Libro Blanco de Seguridad de PlugOS

Versión: V1.1

Descargo de responsabilidad

El contenido de este documento se actualizara periodicamente, Este documento tiene unicamente finesorientativos, y todas las declaraciones, información y sugerencias aqui contenidas no constituyen garantiaalguna, ya sea explicita o implicita.

Contenido

1. Prólogo

1.1. Resumen

A medida que los incidentes de seguridad de los datos se vuelven más frecuentes y la concienciación global sobre la privacidad sigue aumentando, la seguridad de los dispositivos móviles y de informática personal se ha convertido en una cuestión central en la sociedad de la información. Los usuarios no solo están preocupados por el robo de datos por parte de piratas informáticos y aplicaciones maliciosas, sino que también les inquieta la exposición de su privacidad en situaciones como registros forzados o la pérdida del dispositivo. Los dispositivos móviles tradicionales, que a menudo se rigen por objetivos comerciales y funcionales, tienen dificultades para garantizar la soberanía de los datos de los usuarios.

PlugOS es un sistema operativo seguro y privado que se ejecuta en hardware portátil independiente. Con una filosofía de diseño basada en la privacidad como prioridad, el modelo «zero-trust»y la minimización del ámbito de confianza, ha creado una arquitectura de defensa multicapa que abarca el hardware, el núcleo, el sistema y las aplicaciones. Este informe técnico describe las certificaciones de PlugOS, su modelo de amenazas de seguridad, su arquitectura de seguridad y privacidad, y su gestión de la seguridad. Ofrece a los expertos técnicos, responsables de seguridad, responsables de la toma de decisiones y a todos los usuarios preocupados por los derechos digitales una perspectiva transparente, verificable y auditable. Su objetivo es responder a la pregunta más importante: por quéPlugOS es digno de la confianza razonable de los usuarios.

1.2. Introducción

1.2.1 Antecedentes: retos de privacidad y seguridad

En nuestra era digital altamente conectada, los datos personales han pasado de ser un simple soporte de información a convertirse en un activo fundamental que impulsa las decisiones empresariales y la innovación tecnológica. Desde registros de consumo diario y rastros de ubicación hasta datos biométricos y de cuentas financieras, contienen los intereses fundamentales de los usuarios. Los sistemas operativos convencionales suelen tener una tendencia a dar prioridad a los datos. En busca de valor comercial, a menudo habilitan de forma predeterminada la recopilación multidimensional de datos.

Los sistemas operativos convencionales utilizan los permisos del sistema para obtener información como la duración del uso de las aplicaciones y los detalles del hardware, e incluso fusionan datos fragmentados en perfiles de usuario para publicidad dirigida, recomendaciones de productos o el intercambio con terceros sin el consentimiento explícito del usuario. Este modelo de recopilación pasiva difumina los límites de la privacidad y conduce a un flujo de datos fuera de control. Algunos datos pueden llegar a instituciones no autorizadas. Los usuarios desconocen el

uso que se hace de sus datos y tienen dificultades para revocar su consentimiento, lo que debilita gravemente su autonomía en materia de privacidad.

Al mismo tiempo, la soberanía de los datos de los usuarios se enfrenta a amenazas en múltiples escenarios, altamente encubiertas y destructivas. A nivel de red, los ataques a dispositivos móviles se han sofisticado. Los hackers utilizan actualizaciones de sistema falsas, aprovechan vulnerabilidades para implantar código malicioso y recurren al phishing para engañar a los usuarios y que revelen información confidencial. En 2024, los incidentes de phishing móvil a nivel mundial aumentaron un 37 % interanual; casi el 60 % de ellos tenían como objetivo datos de alto valor, como datos financieros y médicos. A nivel físico, el robo de dispositivos y los ataques dirigidos son habituales. Los delincuentes desmontan el hardware para extraer datos sin cifrar, y las vulnerabilidades de la cadena de suministro pueden dar lugar a que los dispositivos sean monitorizados desde la fábrica; más de decenas de millones de dispositivos se ven afectados.

Además, los ataques de coacción y de ingeniería social suponen una amenaza invisible. Los usuarios pueden verse obligados a facilitar contraseñas o información biométrica, mientras que la ingeniería social aprovecha las debilidades psicológicas para burlar las defensas. Estas amenazas entrelazadas provocan filtraciones de datos, pérdidas económicas e incluso el robo de identidad y el daño a la reputación, lo que pone de relieve la urgente necesidad de un sistema altamente seguro y que proteja la privacidad.

1.2.2 PlugOS: Redefiniendo la soberanía de los datos

PlugOS se creó para hacer frente a los retos mencionados. PlugOS reconstruye un sistema operativo basado en la seguridad y la privacidad partiendo de los principios fundamentales, en lugar de ser un mosaico de funciones de seguridad incrementales superpuestas a los sistemas existentes. Encapsula un entorno de ejecución inteligente completo, aplicaciones básicas y datos de usuario dentro de un hardware portátil independiente. Al aprovechar canales cifrados, PlugOS interactúa con los dispositivos anfitriones (teléfonos inteligentes, tabletas o PC) para operaciones de E/S (visualización, entrada y redes), y crea un entorno de ejecución de confianza verificable, controlable y físicamente aislado. PlugOS se libera de la inercia de recopilación de datos de los sistemas operativos convencionales. A través de una estrategia de defensa en profundidad que abarca el hardware → el núcleo → el sistema → las aplicaciones, PlugOS integra medidas de protección de la privacidad en cada etapa. Este enfoque no solo mitiga las amenazas externas, sino que también refuerza el derecho de los usuarios a conocer, controlar y eliminar sus datos personales. PlugOS aspira a ser un guardián de la soberanía del usuario en lugar de un conducto para la monetización de datos.

1.2.3 Objetivo y público destinatario

Este informe técnico tiene como objetivo proporcionar una explicación técnica detallada para expertos en tecnología, responsables de seguridad, responsables políticos y usuarios individuales

que dan prioridad a la seguridad y la privacidad. Demostrará de forma transparente la arquitectura y los mecanismos de PlugOS, y explicará en detalle cómo aborda diversos retos de seguridad en el mundo digital moderno. Dado que este documento profundiza en campos profesionales como la seguridad de sistemas, la criptografía y la seguridad del hardware, se da por supuesto que el lector tiene conocimientos básicos sobre seguridad de la información.

1.3. Términos y definiciones

Los siguientes términos y definiciones se aplican al presente documento.

Término	Abreviatura	Definición
Dispositivo host	Anfitrión	El dispositivo (teléfono inteligente, tableta u ordenador) queproporciona alimentación y periféricos (por ejemplo, pantalla,teclado, pantalla táctil, red) tras la inserción de PlugOS.
Aplicaciónhost / Aplicación complementaria	Aplicación del dispositivo host	La aplicación oficial instalada en el dispositivo host. Sirvecomo puente central para la interacción entre PlugOS y eldispositivo host. Sus funciones principales incluyen: ser elprincipal responsable de reenviar las capacidades de losperiféricos, la transmisión cifrada de la salida de PlugOS y lasupervisión y gestión del estado.
Clave de producto	Clave de producto	Un número de serie único y una credencial criptográfica quese graban en cada PlugOS en el momento de su fabricación, yque se utilizan para la activación del dispositivo yelemparejamiento seguro con el host.
Enlace seguro	Enlace seguro	Proceso de autenticación mutua durante el emparejamientoinicial de PlugOS yun host. Utiliza la verificación decontraseña y tokens dinámicos para vincular de forma seguraPlugOS a un host especifico, impidiendo el acceso noautorizado al host.
Entorno de ejecución confiable	TEE	Area segura creada en una plataforma informática medianteaislamiento de hardware para garantizar la confidencialidad eintegridad del código y los datos. Un TEE se utiliza pararealizar tareas sensibles en un entorno aislado, como laautenticación de privacidad y la protección de datos.
Elemento seguro	SE	Microprocesador dedicado, físicamente independiente y altamente resistente a la manipulación, diseñado para almacenar y procesar información confidencial del más alto nivel, como claves criptográficas.

