中華資安國際
CHT Security

CypherCom:

Un sistema de comunicaciones con cifrado de extremo a extremo
Basado en protección criptográfica a nivel de hardware

Vincent Wang, Doctor en Filosofía.

Compañía de seguridad CHT, Ltd.

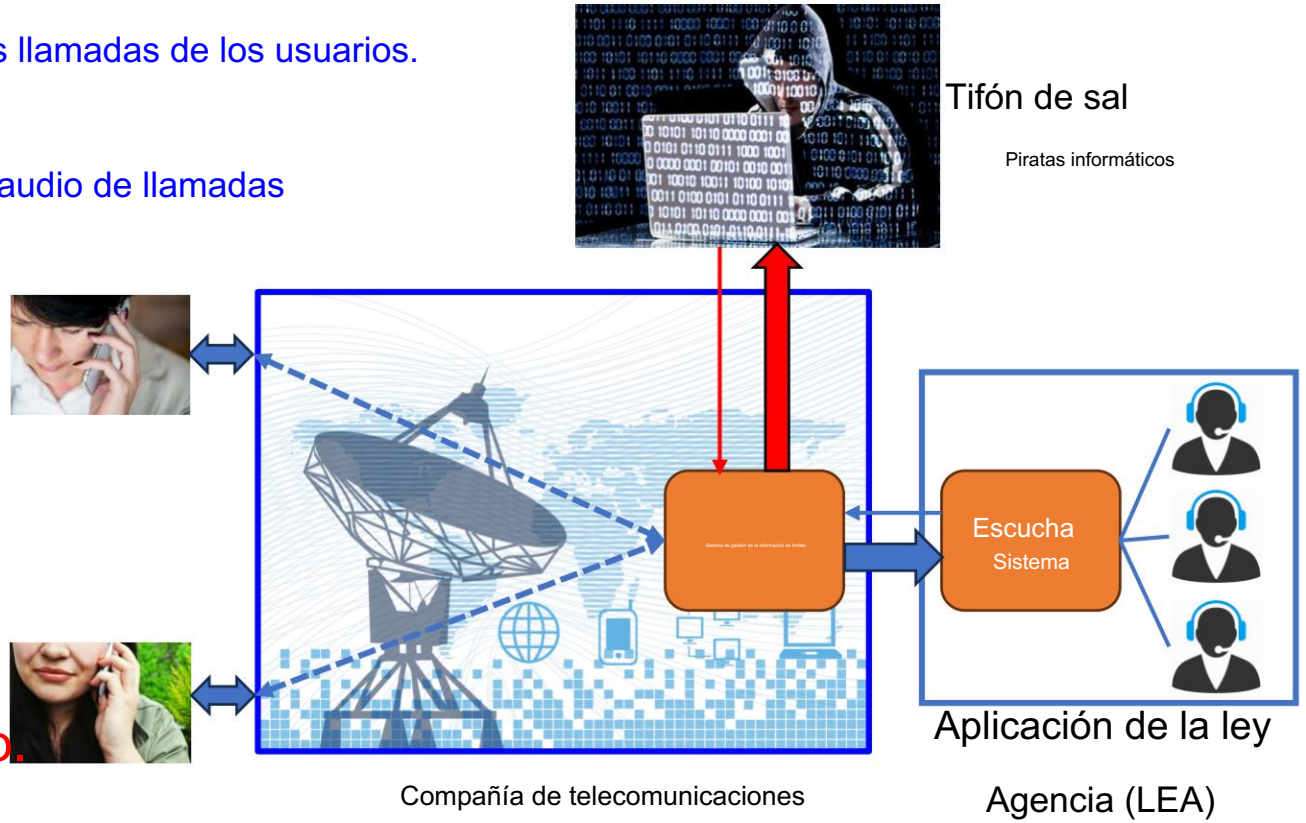
Orden del día

1. Espionaje de Salt Typhoon: Por qué es esencial el cifrado de extremo a extremo (E2EE)
2. Violación del chat grupal de Signal: Por qué la gestión de identidades es fundamental
3. Sistema de comunicaciones E2EE de CypherCom 4.
Riesgos de fuga de claves de la protección de claves basada en
software 5. Ventajas de la protección de claves basada en
hardware 6. Gestión de identidades y gestión de claves para suscriptores
7. Resiliencia en las comunicaciones E2EE
8. Conclusiones clave

Espionaje del tifón salino: por qué es esencial el cifrado de extremo a extremo (E2EE)

- El 13 de noviembre de 2024, una declaración conjunta del FBI y la CISA modificó que una Un grupo de piratas informáticos afiliado a China ha comprometido las redes de varias empresas de telecomunicaciones en EE. UU.:
  - Los piratas informáticos pudieron acceder a los metadatos de las llamadas de los usuarios. y mensajes de texto.
  - En algunos casos, los hackers lograron obtener grabaciones de audio de llamadas telefónicas realizadas por personas de alto perfil. • El 18 de diciembre de 2024, CISA

publicó una "Guía de mejores prácticas en comunicaciones móviles" y recomendó encarecidamente a las personas con un perfil muy específico que utilicen únicamente comunicaciones cifradas de extremo a extremo.



LIMS: Sistema de Mediación de Interceptación Legal

Violación del chat grupal de Signal: Por qué la gestión de identidades es fundamental

- El 24 de marzo de 2025, Jeffrey Goldberg, editor en jefe de The Atlantic, reveló que un grupo de funcionarios de seguridad nacional de Estados Unidos lo agregó por error a un chat grupal en la aplicación de mensajería encriptada Signal sobre planes altamente sensibles para bombardear objetivos hutíes en Yemen.

- ¿ Cómo pudo pasar esto?
  1. En una plataforma de redes sociales en la nube como Signal, WhatsApp, etc., cualquier persona con un número de teléfono móvil o una dirección de correo electrónico puede registrar una cuenta con un nombre.
  2. Podría ocurrir un error al agregar a alguien al grupo de chat.
  3. Las personas no siempre son quienes dicen ser en línea.

