Comunicaciones certificadas y encriptadas para el gobierno

Cifrado de extremo a extremo validado por NIAP y FIPS con criptografía post-cuántica para CUI para Comunicaciones clasificadas.

Cellcrypt Federal, una suite completa de soluciones comerciales para comunicaciones clasificadas (CSfC) diseñada para su uso en redes gubernamentales aprobadas, proporciona seguridad completa de extremo a extremo para llamadas de voz y video, llamadas de conferencia, mensajería y transferencias de archivos, con administración, integración y control de espectro completo.

Cellcrypt Federal proporciona la máxima garantía para las comunicaciones en entornos de confianza cero, donde se supone que las redes se ven comprometidas de forma proactiva. Cellcrypt Federal utiliza múltiples capas de cifrado para proteger los datos entre puntos finales mutuamente autenticados y emplea intercambio de claves efímero para garantizar que se genere un nuevo conjunto de claves para cada mensaje, transferencia de archivos o llamada de voz, negando la necesidad de una administración centralizada de claves COMSEC.

La implementación de Cellcrypt Federal de la Suite de Algoritmos de Seguridad Nacional Comercial (CNSA) cumple o excede los estándares de protección de información a Top Secret según lo definido por la NSA (Agencia de Seguridad Nacional).

CIFRADO DE EXTREMO A EXTREMO CON PROTECCIÓN POST-CUÁNTICA A TRAVÉS DEL TÚNEL NIAP

Túnel NIAP

Todas las comunicaciones están protegidas por una arquitectura validada por NIAP, donde la capa más externa y todos los enlaces del servidor están protegidos con TLS, utilizando algoritmos validados por NIST (ECC-384 y AES-256). La aplicación de una arquitectura NIAP cumple con el estándar de comunicaciones Top Secret en las redes del Gobierno.

Arquitectura del Túnel NIAP

Esta arquitectura está validada para proteger las comunicaciones US Classified Secret y Top Secret. Cellcrypt Federal proporciona esto como línea de base, pero agrega cifrado E2E con criptografía post-cuántica tunelizada a través de la arquitectura.

Cifrado de extremo a extremo del algoritmo de seguridad nacional comercial (CNSA)

Todos los datos se ofuscan utilizando ChaCha20-256, para mitigar cualquier vulnerabilidad potencial de AES en el futuro, luego se protegen de extremo a extremo utilizando la curva elíptica y la criptografía de clave simétrica que cumple con los estándares de longitud de clave más altos de la Suite CNSA de la NSA para comunicaciones de alto secreto.

Cifrado de extremo a extremo con seguridad cuántica a través de una arquitectura de túnel NIAP

Criptografía post-cuántica

El núcleo criptográfico se superpone criptográficamente utilizando Supersingular Isogeny Diffie-Hellman Key Exchange (SIDH 751) para voz y encapsulación de claves de Isogenia Supersingular (SIKE 751) para mensajería y archivos, proporcionando protección post-cuántica.

CELLCRYPT FEDERAL
CARACTERÍSTICAS

Mensajería instantánea segura y transferencia de archivos

- Cellcrypt Federal proporciona mensajería instantánea encriptada de extremo a extremo, uno a uno / grupal con fotos, videos y notas de voz.
- Envíe transferencias de archivos de gran tamaño (500 MB+).
- Cifra todos los contactos, mensajes y archivos almacenados en la aplicación.

Llamadas seguras de voz y video

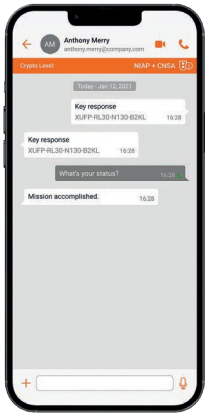
- Voz y video seguros sobre IP (V VoIP) proporciona cifrado de extremo a extremo entre teléfonos inteligentes, tabletas y computadores de escritorio.
- Llamadas seguras realizadas desde cualquier red IP.
- Proporciona autenticación completa de todas las partes en una llamada, eliminando la suplantación de identidad y los ataques man-in-the-middle.
- La Validación de Cellcrypt Federal garantiza la protección de las comunicaciones Top Secret, con facilidad de implementación a través de App y Web.

Llamadas de conferencia seguras

- Conferencias fáciles de realizar sin complicaciones.
- Autenticación única sin pines ni contraseñas.
- Cellcrypt Federal Voice conecta consolas PBX con teléfonos móviles, compuadores de escritorio en conferencias de voz y video.

Una solución solo de software

- Aplicaciones de cliente nativas para Apple iPhone y iPad, teléfonos inteligentes / tabletas Android y dispositivos Microsoft Windows.
- Sin dependencias de hardware, la aplicación se puede descargar de las tiendas de aplicaciones de Apple o Google para su uso inmediato.



Gestión y control de TI

- El Cellcrypt Federal Private Switch le da a la organización un control completo de toda la pila de comunicaciones.
- Los metadatos y la información confidencial están protegidos, con una gestión de espectro completo de usuarios, políticas y permisos.
- El cellcrypt Federal Private Switch se puede implementar en las instalaciones, en varias nubes (Azure o AWS) o en el campo, incluso en un bloc de notas.
- Integración perfecta con Azure Active Directory.

Validaciones y Certificaciones de Cellcrypt Federal

Cellcrypt está validado por el US National Information Assurance Asociación (NIAP) bajo su Esquema de Evaluación y Validación de Criterios Comunes (CCEVS).

Cellcrypt está validado para su uso como protocolo de voz sobre Internet (VoIP) en un componente de Soluciones Comerciales para Soluciones Clasificadas (CSfC).

Cellcrypt está validado por el Instituto Nacional de Estándares y Tecnología (NIST) según FIPS 140-2.

Los productos seguros de voz sobre IP de Cellcrypt Federal figuran en el Catálogo de productos de garantía de información de la OTAN (NIAPC).

Descarga Cellcrypt Federal Aquí:

www.cellcryptfederal.com

NAVGIS CORPORATION
Carrera 13 # 90-17, Piso 1
Bogotá D.C, 110221
Colombia
Teléfono: +573003396273