Raíz de confianza de hardware	HRoT	Una base de confianza establecida durante el proceso de fabricación del hardware que no puede ser modificada por el software. Es el punto de partida para el arranque seguro y las operaciones criptográficas de todo el sistema.
Arquitectura Zero Trust	Arquitectura Zero Trust	Modelo de seguridad cuyo principio fundamental es «nuncaconfíes, siempre verifica». Autentifica y autoriza de formaestricta cualquier solicitud de acceso a los recursos y, pordefecto, no confía en el host ni en su aplicación.
Superficie de ataque	Superficie de ataque	La suma de todos los posibles puntos de entrada en un sistema que un atacante puede explotar. Una superficie de ataque más pequeña suele significar un sistema más seguro.
Cifrado de extremo a extremo	E2EE	Esquema de cifrado de comunicaciones que garantiza que los datos permanezcan cifrados durante todo su recorrido desde el remitente hasta el destinatario, y que solo puedan ser descifrados por las partes que se comunican.
Huella digital del dispositivo	Huella digital del dispositivo	Una huella digital del dispositivo que identifica de forma única a un dispositivo mediante la recopilación de múltiples características de software y hardware del mismo, y que se utiliza a menudo para rastrear a los usuarios.
Sensor Virtualización	Sensor Virtualización	Una técnica que intercepta el acceso de una aplicación a sensores de hardware a nivel del sistema y proporciona datos virtuales controlados por el usuario para contrarrestar la identificación de dispositivos.
Contraseña de coacción / Código de Coacción	Contraseña de emergencia / Código de coacción	Mecanismo de seguridad para hacer frente a situaciones de coacción física. Al introducir esta contraseña, se destruyen los datos o se accede a un «sistema señuelo» sin datos reales.
Autodestrucción de datos	Autodestrucción de datos	Mecanismo mediante el cual el sistema elimina automáticamente todos los datos confidenciales (por ejemplo, archivos de usuario, claves, datos de aplicaciones) cuando se cumplen unas condiciones predefinidas (por ejemplo, activación por parte del usuario, detección de un ataque malicioso, situación de coacción). La eliminación es permanente y no se puede recuperar por medios técnicos. En condiciones de autodestrucción del hardware, el dispositivo puede quedar inutilizable.

Ataque a la cadena de suministro	Ataque a la cadena de suministro	En lugar de atacar directamente a los usuarios finales, los atacantes aprovechan las vulnerabilidades de la cadena de suministro del producto (diseño, producción, distribución) para implantar código malicioso.
Nivel de garantía de evaluación de los Criterios Comunes	CC EAL	Una norma reconocida a nivel mundial para la evaluación de la seguridad de los productos de TI. Un nivel EAL más alto representa un mayor grado de garantía de seguridad para el producto.
Minimización de datos	Minimización de datos	Uno de los principios fundamentales de la protección de la privacidad, que exige que los sistemas y las organizaciones recopilen y utilicen solo la cantidad mínima de información personal necesaria para alcanzar un objetivo empresarial.

2. Responsabilidades de seguridad compartidas

Para hacer frente a los retos cada vez más graves en materia de privacidad y seguridad, PlugOS y sus usuarios deben definir claramente sus respectivas responsabilidades de seguridad. Ambas partes pueden salvaguardar conjuntamente la soberanía de los datos y la seguridad de la privacidad mediante el establecimiento de un sistema de seguridad colaborativo que combine garantías técnicas con protocolos de usuario.

2.1. Responsabilidades de seguridad de PlugOS

PlugOS asume responsabilidades técnicas y de cumplimiento de seguridad fundamentales en su diseño y funcionamiento para garantizar que el propio sistema sea una «base segura» de confianza. Esto incluye:

- **Seguridad de la arquitectura técnica:**

  Aislamiento físico y lógico: PlugOS es independiente del sistema host y cuenta con sus propias capacidades de procesamiento y almacenamiento para evitar la confusión de datos con el host.

  Protección a nivel de hardware: implementa la ejecución y la protección de claves a través de componentes de confianza como TEE y SE; admite cifrado robusto y verificación de hash para garantizar la confidencialidad y la integridad.

  Resistencia a los ataques coercitivos: Mecanismos integrados para la eliminación de ataques de fuerza bruta y la autodestrucción de la contraseña bajo coacción, con el fin de evitar la fuga de datos causada por el robo físico o la coacción.

- **Protección de datos y privacidad:**
  Recopilación mínima de datos por defecto, sin anuncios, sin notificaciones push y sin escucha.
  Los datos se almacenan y procesan localmente para evitar riesgos de cargas invisibles y transferencias transfronterizas de datos.

- **Operaciones seguras y cumplimiento normativo**
  Establece un mecanismo de supervisión y respuesta ante vulnerabilidades, e implementa actualizaciones periódicas y parches de corrección.
  Promueve un programa de recompensas por errores para mejorar la seguridad con la comunidad y los socios.
  Garantiza que el sistema cumpla con las normas de seguridad internacionales y nacionales (por ejemplo, el RGPD, la PIPL y la norma ISO/IEC 27001).

- **Asistencia al usuario y respuesta ante emergencias:**
  Proporciona asistencia técnica en materia de seguridad y orientación.
  Ayuda rápidamente a aislar los riesgos y a restablecer un estado seguro cuando un usuario se enfrenta a una emergencia (por ejemplo, pérdida del dispositivo, sospecha de intrusión).

2.2. Responsabilidades de seguridad de los usuarios

Como usuarios finales de PlugOS, los usuarios desempeñan un papel crucial en la gestión y el uso de los dispositivos. La concienciación sobre la seguridad y el uso adecuado por parte de los usuarios son fundamentales para maximizar la eficacia de la seguridad. Las responsabilidades fundamentales de los usuarios en materia de seguridad incluyen:

- **Gestión adecuada de las credenciales de cuentas y dispositivos:** Guarde de forma segura las contraseñas de desbloqueo de dispositivos, las claves de producto y otras credenciales críticas. No revele la información de la cuenta a terceros. Se recomienda utilizar contraseñas seguras para reforzar la seguridad de la cuenta.
- **Concesión prudente de permisos y autorización de aplicaciones:** Configure los permisos del sistema en función de las necesidades reales y no autorice de forma aleatoria a aplicaciones de terceros a acceder datos sensibles (por ejemplo, ubicación, contactos); hacerlo reduce los riesgos potenciales de ataques de ingeniería social desde el origen.
- **Concienciación sobre el entorno y disciplina operativa:** Al manejar información sensible con PlugOS, debe estar muy atento al entorno físico y buscar dispositivos de vigilancia ocultos (por ejemplo, cámaras, dispositivos de grabación). Evite realizar operaciones

sensibles en zonas públicas complejas o fácilmente espiables (por ejemplo, oficinas diáfanas, transporte público).

- **Garantizar la seguridad física del dispositivo:** Aunque PlugOS cuenta con protección contra manipulaciones a nivel de hardware, los usuarios deben custodiar adecuadamente el dispositivo para evitar su pérdida y que los atacantes obtengan información de forma indirecta a través del dispositivo físico o de operaciones inducid.
- **Mantener el sistema actualizado y responder con prontitud:** Preste atención a las y las notificaciones de actualización de PlugOS, y asegúrese de que el dispositivo siempre ejecute la última versión segura mediante actualizaciones oportunas. En caso de anomalías como la pérdida del dispositivo o sospechas de violaciones de datos, puede ponerse en contacto con el equipo técnico de PlugOS de inmediato para iniciar el proceso de respuesta de emergencia y minimizar el riesgo.

3. Certificaciones de seguridad y cumplimiento normativo

PlugOS no se basa únicamente en declaraciones propias, sino que establece un estándar de seguridad verificable a través de una triple garantía: **«certificaciones internacionales de prestigio, cumplimiento de la normativa mundial y participación en los estándares del sector».** Nos regimos por una filosofía de «verificación externa independiente + mejora interna continua» para garantizar la fiabilidad a largo plazo de PlugOS a nivel mundial. En esta sección se presentan las certificaciones que hemos obtenido, las leyes y normativas que cumplimos, así como nuestras contribuciones a los estándares del sector.

3.1. Certificaciones internacionales de sistemas

Nos adherimos estrictamente a los estándares internacionales de autoridad en el establecimiento de nuestros sistemas de I+D y gestión. Se integran rigurosas consideraciones de seguridad en cada paso, desde el análisis de requisitos y el diseño de la arquitectura hasta el desarrollo y las pruebas. Hemos obtenido múltiples certificaciones de terceros de prestigio, entre las que se incluyen: ISO/IEC 9001:2015, ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 29151:2017 y CMMI Nivel 3. Contamos con capacidades maduras, estandarizadas y sostenibles en materia de seguridad de la información, protección de la privacidad y gestión de la ingeniería de software, lo que sienta una base sólida para el excelente rendimiento de seguridad de PlugOS.

3.1.1 ISO/IEC 9001 (Certificación del Sistema de Gestión de la Calidad)

La norma ISO/IEC 9001 es una norma mundial para sistemas de gestión de la calidad publicada conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Se centra en tres conceptos fundamentales: orientación al usuario, enfoque basado en procesos y mejora continua, y proporciona a las organizaciones un marco sistemático para la gestión de la calidad con el fin de garantizar que los productos y servicios satisfagan de forma coherente las necesidades de los usuarios y los requisitos reglamentarios a lo largo de su ciclo de vida.