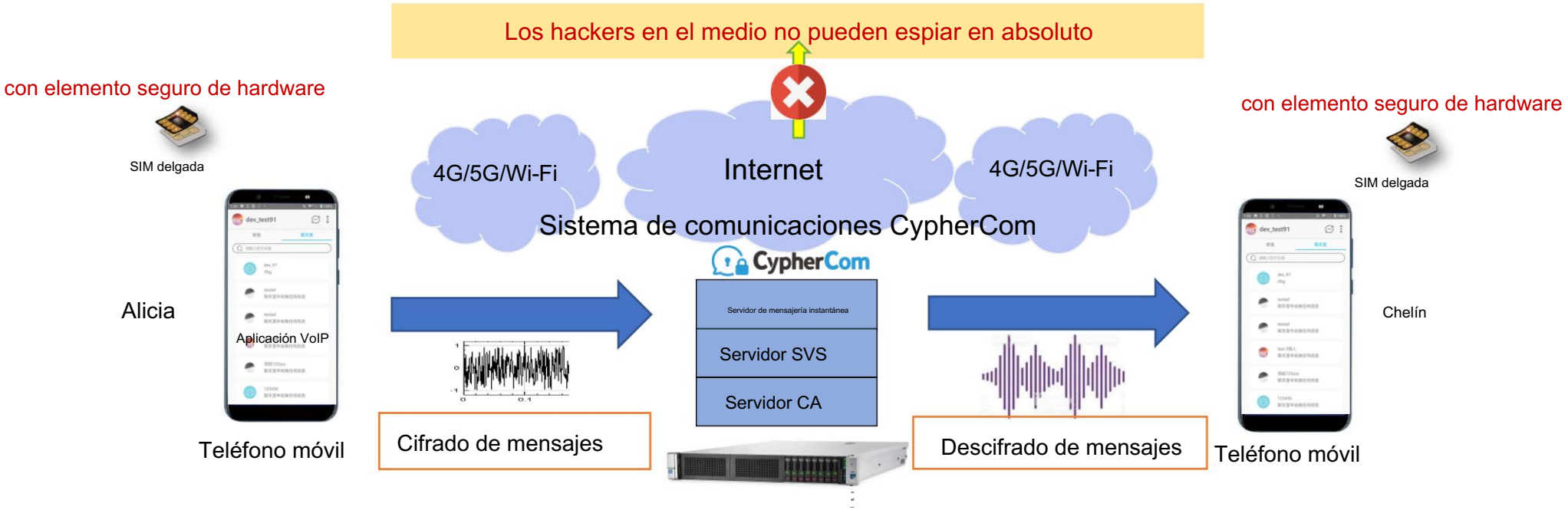
     (En realidad, la NSA envió internamente un boletín especial de seguridad operativa llamado "Vulnerabilidad de la señal" a sus empleados en febrero de 2025 advirtiéndoles sobre este riesgo).

- Pautas de identidad digital NIST SP 800-63:
  - Nivel de garantía de identidad (IAL): se refiere al proceso de comprobación de identidad.
  - Nivel de garantía de autenticación (AAL): se refiere al proceso de autenticación.

- La mayoría de las plataformas de redes sociales en la nube no son responsables de la gestión de identidad y Por lo tanto, falta IAL.

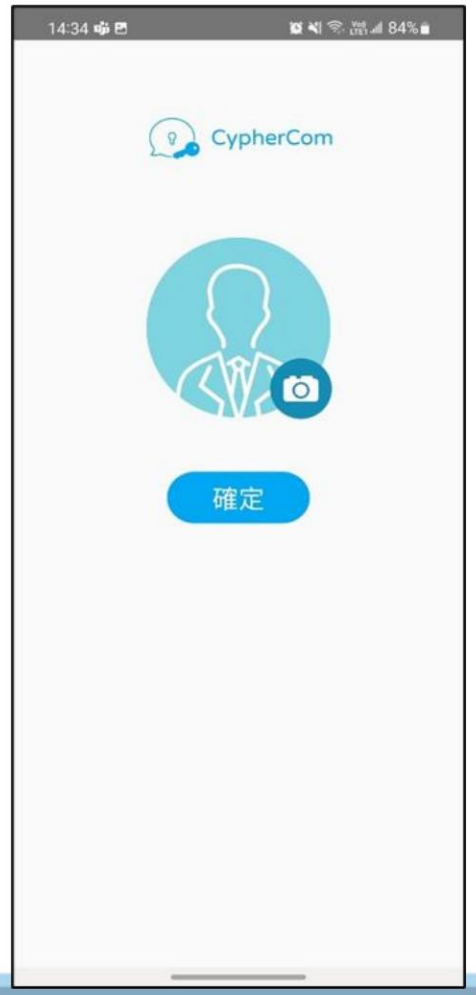
Sistema de comunicaciones CypherCom E2EE

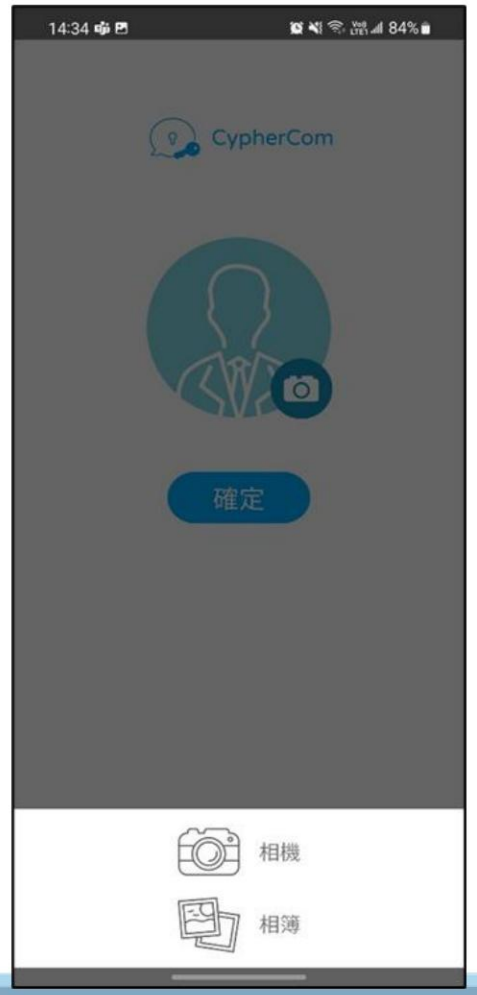
- Elemento seguro de hardware (SIM delgada) con certificación FIPS 140-2 Nivel 3 para garantizar que la clave privada no pueda ser comprometida.
- Admite cifrado de extremo a extremo (E2EE) de 256 bits de voz, video, texto, fotos y archivos durante comunicaciones.



