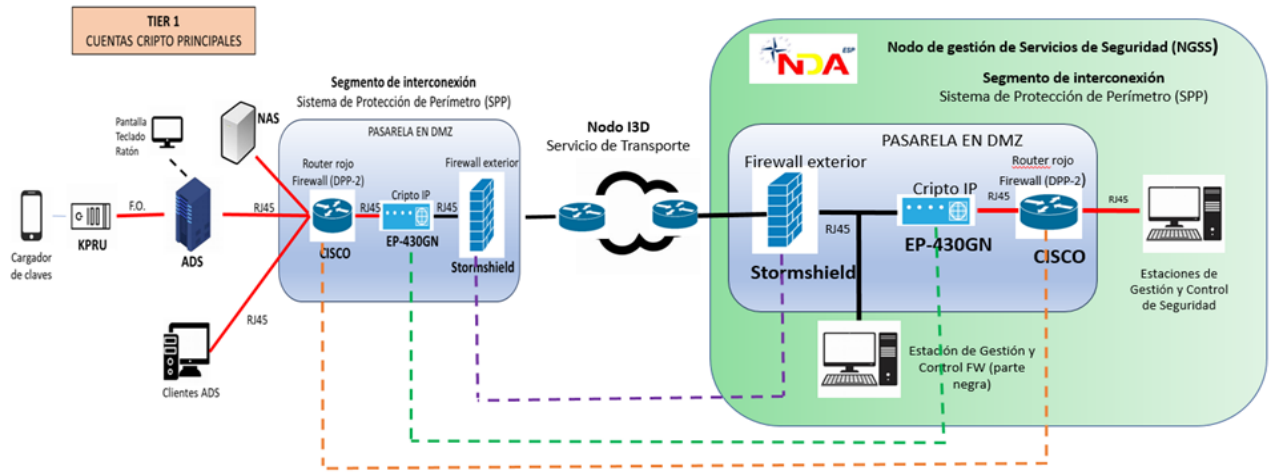

Figura 2. Conexión entre NGSS y nodos EKMS

3. Conclusiones

El establecimiento del sistema EKMS-ESP en este primer nivel puede ser la base para escalar la red progresivamente en los distintos ámbitos, marcando un hito en la gestión del material criptográfico del ámbito de Defensa. La Armada es el ámbito mejor posicionado, puesto que cuenta con nodos EKMS para sus subcuentas de cifra y se plantea la adquisición de nodos de menor nivel para las unidades.

En el aspecto operativo, la red EKMS-ESP facilita una gestión eficiente y centralizada de las claves de cifrado. Esto no sólo mejora la rapidez y eficacia en la distribución de claves, sino que también reduce la posibilidad de errores humanos, un factor crítico en la gestión de la seguridad de la información. El sistema permite no sólo una distribución más ágil de las claves, sino una producción de la documentación asociada a las mismas (partes de transferencia, de destrucción, inventarios, etc.) más sencilla para los criptocustodios de cada unidad, logrando un mayor control y seguimiento de un material tan sensible.

La implantación de este sistema no solo es necesaria desde el punto de vista de la seguridad, si no por la futura descertificación de los equipos que se usan para hacer distribución OTAD/OTAT, que imposibilitará la distribución de las claves electrónicas por esta vía en el futuro en casos puntuales y de necesidad.

Estratégicamente, la implantación de este sistema colocaría al Ministerio de Defensa en la vanguardia en términos de capacidades de cifrado y seguridad de la información. Esto no sólo refuerza la postura de defensa nacional, sino que puede contribuir a la imagen de España como un aliado de confianza y tecnológicamente avanzado dentro del seno de la OTAN.

Agradecimientos

A los directores de mi Trabajo de Fin de Máster, a los profesores del CUD de la Escuela Naval Militar, a mis compañeros de Máster y de Especialidad y a mi familia, por haberlo hecho posible.

Referencias

[1] C. C. Nacional, *Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicaciones.*

[2] I. M. Staff, *Cryptographic Modernisation Timed Roadmap V7 (NATO SECRET)*, 2020.

[3] S. d. E. d. Defensa, *Instrucción 58/2016 Arquitectura Global CIS/TIC del Ministerio de Defensa*, 28 de octubre de 2016.

[4] C. C. Nacional, *CCN-STIC-302 "Interconexión de sistemas de las Tecnologías de la Información y las Comunicaciones que manejan información clasificada"*.