La norma ISO/IEC 9001 es la piedra angular de la gestión de la calidad de PlugOS. Al integrar los requisitos de la norma en todo el proceso de I+D, producción, entrega y servicio,PlugOS ha logrado los objetivos de funciones de seguridad estables, una experiencia de producto consistente y una respuesta eficiente a las necesidades de los usuarios. Proporcionamos a los usuarios una solución de sistema operativo segura y de alta calidad.

3.1.2 ISO/IEC 27001 (Certificación del sistema de gestión de la seguridad de la información

La norma del Sistema de Gestión de la Seguridad de la Información (ISO/IEC 27001) ha sido desarrollada conjuntamente por la ISO y la IEC, y constituye una referencia reconocida a nivel mundial en el ámbito de la gestión de la seguridad de la información. Desempeña un papel insustituible en la protección de los recursos de información y en la promoción del desarrollo saludable de las tecnologías de la información. Permite proteger eficazmente los recursos de información y garantizar un proceso de tecnologías de la información saludable, ordenado y sostenible.

La norma ISO/IEC 27001 especifica diversos requisitos y mejores prácticas para la gestión de la seguridad de la información; nosotros cumplimos con el marco de seguridad para la gestión de I+D de PlugOS. Garantiza que todos los eslabones cumplan con la seguridad de la información y ayuda a la organización a cumplir los requisitos de cumplimiento de la seguridad de la información para evitar riesgos legales y daños a la reputación derivados del incumplimiento.

3.1.3 ISO/IEC 27701 (Privacidad Gestión Gestión)

La norma ISO/IEC 27701 es una norma internacional desarrollada conjuntamente por la ISO y la IEC. Se trata de una extensión de la norma ISO/IEC 27001 sobre sistemas de gestión de la seguridad de la información. Se centra en la gestión de la información sobre privacidad. Proporciona un marco sistemático y operativo para que las organizaciones protejan la información personal, y sus requisitos están estrechamente alineados con las principales normativas de

privacidad a nivel mundial (la PIPL de China, el RGPD de la UE, la CCPA/CPRA de EE. UU., la LGPD de Brasil, etc.).
Hemos utilizado la norma ISO/IEC 27701 para revisar todo el proceso de gestión del ciclo de vida de la información personal de PlugOS, establecer un mecanismo estandarizado de control de riesgos de privacidad, eliminar los puntos ciegos de la gestión y optimizar continuamente.

3.1.4 ISO/IEC 29151 (Código de prácticas para la Protección de la información de identificación personal)

La norma ISO/IEC 29151 es una norma internacional publicada conjuntamente por la ISO y la IEC relativa a la protección de la información de identificación personal. Se centra en el código de conducta que deben seguir los responsables del tratamiento de datos personales al manejar dicha información. El objetivo es mejorar la protección de la información de identificación personal, salvaguardando así los derechos de privacidad del público. Desempeña un papel significativo en el proceso de digitalización global.
PlugOS aplica estrictamente esta norma y regula la recopilación, el almacenamiento, el tratamiento, el uso y la divulgación de la información personal para proteger los derechos de privacidad de los usuarios.

3.1.5 CMMI Nivel 3 Certificación (Madurez Nivel Nivel 3 de integración)

CMMI (Capability Maturity Model Integration) es un estándar reconocido a nivel mundial para evaluar las capacidades de una organización en materia de gestión de proyectos, desarrollo de ingeniería y gestión de procesos. El nivel 3 de CMMI (nivel gestionado) constituye un hito clave para que una organización pase de una reacción pasiva a un control proactivo. Las organizaciones se estandarizan y pueden ofrecer de forma sistemática resultados de alta calidad basados en el nivel 3.
La I+D y el diseño de PlugOS se rigen por el CMMI. Hemos comparado los requisitos del CMMI en cuanto a procesos estandarizados, ejecución conforme y activos reutilizables. Todo

el ciclo de vida de PlugOS cumple con el Nivel 3, desde el análisis de requisitos y el diseño arquitectónico hasta el desarrollo, las pruebas y el mantenimiento operativo. Esto garantiza la seguridad, la estabilidad y la escalabilidad del producto.

3.2. Certificaciones de seguridad del producto

La seguridad de PlugOS se basa en componentes de hardware que han sido verificados según los estándares más estrictos del sector. Los componentes de hardware han superado el sistema de certificación CC (Criterios Comunes). El CC (Criterios Comunes para la Evaluación de la

Seguridad de la Tecnología de la Información) es el estándar más autorizado y ampliamente utilizado para evaluar la seguridad de productos y sistemas de TI a nivel mundial. Permite el reconocimiento mutuo de los resultados de las evaluaciones de seguridad entre diferentes países y regiones, y ayuda a las empresas y organizaciones a elegir productos seguros como opción más fiable.

3.2.1 Certificación de seguridad del sistema operativo TEE

El sistema operativo TEE integrado en PlugOS, como defensa clave para la seguridad del sistema, ha superado con éxito la certificación de seguridad CC EAL4+. Esto no solo demuestra su capacidad para resistir ataques comunes, sino que también pone de manifiesto su seguridad y fiabilidad en escenarios comerciales a gran escala. Se trata de una garantía fundamental de nuestra solidez técnica y de la experiencia de seguridad del usuario.

Este sistema operativo TEE también ha sido validado mediante la producción en masa de más de mil millones de dispositivos. Esta experiencia de producción a gran escala verifica la fiabilidad técnica del sistema operativo TEE y demuestra su viabilidad y estabilidad en aplicaciones comerciales a gran escala. Tenemos plena confianza en el rendimiento de seguridad de PlugOS.

3.2.2 Certificación de seguridad SE

El componente independiente Secure Element (SE) utilizado en PlugOS crea una barrera de seguridad inquebrantable para los usuarios gracias a sus excepcionales características de seguridad. Este chip ha obtenido la certificación de seguridad CC EAL6+, que representa un nivel alto en el sistema de estándares de seguridad global para diversos escenarios de aplicación.

La certificación CC EAL6+ garantiza que este componente de chip puede funcionar de forma estable en entornos financieros complejos. Tanto si PlugOS se utiliza para transacciones bancarias básicas como para proteger información confidencial, como las contraseñas de pago de los usuarios y los registros de transacciones, ofrece una seguridad fiable, lo que permite a los usuarios disfrutar de los servicios financieros digitales con total tranquilidad.

3.3. Cumplimiento de la legislación y la normativa internacionales

PlugOS aplica los principios de **«privacidad desde el diseño»** y **«minimización de datos»**. No recopilamos, procesamos ni almacenamos ningún dato que permita identificar a los usuarios. Este diseño arquitectónico hace que cumpla de forma inherente con los requisitos fundamentales de las principales normativas mundiales en materia de protección de datos, como la PIPL de China, el RGPD de la UE y la CCPA de EE. UU.

3.3.1 Ley de Protección de la Información Personal de la República Popular China (PIPL)

La PIPL es la primera ley integral promulgada en China para proteger los derechos e intereses de la información personal de los individuos, normalizar las actividades de tratamiento de la información personal y promover el uso razonable de la misma. La ley establece explícitamente que la información personal de las personas físicas está protegida por la ley, y que ninguna organización o individuo puede infringir los derechos e intereses de la información personal de una persona física. Las actividades que impliquen el tratamiento de información personal de personas físicas dentro de China están sujetas a sus restricciones.

El diseño y las características de PlugOS se ajustan plenamente a los requisitos de esta ley. Desde el punto de vista del diseño, PlugOS se adhiere al principio de «privacidad desde el diseño», rechazando firmemente la recopilación de datos y el análisis del comportamiento. El sistema no contiene anuncios, recomendaciones, escucha ni subidas de datos, respetando plenamente el derecho de las personas a controlar su propia información. Esto es totalmente coherente con la disposición de la PIPL que establece que los responsables del tratamiento de datos personales deben seguir los principios de legalidad, corrección y buena fe.

3.3.2 Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (RGPD) es la normativa de protección de datos de mayor influencia de la UE. No solo tiene un profundo impacto en las organizaciones de la UE, sino que también exige a todas las empresas del mundo que participan en el tratamiento de datos personales de la UE que adapten sus estrategias de gestión de datos para garantizar el cumplimiento de la normativa. El RGPD ha establecido un punto de referencia en el ámbito de la protección de datos a nivel mundial y cambia significativamente la forma en que las empresas tratan los datos personales, llevando la protección de estos a un nuevo nivel.