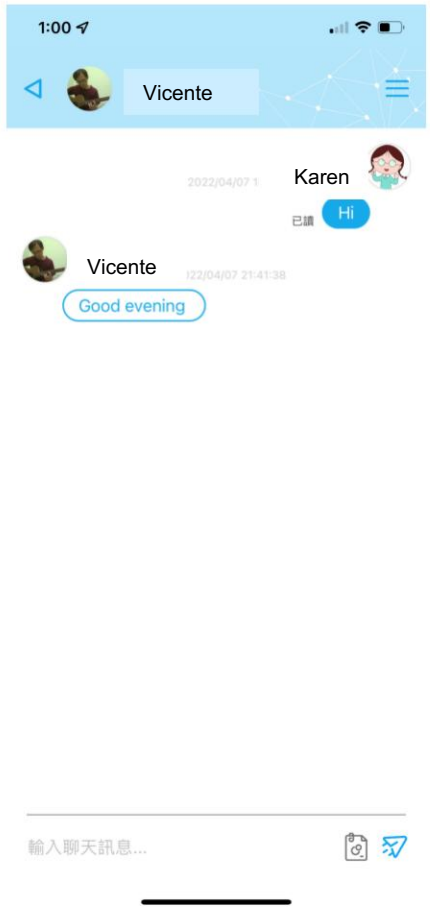
Interfaz de usuario de la aplicación CypherCom

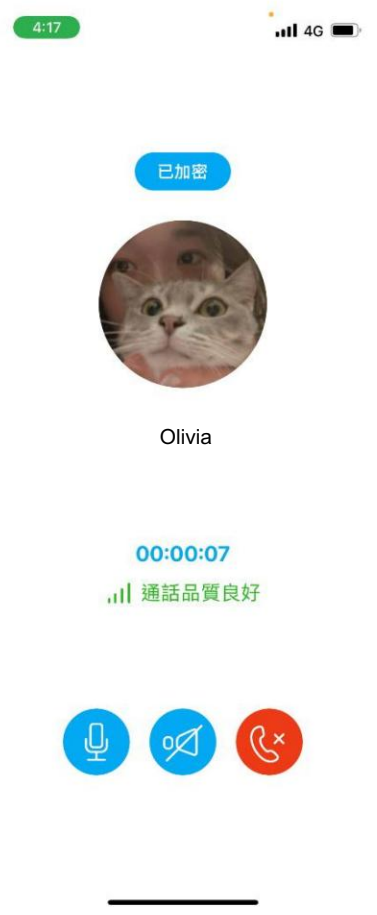
- Registro y configuración de cuenta





- Mensajería instantánea, transmisión de archivos y llamadas de voz/video.

