MINISTERIO DE DEFENSA

SECRETARIA DE ESTADO DE DEFENSA

Instituto Nacional de Técnica Aeroespacial

Área de especialización: Seguridad y criptografía de los sistemas espaciales.

Supuesto Práctico 1

Una entidad del ámbito aeroespacial se propone implementar un sistema acreditable de intercambio de archivos que utilizando operaciones criptográficas permita conservar su integridad, confidencialidad y no repudio de los ficheros en reposo.

El sistema debe permitir el acceso de múltiples receptores a cada archivo mediante el uso de certificado sin que estos conozcan la clave utilizada para el cifrado del archivo.

Dicho sistema además debe asegurar un canal de transferencia entre los participantes que garantice, por una parte, la autenticación mutua entre ellos, y las mismas propiedades de seguridad de los archivos en reposo.

a) Análisis de riesgos
b) Contramedidas propuestas para su mitigación
c) Hipótesis y principios de la solución adoptada
d) Descripción de la solución propuesta. Estándares aplicables.
e) Acreditabilidad del sistema

MINISTERIO DE DEFENSA

SECRETARIA DE ESTADO DE DEFENSA

Instituto Nacional de Técnica Aeroespacial

Área de especialización: Seguridad y criptografía de los sistemas espaciales.

Supuesto Práctico 2

En un futuro Programa Espacial de la Unión Europea se decide incluir un nuevo componente cuyo objetivo sea proporcionar un servicio global basado en una constelación de satélites europea propia que permita la transmisión robusta y segura de claves criptográficas entre las entidades y los usuarios a los que se les conceda autorización de acceso a tal servicio.

Elabórese un diseño preliminar, similar al requerido para una revisión preliminar de diseño (PDR), de la solución propuesta, y desarróllese de acuerdo con el siguiente esquema:

a) Hipótesis y principios de la solución adoptada
b) Descripción de la solución funcional y documentación de diseño que incluya: croquis general, definición de infraestructuras, componentes del sistema, etc.
c) Modelización de amenazas
d) Contramedidas adoptadas para garantizar la seguridad del sistema y la continuidad del servicio
e) Estrategia de acreditación de la seguridad para su entrada en servicio

MINISTERIO DE DEFENSA

SECRETARIA DE ESTADO DE DEFENSA

Instituto Nacional de Técnica Aeroespacial

Área de especialización: Seguridad y criptografía de los sistemas espaciales.

Supuesto Práctico 3

En la definición de los requisitos de un nuevo satélite se establece que sus datos de telemetría serán accesibles solamente para una relación de usuarios autorizados.

Los datos serán enviados a una estación terrestre y serán almacenados en un servidor centralizado situado en las instalaciones de la organización encargada de tal operación.

Únicamente los usuarios legítimamente autorizados deben tener acceso a dichos datos, por lo que deberá garantizarse la confidencialidad punto a punto de los mismos, ni los administradores del equipo ni otros usuarios podrán acceder a los mensajes.

Se identifican tres tipos de usuarios:

I. Usuarios conectados a la misma red del servidor.

II. Usuarios conectados a una red diferente, pero dentro de la organización.

III. Usuarios conectados desde redes externas, como Internet.

Se pide diseñar y desarrollar una solución que garantice el cumplimiento del requisito establecido, siguiendo el siguiente esquema:

a) Decisiones de diseño justificadas atendiendo a un modelado de amenazas,
b) Arquitectura de seguridad propuesta, a nivel organizativo y técnico,
c) Mecanismos criptográficos necesarios para cumplir con los requisitos del sistema,
d) Descripción de la operativa.