PlugOS cumple plenamente con los estrictos requisitos del RGPD. Nos adherimos a la filosofía de «Privacidad desde el diseño», eliminando la recopilación de datos y el análisis de comportamiento. Sus componentes independientes Secure Element (SE) o Trusted Execution Environment (TEE) proporcionan cifrado a nivel de hardware para el almacenamiento, el arranque seguro y la

resistencia a la manipulación, con el fin de garantizar la seguridad y la confidencialidad de los datos. El mecanismo de autodestrucción puede destruir rápidamente los datos para evitar fugas, protegiendo de forma integral los derechos de los usuarios sobre sus datos.

3.3.3 Ley de Privacidad del Consumidor de California (CCPA)

La Ley de Privacidad del Consumidor de California (CCPA) es una ley estatal de California, EE. UU. Se promulgó para reforzar los derechos de privacidad y la protección del consumidor de sus residentes. Como primera legislación integral sobre privacidad de datos en EE. UU., la CCPA tiene como objetivo dar a los residentes de California un mayor control sobre sus datos personales para construir una sólida barrera legal para la privacidad del consumidor y la seguridad de los datos.

En el marco de la tendencia hacia la protección de la privacidad de los datos, PlugOS cumple estrictamente con los requisitos de la CCPA. En su diseño, elimina la recopilación de datos y el análisis de comportamiento, sin anuncios, sin recomendaciones, sin escucha y sin cargas, respetando plenamente el derecho de los consumidores a controlar su información personal. Esto se ajusta al espíritu fundamental de la CCPA de empoderar a los consumidores. En su implementación funcional, el TEE y el SE desempeñan un papel clave, cumpliendo con los requisitos de la CCPA en materia de confidencialidad de la información. La protección de datos emplea cifrado AES y mecanismos de gestión de claves para garantizar la confidencialidad, y utiliza algoritmos hash para verificar la integridad, cumpliendo así los requisitos de la CCPA en materia de calidad de la información. Además, su compatibilidad con mecanismos de eliminación de ataques de fuerza bruta y de autodestrucción de contraseñas bajo coacción permite la destrucción activa de la información en situaciones de alto riesgo, protegiendo eficazmente los derechos de los consumidores sobre la información y cumpliendo plenamente los requisitos de la CCPA.

3.4. Establecimiento de estándares del sector y contribuciones

Estamos comprometidos con el avance de la mejora de los estándares del sector de la seguridad de la información y hemos participado activamente en el desarrollo de múltiples especificaciones clave de estándares de seguridad. Esto incluye:

- **Norma del sector:** «Requisitos técnicos para eSIM basadas en un entorno de ejecución de confianza (TEE)» (YD/T 6153-2024).
- **Normas del grupo:** «Especificación técnica para unidades centrales de procesamiento de chips de seguridad financiera»(T/BFIA 007—2021) y «Requisitos técnicos de seguridad de la información para en terminales móviles inteligentes»(T/TAF 074—2020).

Al participar en la elaboración de normas, no solo aportamos nuestros conocimientos técnicos al sector, sino que también integramos estos requisitos de alta seguridad en la arquitectura técnica de PlugOS desde el principio, lo que sitúa a nuestro producto en los niveles de seguridad más exigentes del sector.

3.5. Auditorías de seguridad independientes realizadas por terceros y gestión interna del cumplimiento

PlugOS ha establecido un mecanismo de cumplimiento de doble vía: «verificación externa independiente + mejora continua interna».

- **Verificación externa independiente:** contratamos periódicamente a empresas de seguridad externas independientes de primer nivel para que realicen pruebas de penetración exhaustivas y auditorías de seguridad a nivel de código fuente del sistema operativo PlugOS, el diseño de hardware, las implementaciones criptográficas y la aplicación complementaria del host.
- **Ciclo interno de cumplimiento normativo:** Hemos creado un equipo profesional de gestión del cumplimiento normativo que realiza un seguimiento dinámico de los cambios en las normativas y estándares internacionales. Llevamos a cabo una auditoría interna de cumplimiento normativo que abarca todo el proceso al menos cada seis meses para garantizar que la dirección, I+D y los procesos de entrega, mejorando así continuamente la eficacia del programa de cumplimiento de PlugOS.

4. Modelo de amenazas de seguridad y principios de diseño

Un sistema de seguridad sólido comienza con un profundo conocimiento de las amenazas y una filosofía de diseño clara. El modelo de amenazas de seguridad es la base del diseño de seguridad de PlugOS. Al definir «qué proteger», «contra quién defenderse», «cómo delimitar el perímetro de confianza» y «qué no se puede resolver», define claramente el alcance fundamental de la protección de seguridad.

4.1. Activos protegidos fundamentales

PlugOS estádiseñado para proteger los datos y las aplicaciones almacenadas o ejecutadas en PlugOS. Estos activos incluyen, entre otros:

- **Claves y credenciales:** claves criptográficas, tokens de autenticación, diversas contraseñas de cuentas, etc.

- **Datos privados del usuario:** archivos, registros de mensajes, contactos, calendarios, fotos, audio y vídeo, etc.
- **Metadatos y contenido de las comunicaciones:** el comportamiento de las comunicaciones en sí, el contenido de las sesiones, los gráficos de relaciones, etc.
- **Activos financieros y credenciales de identidad:** claves privadas de moneda digital, credenciales de banca en línea, certificados de identidad digital, etc.
- **Rastros de ubicación y comportamiento:** información de ubicación geográfica, registros de uso de aplicaciones, historial de acceso a la red, etc.

4.2. Sujetos defensivos (modelo de atacante)

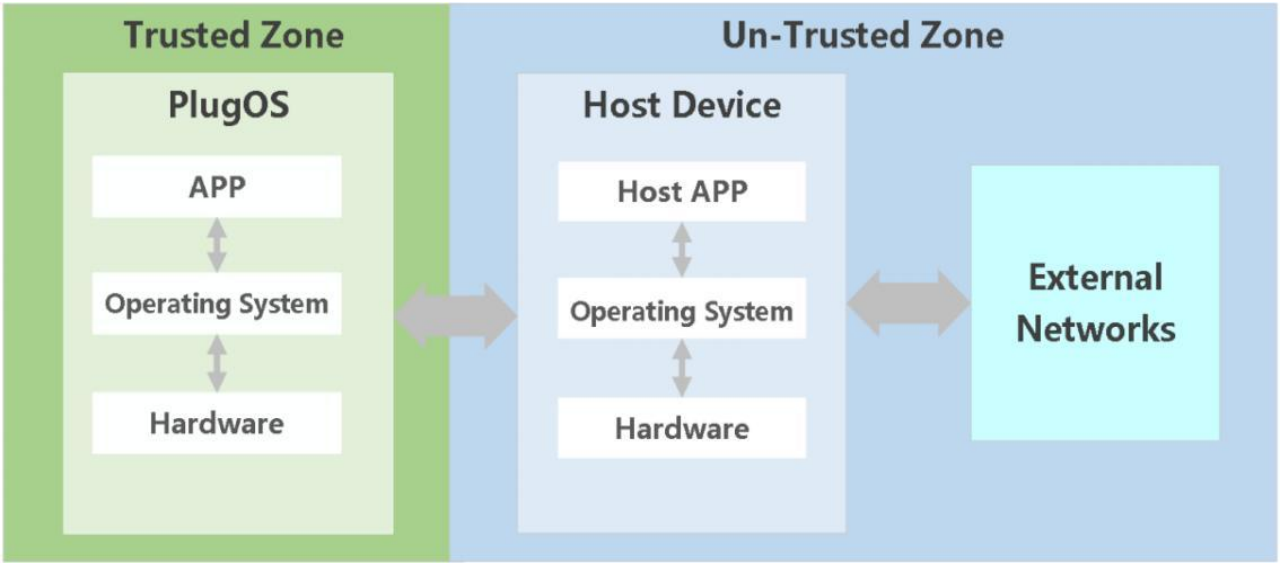
El modelo de defensa de PlugOS abarca tipos de atacantes multidimensionales y con múltiples niveles, entre los que se incluyen, entre otros, los siguientes tipos habituales:

- **Coaccionadores físicos:** personas que intentan obligar a un usuario a desbloquear un dispositivo y entregar sus credenciales bajo coacción o presión física. Por ejemplo, si un usuario es secuestrado, resistirse podría poner en peligro su vida, mientras que ceder significa que el atacante le robarátanto sus activos financieros como su privacidad.
- **Atacantes físicos:** técnicos que, tras la pérdida o el robo de un dispositivo, intentan extraer datos del mismo utilizando medios físicos como ataques de arranque en frío, depuración JTAGo análisis forense de chip-off. Tras el robo de un dispositivo, el atacante intenta extraer datos de PlugOS mediante estos métodos.
- **Atacantes de la cadena de suministro:** personal interno o externo que intenta implantar puertas traseras, firmware malicioso o paquetes de software contaminados durante las fases de producción, transporte, distribución o actualización de software del dispositivo.
- **Intrusos en el host:** atacantes que obtienen el control total del dispositivo host (PC o teléfono) al que está conectado PlugOS e intentan atacar PlugOS mediante malware del lado del host.
- **Proveedores de aplicaciones maliciosas**: atacantes que engañan a los usuarios para que instalen aplicaciones maliciosas en PlugOS, intentando robar datos de otras aplicaciones, realizar operaciones no autorizadas o establecer un canal encubierto.
- **Atacantes de red:** atacantes que intentan espiar o manipular las comunicaciones de red de PlugOS mediante ataques de tipo «hombre en el medio»(MITM), secuestro de DNS, puntos de acceso Wi-Fi maliciosos, etc.