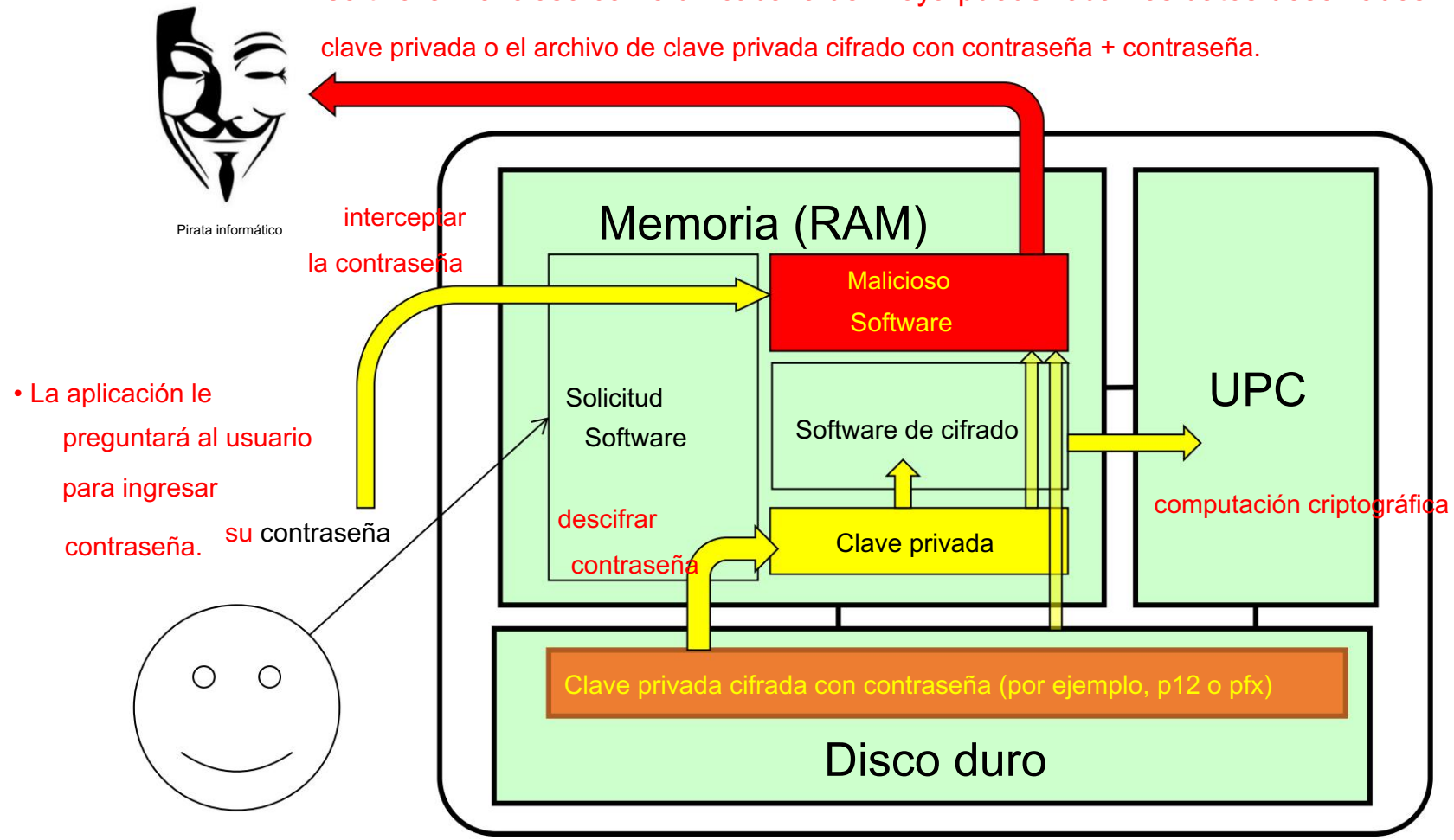




Riesgos de fuga de claves en la protección de claves basada en software

• El software malicioso como un caballo de Troya puede robar los datos descifrados.

clave privada o el archivo de clave privada cifrado con contraseña + contraseña.



• La aplicación le preguntará al usuario para ingresar su contraseña.

• Para que la CPU pueda utilizarlo, el archivo de clave privada cifrado con contraseña en el disco duro debe descifrarse en la memoria.

Eventos de ciberseguridad con fuga de claves

1. 2023/07: Violación de la clave de firma del token de autenticación de la cuenta Microsoft

Las agencias del gobierno de EE. UU. fueron hackeadas después de que Microsoft perdiera sus claves

https://www.ithome.com.tw/news/158631

Entrada del blog de Microsoft: Resultados de las principales investigaciones técnicas para la adquisición de la clave Storm-0558

Resultados de importantes investigaciones técnicas para la adquisición de claves de Storm 0558

Nuestra investigación reveló que una falla del sistema de firma del consumidor en abril de 2021 generó una instantánea del proceso bloqueado ("volcado de memoria"). Estos volcados de memoria, que ocultan información confidencial, no deberían incluir la clave de firma. En este caso, una condición de carrera permitió que la clave estuviera presente en el volcado de memoria (este problema se ha corregido). Nuestros sistemas no detectaron la presencia de materiales de la clave en el volcado de memoria (este problema se ha corregido).

Después de abril de 2021, cuando la clave se filtró al entorno corporativo en el volcado de memoria, el actor Storm-0558 logró comprometer la cuenta corporativa de un ingeniero de Microsoft. Esta cuenta tenía acceso al entorno de depuración que contenía el volcado de memoria, el cual contenía incorrectamente la clave. Debido a las políticas de retención de registros, no disponemos de registros con evidencia específica de esta exfiltración por parte de este actor, pero este fue el mecanismo más probable por el cual obtuvo la clave.

2.

Eventos de ciberseguridad con fuga de claves

2. Evento Operación ShadowHammer del 3/2/2019: Se robó la clave de firma de código para actualizaciones de software de uno de los fabricantes de computadoras más grandes del mundo.

   Noticias de Media: https://securelist.com/operation-shadowhammer/89992/

   Extractos de noticias de Motherboard Midia: https://www.vice.com/en/article/pan9wn/hackers-secuestraron-actualizaciones-de-software-de-asus-para-instalar-puertas-traseras-en-miles-de-computadoras

   Investigadores de la firma de ciberseguridad Kaspersky Lab afirman que la Compañía A, uno de los mayores fabricantes de computadoras del mundo, fue utilizada para instalar inadvertidamente una puerta trasera maliciosa en miles de computadoras de sus clientes el año pasado, después de que atacantes comprometieran un servidor de la herramienta de actualización de software en vivo de la compañía. El archivo malicioso estaba firmado con certificados digitales legítimos de la Compañía A para que pareciera una actualización de software auténtica de la compañía, según Kaspersky Lab.

   Los investigadores estiman que medio millón de máquinas Windows recibieron la puerta trasera maliciosa a través del servidor de actualizaciones de la Compañía A, aunque los atacantes parecen haber atacado solo a unos 600 de esos sistemas. El malware buscaba los sistemas objetivo a través de sus direcciones MAC únicas. Una vez en un sistema, si encontraba una de estas direcciones objetivo, el malware se conectaba a un servidor de comando y control operado por los atacantes, que a su vez instalaba malware adicional en esas máquinas.

Eventos de ciberseguridad con fuga de claves

3. 2015/09: Una gran empresa de dispositivos de red publicó accidentalmente sus claves privadas de firma de código para los certificados que utilizan para firmar su software.

Noticias de Media: https://news.ycombinator.com/item?id=10235382

La empresa D publicó accidentalmente claves privadas para los certificados que utiliza para firmar su software. Fue posible extraer las claves de los paquetes de firmware de código abierto de los fabricantes. Esto permitió a los delincuentes abusar de los certificados.

- El error fue detectado por bartvbl, quien informó al reportero del problema. Había comprado una empresa D. Cámara de seguridad MODEL-XXXXX y quería descargar el firmware. La empresa D publica el código fuente de numerosos firmwares bajo licencia GPL. "Tras revisar los archivos, resultó que contenían las claves privadas que se usan para firmar el código", informó bartbvl. "La cosa se pone peor: algunos archivos por lotes contenían los comandos y las contraseñas necesarias para firmar el software".

El usuario pudo confirmar que la clave podía usarse firmando un archivo que no era de la Compañía D. El certificado expiró a principios de septiembre, lo que significa que el truco ya no funciona. Incluso después de la fecha de expiración, el software firmado seguirá considerándose válido. Windows solo muestra un error de certificado después de que se hayan retirado los certificados. Esta retirada ya se ha producido, por lo que este [error/fallo] no se puede aprovechar.

Eventos de ciberseguridad con fuga de claves

4. 2023/07: Noticias de PCWold Media: 133 controladores de Windows con licencia válida de Microsoft

   Se encontraron firmas repletas de malware

   • https://www.pcworld.com/article/1991875/caution-malware-in-133-windows-drivers-this-is-cómo reacciona Microsoft.html

   Los controladores habrían provenido de diferentes socios de Microsoft, y las cuentas descubiertas han sido suspendidas.

   Los certificados de desarrollador utilizados para firmar los controladores infectados con malware fueron aparentemente robados a los fabricantes de software y vendidos por internet.

5. El inquietante ataque a la cadena de suministro que corrompió a CCleaner

   • https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

   • Recientemente, 2,27 millones de computadoras que ejecutaban Windows se infectaron con malware firmado con un certificado robado de los creadores de una aplicación popular llamada CCleaner e insertado en su mecanismo de actualización de software.

      • https://blog.trailofbits.com/2017/10/10/tracking-a-stolen-code-signing-certificate-with-osquery/

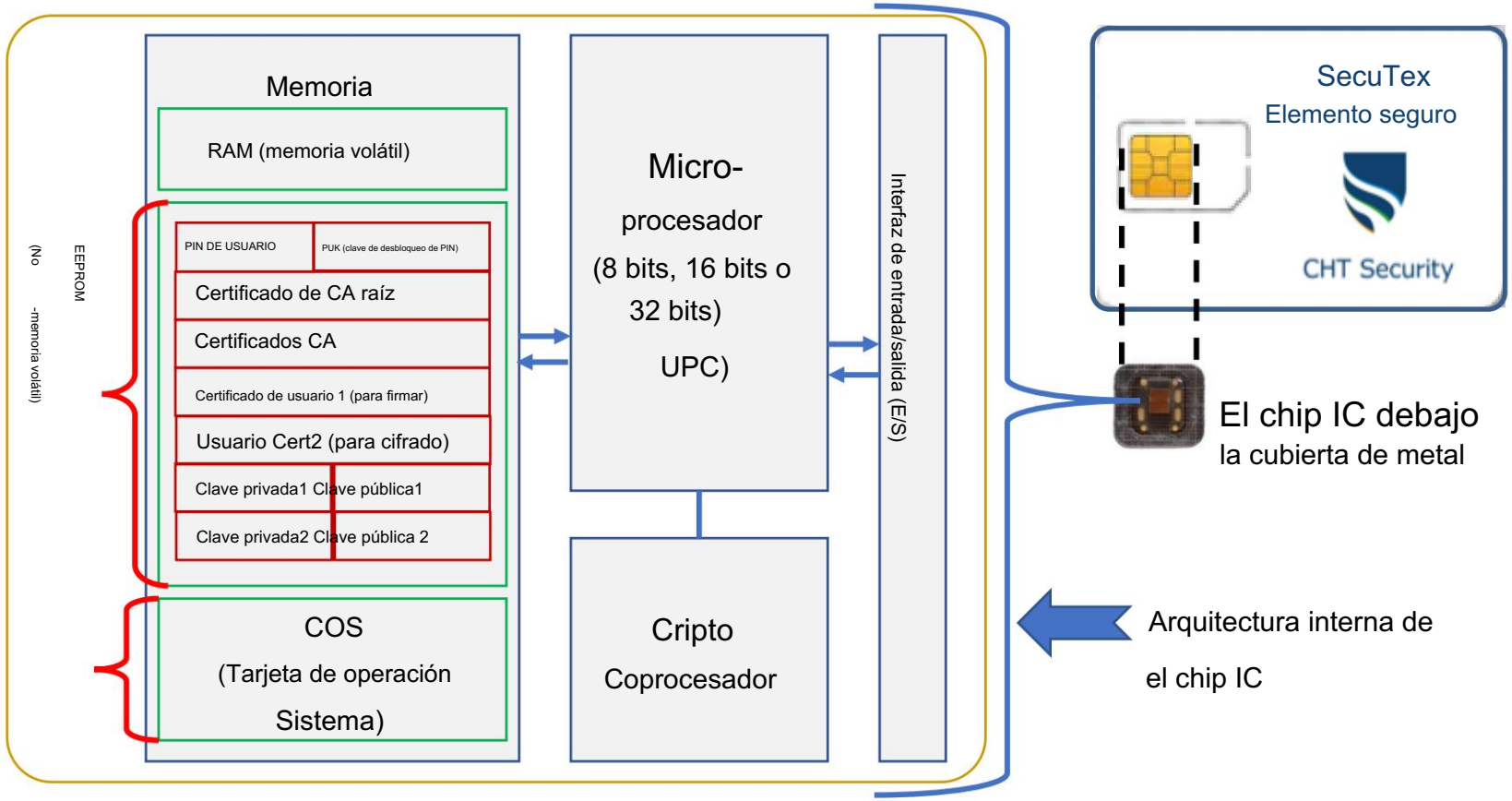
Eventos de ciberseguridad con fuga de claves

6. 2023/10: Una filtración de LastPass está vinculada al robo de 4,4 millones de dólares en criptomonedas.
   - https://www.bleepingcomputer.com/news/security/lastpass-breach-linked-to-theft-of-44-million-en criptografía/
   - Los piratas informáticos robaron 4,4 millones de dólares en criptomonedas el 25 de octubre utilizando claves privadas y frases de contraseña almacenadas en bases de datos robadas de LastPass, según una investigación realizada por investigadores de fraude criptográfico que han estado investigando incidentes similares.

7. 01/02/2018: Coincheck: $534 millones en NEM robados fueron almacenados en un lugar de baja seguridad. Billetera
   - https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-billetera caliente
   - Según representantes del exchange, los hackers lograron robar la clave privada para la billetera caliente donde se almacenaban las monedas NEM, lo que les permitió drenar los fondos.