4.3. Límite de confianza (Zero Trust)

«Zero Trust» es la filosofía de seguridad central de PlugOS, lo que significa que, por defecto, no confía en ninguna red, aplicación externa o sistema vecino. El límite de confianza se define de forma explícita y mínima para reducir la superficie de ataque del sistema.

- **Zona de confianza:** el dispositivo de hardware PlugOS, su firmware y el sistema operativo que ha superado la verificación de firmas. Todos los datos y aplicaciones del usuario se ejecutan en esta zona.
- **Zona no confiable:** El sistema operativo del host, la aplicación complementaria del host y todas las redes externas.



Trust Boundary Diagram

Existe un límite de seguridad claro, impuesto por el hardware, entre la zona de confianza y la zona no confiable. Ambas solo interactúan a través de un canal de E/S limitado y cifrado de extremo a extremo. La tabla define las responsabilidades y los permisos de ambas:

Dimensión	Zona de confianza (PlugOS)	Zona no confiable (dispositivo host
Entorno de ejecución	Hardware independiente + TEE/SE + SO seguro.	Sistema operativo abierto del host (p. ej., Android/iOS/Windows).
Ámbito de permisos	Gestiona todas las aplicaciones y datos internos, con capacidades de cifrado y aislamiento a nivel de hardware	Actúa únicamente como un proxy de E/S; no tiene permiso para acceder a ningún dato en texto plano dentro de PlugOS
Almacenamiento de datos	Almacenamiento cifrado por hardware para los datos de los usuarios; los datos circulan en un bucle cerrado interno.	Solo almacena datos de configuración no confidenciales; no se almacenan datos de usuario
Responsabilidad de seguridad	Asume la responsabilidad de la seguridad y la privacidad de los datos de los usuarios durante todo su ciclo de vida, lo que abarca el almacenamiento, el procesamiento y la destrucción.	Solo garantiza la integridad de su propio código y la seguridad de los canales relacionados; no participa en la toma de decisiones fundamentales sobre seguridad.

4.4. Amenazas de seguridad irresolubles

Para mantener la transparencia, debemos señalar claramente los riesgos de seguridad que el modelo de amenazas de PlugOS no puede cubrir directamente. Estos riesgos se derivan principalmente de factores ajenos a la zona de confianza, y su mitigación depende de la concienciación y el comportamiento del usuario en materia de seguridad. Existen dos categorías principales.

4.4.1 Riesgos derivados de errores del usuario

PlugOS estádiseñado para impedir el acceso no autorizado, pero no puede evitar operaciones inseguras realizadas de forma activa o inadvertida por los usuarios. Esto incluye:

- **Ataques de ingeniería social y phishing:** se engaña a los usuarios para que hagan clic en enlaces maliciosos, descarguen archivos adjuntos maliciosos o introduzcan activamente sus credenciales en sitios web falsos.
- **Fuga de credenciales:** los usuarios revelan activamente credenciales de alto privilegio (por ejemplo, contraseñas de desbloqueo o claves de producto) a otras personas, o las almacenan en una ubicación insegura, lo que provoca su filtración.
- **Autorización de aplicaciones maliciosas**: los usuarios instalan activamente una aplicación desconocida en PlugOS y le conceden permisos excesivos.

Mitigación: Aunque PlugOS proporciona protección técnica a través de mecanismos como el principio de privilegios mínimos, el aislamiento de aplicaciones y un cortafuegos de red, la última línea de defensa sigue siendo la concienciación del usuario en materia de seguridad. Recomendamos encarecidamente que los usuarios solo instalen aplicaciones de fuentes de confianza y concedan permisos con prudencia. Para obtener orientación adicional, consulte el capítulo 11, «Lista de verificación de seguridad operable por el usuario».

4.4.2 RiesgosDerivadosde entornos entornos (host y el entorno físico)

El perímetro de seguridad de PlugOS termina en su hardware físico. Puede existir riesgo de fuga de información cuando el entorno físico externo o el entorno del host conectado están completamente controlados por un atacante.

- **Espionaje en el entorno físico**: Los atacantes pueden utilizar cámaras ocultas, mirar por encima del hombro o métodos similares para robar información cuando los usuarios introducen una contraseña o miran la pantalla. Esto va más allá de las capacidades de protección de cualquier dispositivo terminal en sí mismo. Se recomienda que los usuarios garanticen la seguridad de su entorno físico al manejar información confidencial.

- **Hosts totalmente comprometidos:** PlugOS está diseñado para garantizar que, incluso si un host está infectado con malware, este no pueda acceder directamente a los datos estáticos (datos en reposo) ni a los datos en tiempo de ejecución (datos en uso) dentro de PlugOS. Sin embargo, los datos deben pasar por el host no confiable para las operaciones de E/S cuando se muestran (datos en pantalla) y se introducen (datos de entrada). Por lo tanto, un host totalmente controlado por malware a nivel del núcleo (por ejemplo, keyloggers avanzados, herramientas de captura de pantalla de bajo nivel) podría, en teoría, registrar las entradas del teclado de los usuarios y el

Mitigación: Se trata de una elección arquitectónica que equilibra la seguridad, la portabilidad y la rentabilidad. La aplicación complementaria del host de PlugOS incluye capacidades integradas de detección de amenazas en el entorno de ejecución, que pueden contrarrestar eficazmente la mayoría de los ataques de captura de pantalla, grabación e inyección a nivel de aplicación. Sin embargo, frente a los ataques a nivel del núcleo del sistema operativo del host, ninguna protección a nivel de aplicación puede ofrecer una garantía absoluta. Por lo tanto, recomendamos que los usuarios conecten PlugOS a un dispositivo host que sea de su propiedad, que controlen y mantengan en un buen estado de seguridad para minimizar este riesgo.

5. Arquitectura de seguridad

La arquitectura de seguridad de PlugOS se rige por el principio fundamental de la defensa en profundidad. Se basa en una raíz de confianza de hardware a prueba de manipulaciones y construye un entorno informático de confianza totalmente conectado, desde el chip hasta la capa de aplicaciones, mediante mecanismos de seguridad en capas que se complementan entre sí. No solo adoptamos y mejoramos el modelo de seguridad consolidado de AOSP (Android Open-Source Project), sino que también nos esforzamos por contrarrestar amenazas extremas —desde intrusiones físicas y ataques a la cadena de suministro hasta coacción forzada— a través de la innovación arquitectónica, garantizando la confidencialidad y la integridad de los datos de los usuarios.

En esta sección se analizarán uno a uno los mecanismos de seguridad fundamentales de PlugOS, abarcando el hardware físico, los chips, el núcleo del sistema, los datos y los servicios básicos. El objetivo de estos mecanismos es proporcionar una seguridad verificable basada en la arquitectura, en lugar de una seguridad basada en promesas.