Protección de claves basada en hardware

El Hardware Secure Element (SE) es en sí mismo una computadora súper pequeña.



Nota: El chip IC es en realidad una microcomputadora con CPU (microprocesador), RAM, ROM, EEPROM y su propio sistema operativo (Sistema Operativo de Tarjeta, COS). Normalmente, para acelerar el procesamiento criptográfico, si se utiliza en un criptosistema, el chip IC incorpora un coprocesador criptográfico .

¿Por qué Secure Element (SE)?

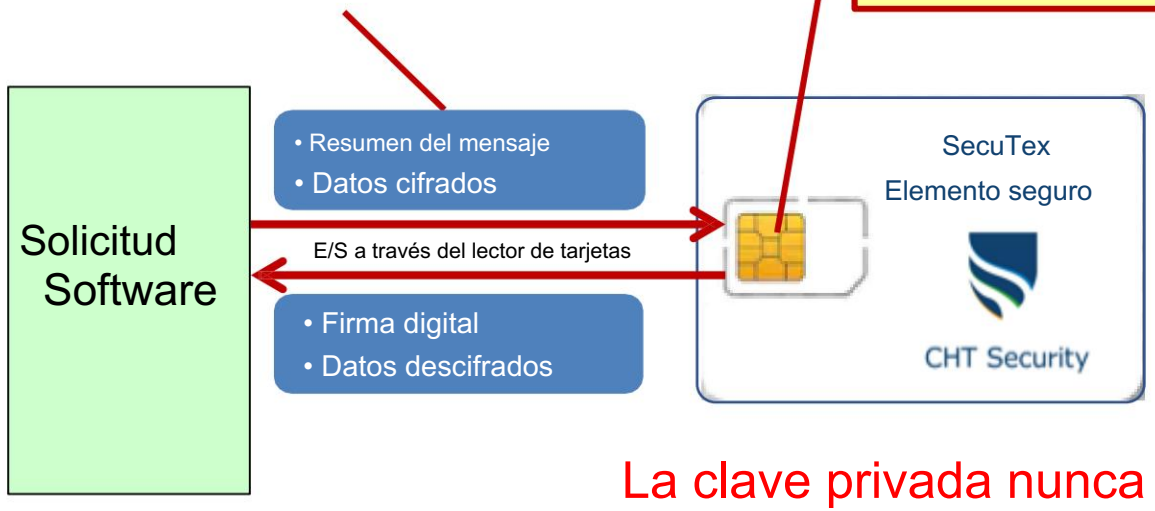
El Hardware Secure Element (SE) es en sí mismo una computadora súper pequeña.

Computación criptográfica en chip

- Cuando la computadora necesita generar una firma digital o descifrar un sobre digital, los datos (resumen del mensaje o La clave secreta se enviará al chip para el cálculo criptográfico con la clave privada.

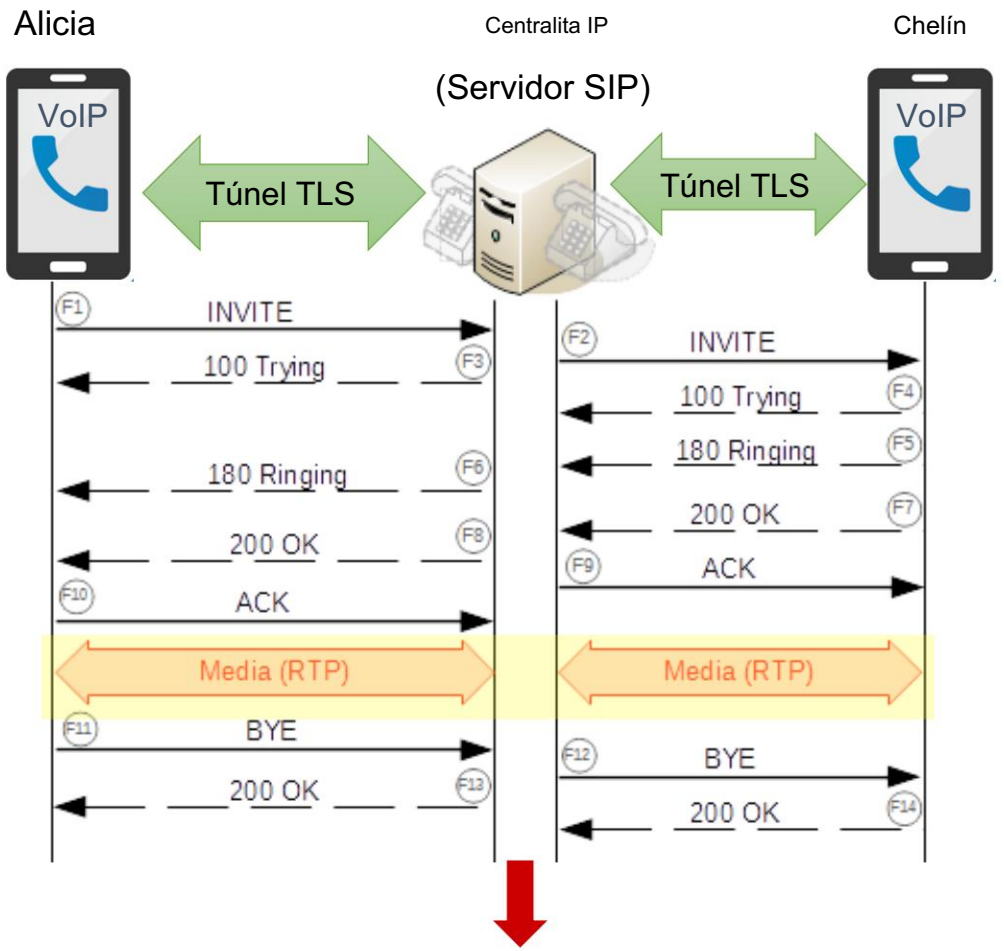
Generación de claves en chip

- El par de claves pública-privada del usuario se generó dentro del chip
- La clave privada del par de claves no se puede leer ni exportar desde el chip y esto lo exige COS.



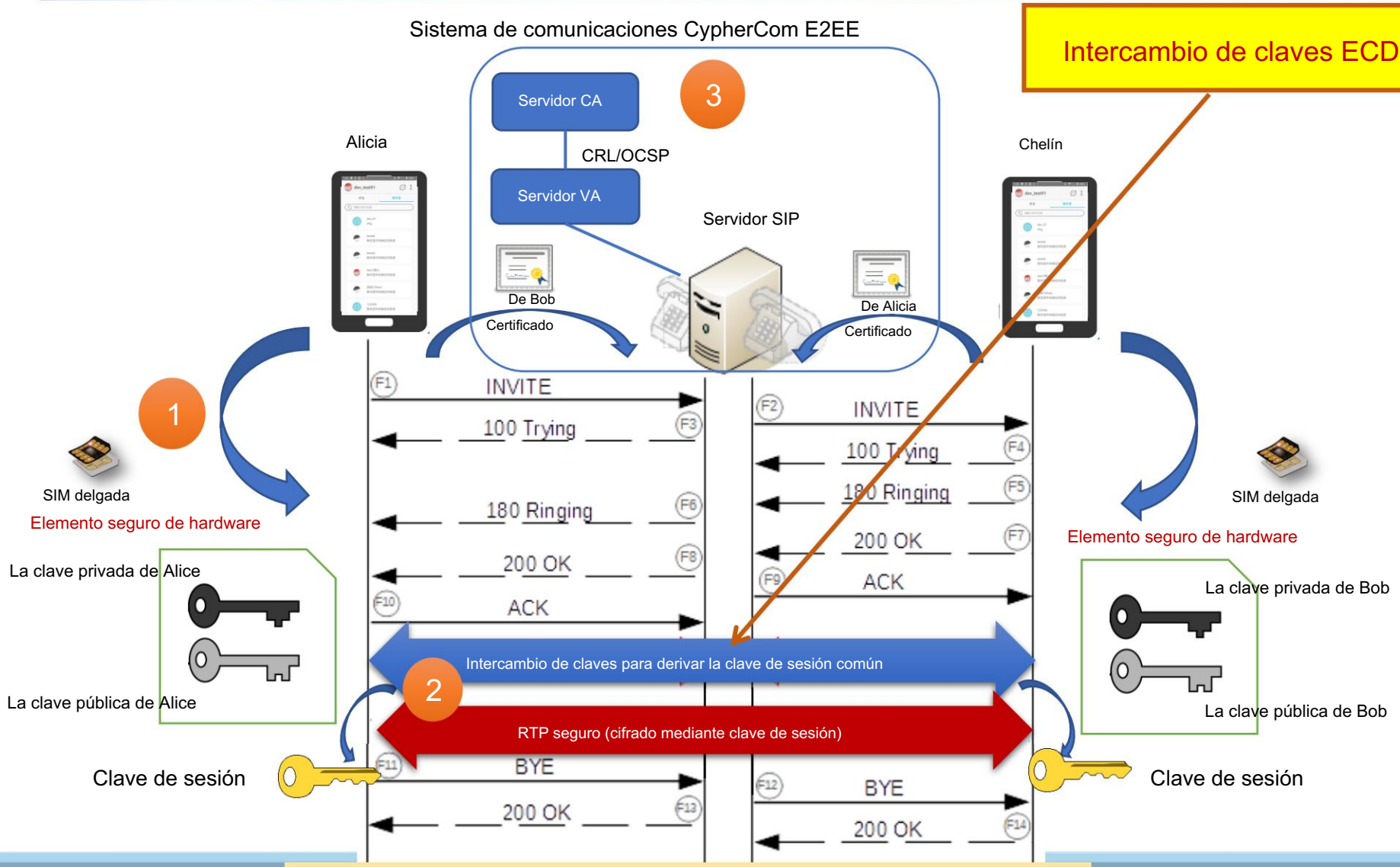
La clave privada nunca estará expuesta a un entorno informático inseguro.

VoIP tradicional (sin cifrado de extremo a extremo)



Los datos de voz podrían ser interceptados y espiados.

Intercambio de claves de extremo a extremo con elemento seguro de hardware



1. Cuando el usuario realiza la llamada a través de la aplicación CypherCom, la cuenta de usuario puede iniciar sesión después de la verificación de la clave privada en el elemento seguro a nivel de hardware .

2. Los usuarios pueden comunicarse con otros una vez que hayan iniciado sesión. La clave de sesión se generará en el proceso de intercambio de claves y la comunicación se puede descifrar solo entre los dos usuarios.

3. El sistema CA verificará si el Los certificados de ambos usuarios son válidos o no. Una vez suspendido o revocado el certificado , los usuarios no pueden realizar la llamada.

Los hackers en el medio no pueden espiar en absoluto

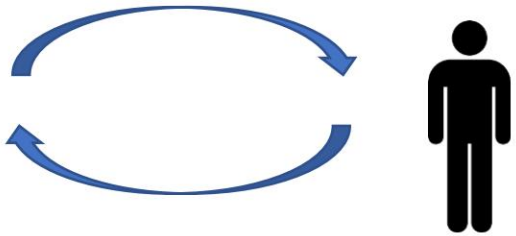
Gestión de identidad y gestión de claves para suscriptores