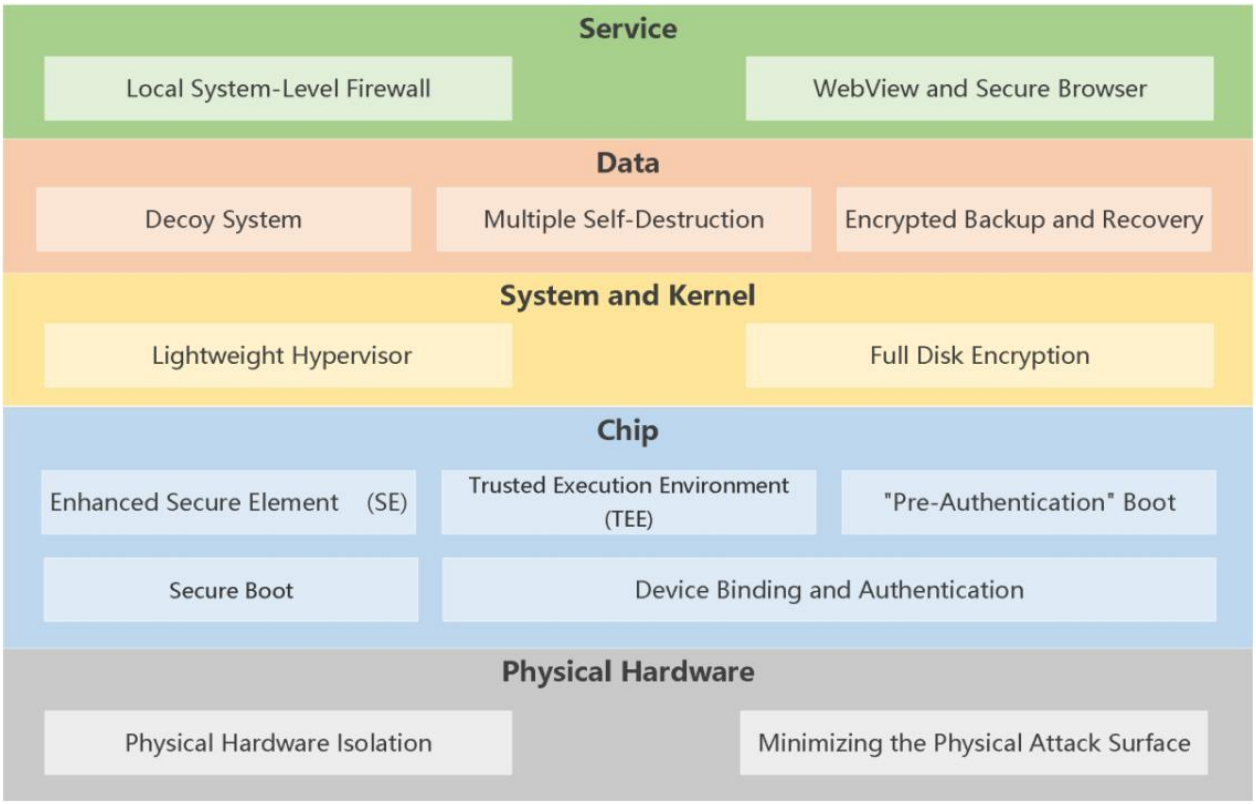


Diagrama de la arquitectura de seguridad de PlugOS

5.1. Físico Hardware Aislamiento y Ataque Minimización de la superficie de ataque

Esta es la primera y más intuitiva línea de defensa contra las amenazas externas.

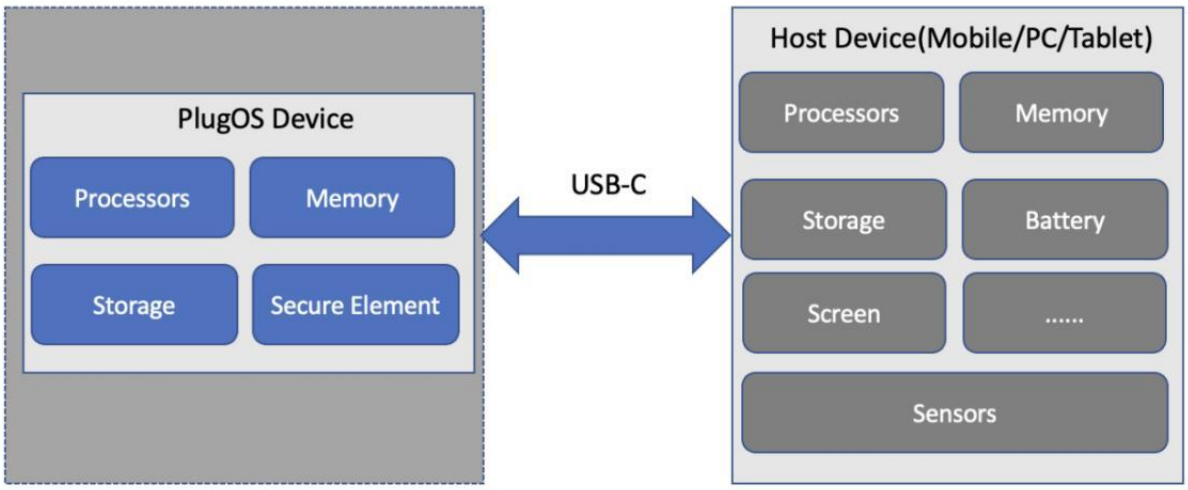


Diagrama de la arquitectura de los componentes de hardware

Aislamiento físico del hardware: PlugOS es una unidad completa e independiente de computación y almacenamiento, equipada con su propio procesador de alto rendimiento, memoria de alta velocidad y almacenamiento de gran capacidad. Está físicamente aislada del sistema host (es decir, el ordenador o el teléfono del usuario). Esto significa que el sistema operativo host no

puede acceder, desde el punto de vista arquitectónico, al espacio de direcciones de memoria o al chip de almacenamiento de PlugOS. Incluso si el sistema anfitrión se viera totalmente comprometido por malware, no podría traspasar este límite físico.

Reducción al mínimo de la superficie de ataque física: El diseño de hardware de PlugOS se rige por un principio minimalista. El dispositivo prescinde de componentes complejos de radiofrecuencia (RF), como bandas base de telefonía móvil, NFC y GPS, así como de sensores innecesarios. Solo interactúa con el exterior a través de una única interfaz USB-C protegida por un sólido protocolo de cifrado. Este diseño reduce significativamente la superficie de ataque física y de software, mitigando desde el origen el riesgo de ataques remotos o de corta distancia.

5.2. Aislamiento de seguridad a nivel de chip

El hardware es el punto de partida de toda seguridad. El modelo de seguridad de PlugOS comienza con una raíz de confianza de hardware (Hardware Root of Trust) reforzada por el hardware y resistente a la manipulación.

5.2.1 Fundamentos del aislamiento de seguridad a nivel de chip

El aislamiento de seguridad de PlugOS se basa en el chip Secure Element (SE) y el entorno de ejecución de confianza (TEE), lo que garantiza que las operaciones críticas no puedan ser manipuladas

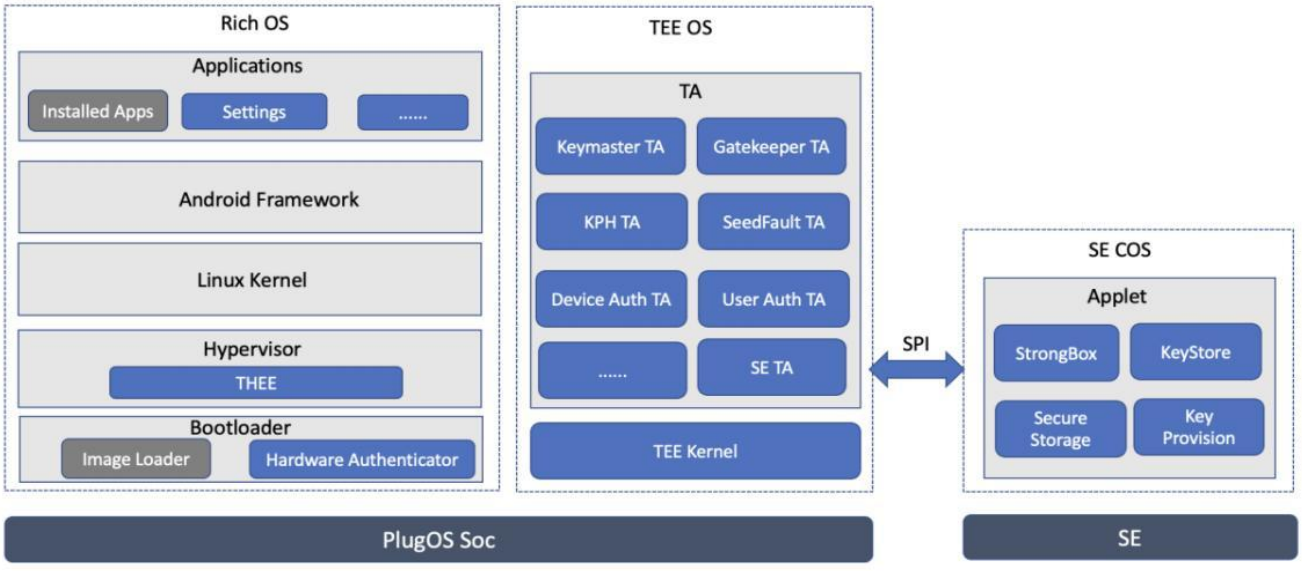


Diagrama de la arquitectura de aislamiento del chip de PlugOS

Elemento seguro (SE) mejorado: algunos modelos de PlugOS incluyen un chip SE independiente integrado con certificación CC EAL6+. El SE es un ordenador seguro y compacto con resistencia física a la manipulación, que proporciona una protección de «nivel de caja fuerte física» para la información confidencial esencial, como las claves criptográficas. CC EAL6+ es una

de las certificaciones de seguridad de chips de más alto nivel disponibles en la actualidad. Al integrar profundamente las capacidades del SE, PlugOS es compatible de forma nativa con la especificación Android StrongBox Keymaster, lo que garantiza que la generación, el almacenamiento y el uso de claves se realicen íntegramente dentro del hardware y sean inaccesibles para cualquier software externo, incluido el sistema operativo. Esto ofrece garantías de seguridad de hardware para las operaciones criptográficas y la gestión de credenciales a la altura de las de un chip de tarjeta bancaria.

Entorno de ejecución de confianza (TEE): Todos los dispositivos PlugOS están equipados con un TEE basado en la tecnología ARM TrustZone. Su núcleo de sistema operativo TEE, proporcionado por el líder del sector TrustKernel, cuenta con Ha superado la certificación de seguridad CC EAL4+ y ha sido validado mediante su producción en masa en más de mil millones de dispositivos. El TEE crea un entorno de ejecución aislado por hardware paralelo al sistema operativo principal, que admite la autenticación de dos factores de PlugOS (usuario y dispositivo), el cifrado y descifrado de datos, la gestión de claves y la gestión del entorno seguro (SE). Esto evita de manera eficaz que las vulnerabilidades del sistema operativo principal afecten a las funciones de seguridad fundamentales

5.2.2 Innovación arquitectónica: proceso de arranque con «autenticación previa»

PlugOS subvierte el modelo tradicional de «autenticación posterior al arranque». Si bien el arranque seguro tradicional puede verificar la integridad de las firmas del sistema, no puede impedir que el firmware con puertas traseras se ejecute antes de la autenticación del usuario. Por ejemplo, muchas herramientas comerciales de craqueo pueden eludir físicamente las medidas de seguridad y extraer datos de usuario de un dispositivo sin autorización, principalmente aprovechando vulnerabilidades en el firmware de bajo nivel del dispositivo. PlugOS aborda este problema a nivel arquitectónico: antes de que se cargue, verifique o ejecute cualquier código del sistema, el dispositivo debe completar una autenticación de dos factores (tanto del usuario como del dispositivo host) a nivel de chip. **Esto frustra los métodos tradicionales de eludir las defensas de autenticación mediante ataques físicos, manipulación de la cadena de suministro o vulnerabilidades del firmware de bajo nivel.** Por ejemplo, incluso si existe una puerta trasera en el firmware del chip o en la capa del núcleo de Linux, el firmware de la cadena de suministro afectado por la puerta trasera nunca se activará ni se ejecutará a menos que se haya completado la autenticación de dos factores (del usuario y del dispositivo) a través del chip de seguridad de hardware.

Arranque seguro: Cada etapa del proceso de arranque del dispositivo se verifica mediante una firma digital, formando una «cadena de confianza» completa. No se cargará ni ejecutará ningún firmware no autorizado o imagen del sistema manipulada, ya que la clave de descifrado del disco

de la que depende no está presente en la memoria hasta que la autenticación se haya completado con éxito.

Vinculación y autenticación de dispositivos: PlugOS solo permite conexiones a dispositivos host autenticados y autorizados. Al utilizarlo con un host por primera vez, el usuario debe vincular el host utilizando la clave de producto del dispositivo PlugOS. Para conexiones posteriores, solo se reconocerán los hosts que hayan sido vinculados y verificados. La autenticación del host se basa en la identificación de las características físicas del hardware del host. Tras la vinculación inicial, PlugOS genera un par de claves de vinculación para el host, que sirve como factor de autenticación para las conexiones posteriores. Esto evita los ataques de intermediario (MITM) y el acceso no autorizado.

5.3. Fortalecimiento de la seguridad a nivel del sistema y del núcleo

Basándose en garantías de hardware, PlugOS establece una sólida defensa de aislamiento de software mediante tecnología de virtualización avanzada y mecanismos de cifrado obligatorios.

Aislamiento del núcleo basado en un hipervisor ligero: en una arquitectura de núcleo monolítica tradicional, una vez que un atacante obtiene privilegios de root, todo el sistema queda totalmente comprometido. PlugOS cuenta con un hipervisor ligero (monitor de máquina virtual) de desarrollo propio que virtualiza y aísla los componentes críticos del núcleo del sistema operativo (por ejemplo, los componentes de gestión de memoria y los de gestión de políticas de seguridad). Crea un dominio de seguridad independiente para cada aplicación con restricciones de política estrictas. Este diseño dificulta que las vulnerabilidades de una sola aplicación o servicio del sistema se propaguen lateralmente, lo que limita el alcance del impacto de la vulnerabilidad en el núcleo u otras aplicaciones y mejora las capacidades de protección contra intrusiones del sistema.

Cifrado completo del disco (cifrado al escribir): PlugOS habilita de forma predeterminada el cifrado completo del disco a nivel de archivo. Cualquier dato escrito en el medio de almacenamiento es cifrado automáticamente por el motor de cifrado de hardware en el momento de la escritura. Cada archivo se cifra con una clave independiente, y estas claves de archivo están protegidas por una clave maestra. Esta clave maestra se almacena de forma segura en el TEE/SE y está fuertemente vinculada a las credenciales de desbloqueo del usuario. Esto significa que, incluso si un atacante obtiene físicamente el chip de memoria flash (por ejemplo, mediante análisis forense chip-off), no podrá leer ninguna información valiosa en texto plano.

5.4. Autodestrucción de datos y recuperación segura

Además de una sólida arquitectura de seguridad tradicional, PlugOS ha introducido de forma innovadora mecanismos de protección de datos para escenarios extremos, como la coacción física y los ataques de fuerza bruta. Esto constituye la última línea de defensa para la seguridad

de los datos de los usuarios, garantizando que estos mantengan un control absoluto sobre sus propios datos.

Para contrarrestar la coacción extrema o el craqueo físico, PlugOS cuenta con múltiples mecanismos de autodestrucción de datos integrados. Estos mecanismos pueden activarse tras varias entradas incorrectas de contraseña consecutivas o cuando un usuario introduce activamente una contraseña de coacción preestablecida en la pantalla de desbloqueo. Una vez activados, el sistema destruye irreversiblemente las claves de cifrado, lo que hace que todos los datos del disco sean irrecuperables al instante. Además, PlugOS ofrece una solución de copia de seguridad y recuperación cifrada de extremo a extremo. Los usuarios pueden realizar copias de seguridad de sus datos de forma segura en una ubicación de almacenamiento de confianza de su elección, manteniendo la clave de cifrado bajo su control. Esto garantiza capacidades autónomas de almacenamiento y recuperación, con la soberanía de los datos en manos del usuario.

5.4.1 Contraseña de coacción

- **Cómo funciona:** Los usuarios pueden configurar una contraseña de emergencia. Cuando se utiliza esta contraseña para desbloquear el dispositivo, PlugOS borraráde forma automática todos los datos internos.
- **Caso de uso:** En una situación en la que los usuarios se vean obligados a desbloquear el dispositivo, pueden utilizar la contraseña de emergencia para proteger su seguridad y sus datos reales, presentando asíun objetivo sin valor para el atacante.

5.4.2 Mecanismo de autodestrucción

- **Condiciones de activación:**

  Antifuerza bruta: El número de intentos consecutivos de contraseña incorrecta alcanza un umbral configurado por el servidor.

  Resistencia a la manipulación física (solo en algunos modelos): Detección de que se ha abierto la carcasa del dispositivo o de que un chip crítico está siendo objeto de un ataque físico.

  Activación mediante contraseña de coacción: Los usuarios pueden configurar una contraseña de coacción para activar la autodestrucción silenciosa.

- **Proceso de ejecución:** Una vez activado, el TEE o SE ejecuta un proceso irreversible de destrucción de claves de cifrado, convirtiendo instantáneamente todos los datos cifrados en un galimatías irrecuperable y logrando así un borrado completo de todos los datos confidenciales.