Sistema de comunicaciones CypherCom E2EE

3. Solicitud de Certificado

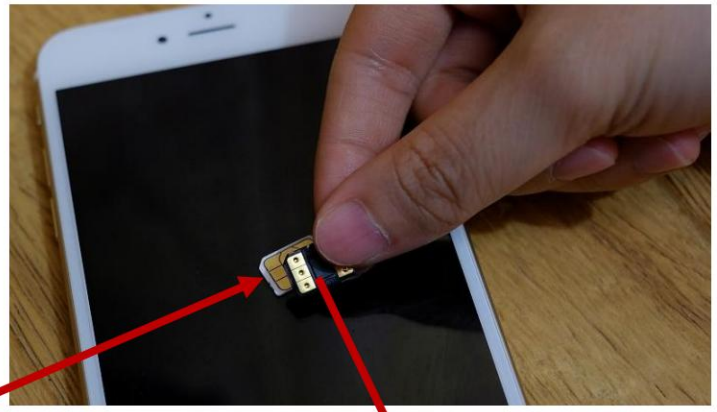
4. Emitir certificado en SIM delgada

5. Enviar Slim SIM al suscriptor

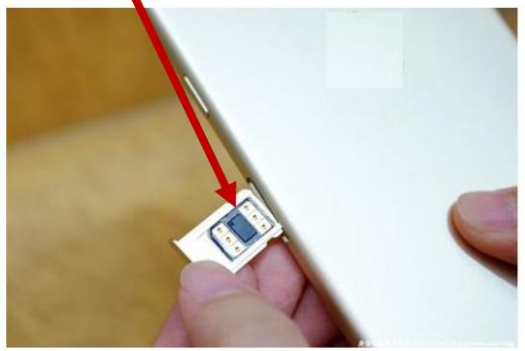


1. Solicita una tarjeta SIM Slim

2. El administrador verifica la identidad



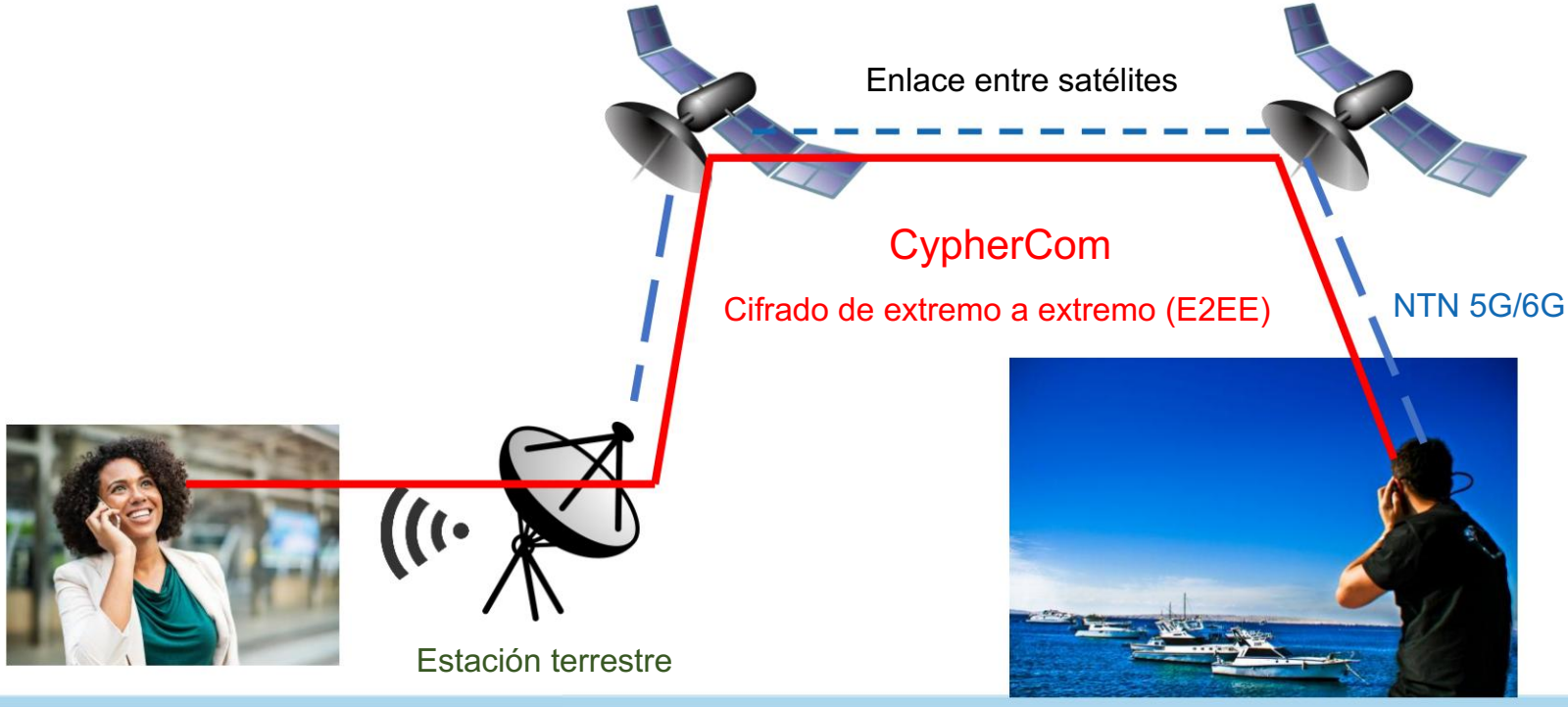
6. El Suscriptor conecta la SIM Slim a su SIM estándar existente.



7.El Suscriptor inserta el combinado SIM en su teléfono inteligente

Resiliencia en las comunicaciones E2EE

- En un entorno de red de bajo ancho de banda, el sistema de comunicaciones digitales debe seguir admitiendo comunicaciones de forma confiable para mantener la resiliencia digital.
- Interconexión de redes a través de satélites: bajo ancho de banda, alta latencia, solo Segmentación/Cifrado de enlaces
- CypherCom: ofrece un modo de bajo ancho de banda con alta calidad pero una tasa de bits muy baja Códecs y compresión de paquetes para soportar comunicaciones E2EE a través de satélites.



Conclusiones clave

1. El cifrado de extremo a extremo (E2EE) es esencial para evitar escuchas clandestinas.
2. La gestión de la identidad es fundamental para garantizar la seguridad de las comunicaciones.
3. Existen riesgos de fuga de claves si no se utiliza protección de claves basada en software. adoptado.
4. Utilice elementos de seguridad de hardware para proteger sus claves siempre que posible.
5. Tenga en cuenta la resiliencia al elegir su sistema de comunicaciones.

¡Gracias!

中華資安國際
CHT Security

www.chtsecurity.com

Potencie su seguridad