5.4.3 Copia de seguridad y recuperación cifradas

Las capacidades de copia de seguridad y recuperación cifradas de extremo a extremo que ofrece PlugOS garantizan que todos sus datos permanezcan cifrados durante la copia de seguridad, la transmisión y la recuperación, lo que evita al máximo el acceso no autorizado. Los datos de la copia de seguridad se cifran de extremo a extremo en el dispositivo utilizando una clave conocida solo por el usuario antes de exportarse a una ubicación de almacenamiento seleccionada por el usuario (por ejemplo, un ordenador personal, un dispositivo de almacenamiento externo, etc.). El proceso de recuperación también requiere que el usuario proporcione la clave para completar el descifrado localmente. Como proveedor de servicios, no podemos acceder a ningún contenido en texto plano de la copia de seguridad del usuario durante todo el proceso, lo que garantiza la integridad de la soberanía de los datos del usuario durante la copia de seguridad y la recuperación.

5.5. Mejoras críticas en la seguridad de los servicios

PlugOS ha rediseñado y mejorado en profundidad varios servicios básicos del sistema que están estrechamente relacionados con la privacidad y la seguridad. Por ejemplo:

Cortafuegos local a nivel del sistema: como uno de los componentes fundamentales de seguridad de red de PlugOS, el cortafuegos está profundamente integrado en la pila de red del sistema, lo que le permite aplicar el control de acceso sobre todas las actividades de red de las aplicaciones (incluidas las aplicaciones del sistema). Se ejecuta de forma local, no comparte ni sube ningún registro, y puede identificar y bloquear los rastreadores de aplicaciones integrados y las conexiones de telemetría. Los usuarios pueden definir políticas de acceso a la red muy detalladas basadas en aplicaciones, nombres de dominio, direcciones IP y puertos, logrando así un control total sobre cada conexión.

WebView y navegador seguro: El navegador integrado de PlugOS y los componentes WebView de la aplicación se basan en Chromium e integran parches mejorados de varios proyectos de seguridad líderes. Hemos eliminado todas las dependencias de los servicios de Google y el código de telemetría, desactivado las API web de alto riesgo de forma predeterminada, habilitado políticas estrictas de aislamiento de cookies y protección contra el rastreo, y reforzado el compilador JIT para defenderse contra los ataques basados en la memoria. Esto proporciona a los usuarios un entorno de navegación limpio que no recopila datos, no rastrea la actividad ni causa molestias.

6. Arquitectura de privacidad

A diferencia de la recopilación predeterminada de datos y comportamiento de los sistemas operativos convencionales, con un modelo de exclusión voluntaria opcional, PlugOS se adhiere estrictamente al principio fundamental de «privacidad desde el diseño». No creamos una

plataforma publicitaria más segura; en su lugar, eliminamos arquitectónicamente cualquier forma de recopilación de datos innecesaria. Todos los mecanismos de PlugOS giran en torno a tres objetivos: **la localización de datos, la no análisis del comportamiento y el control total por parte del usuario**, garantizando que cada acción digital que realice un usuario sirva únicamente a sus propias intenciones.

En esta sección se detallan las tecnologías de privacidad fundamentales que PlugOS ha desarrollado para alcanzar estos objetivos.

6.1. Cero recopilación de datos

En los sistemas operativos móviles tradicionales, incluso si los usuarios desactivan la mayoría de las opciones de intercambio de datos, la telemetría en segundo plano a nivel del sistema y el análisis de comportamiento siguen existiendo. Esta recopilación invisible se utiliza a menudo para optimizar servicios o para publicidad dirigida, pero debilita fundamentalmente la soberanía de la privacidad del usuario. La telemetría cero y la localización de datos son los pilares del compromiso de privacidad de PlugOS: no recopilamos tus datos porque nuestro sistema no está diseñado para hacerlo.

- **Telemetría y análisis desactivados por defecto**: PlugOS se basa en AOSP, pero durante el proceso de compilación y personalización, eliminamos o desactivamos sistemáticamente todos los marcos de servicios de Google y los componentes integrados de AOSP de telemetría, informes de fallos y análisis del comportamiento del usuario, desde la capa del sistema hasta las capas del marco y de las aplicaciones principales. En PlugOS, no hay servicios en segundo plano que envíen tus hábitos de uso de las aplicaciones, datos de rendimiento del sistema o preferencias personales al fabricante del dispositivo o al desarrollador de software.
- **Sin anuncios, sin recomendaciones**: dado que no se realizan perfiles de usuario ni análisis de comportamiento, el sistema PlugOS no contiene, en general, anuncios ni contenido de recomendaciones personalizadas. La experiencia digital del usuario se rige por su propia voluntad, no por algoritmos.
- **Principios de localización y minimización de datos**: Nuestra filosofía es que los datos que no se almacenan son los más seguros. Hemos rediseñado el propio sistema y todas sus aplicaciones básicas integradas (por ejemplo, el navegador, el teclado o el gestor de archivos) para seguir estrictamente los principios de localización y minimización de datos. Por ejemplo, nuestro teclado solo procesa las entradas del usuario localmente en el dispositivo y no realiza ningún tipo de sugerencia en la nube ni carga el diccionario del usuario.
- **Modelo de conocimiento cero**: Ni siquiera el fabricante del sistema ni TrustKernel pueden acceder a a ningún dato sensible del usuario a través de PlugOS. Toda la información del

usuario permanece en manos del propio usuario, y el papel del fabricante se limita a proporcionar una herramienta segura.

Los sistemas tradicionales como Android e iOS, incluso con las restricciones de seguimiento publicitario activadas, siguen subiendo algunos datos anonimizados a través de la telemetría. PlugOS, por el contrario, no tiene ese interruptor de restricción, ya que la recopilación de datos no existe en primer lugar.

6.2. Virtualización de sensores: bloqueo del seguimiento de huellas digitales de hardware

Las aplicaciones modernas utilizan ampliamente la «huella digital del dispositivo» para identificar y rastrear a los usuarios. Estas huellas suelen combinar cientos de parámetros procedentes de características de hardware (por ejemplo, IMEI, ID del sensor, información de banda base), del entorno de red (dirección IP, DNS, zona horaria) y del estado del software para crear un identificador único del usuario y del dispositivo. Incluso si un usuario cambia de cuenta o borra la caché, resulta difícil evitar la reidentificación y el rastreo continuo. La huella digital del dispositivo no suele requerir permisos especiales, y los usuarios a menudo no son conscientes de ello, lo que puede dar lugar continuamente a la filtración de información privada y al seguimiento de sus patrones de comportamiento.

Mediante la virtualización de sensores a nivel del sistema, PlugOS corta la ruta de generación de huellas digitales de dispositivos, protegiendo así de forma eficaz la identidad personal y la privacidad del comportamiento.

6.2.1 Virtualización de identificadores de identidad

Para los ID de hardware que pueden servir como identificadores únicos, PlugOS implementa la virtualización. Cuando las aplicaciones solicitan dicha información, el sistema proporciona de forma selectiva valores predeterminados genéricos y sin significado, o valores aleatorios diferentes para cada aplicación, en lugar de números de serie de hardware reales, información de la tarjeta SIM (IMSI/ICCID), direcciones MAC y similares.

6.2.2 Simulación de datos de sensores

Los usuarios pueden simular diversa información ambiental a través de un panel de control de privacidad centralizado para proporcionar datos falsos pero plausibles a las aplicaciones, con el fin de satisfacer sus necesidades operativas al tiempo que se protege la información real. Por ejemplo:

- **Ubicación geográfica virtual**: los usuarios pueden establecer una ubicación virtual fija o una ruta de desplazamiento virtual dinámica.

- **Estado de red virtual**: simula diferentes operadores de redes móviles, tipos de red e información de torres de telefonía móvil.

6.2.3 Conmutación dinámica de paso de hardware

Cuando sea necesario, los usuarios pueden, previa confirmación de permiso, pasar el hardware real del host (cámara, micrófono, Bluetooth) directamente a una aplicación específica dentro de PlugOS, alternando de forma flexible entre funcionalidad y protección de la privacidad. Los usuarios pueden revocar la autorización en cualquier momento, lo que garantiza que el acceso al hardware sea bajo demanda y se desactive cuando no se utilice.

Este diseño garantiza que incluso los algoritmos de identificación más agresivos tengan dificultades para establecer un vínculo de identidad fiable, maximizando así el anonimato y la desidentificación del usuario y del dispositivo.

6.3. Conexiones de red transparentes y controlables

El tráfico de red es una de las principales vías de fuga de datos. Muchas aplicaciones envían registros, datos de SDK o información sobre el comportamiento a servidores de terceros sin avisar al usuario.

PlugOS cuenta con un cortafuegos integrado a nivel del sistema que ofrece a los usuarios una visibilidad y un control sin precedentes sobre el tráfico de red, lo que les permite conocer, controlar y rastrear cada conexión de datos. Su herramienta principal es el cortafuegos a nivel del núcleo mencionado en el capítulo 3; esta sección se centra en sus funciones de protección de la privacidad.

- **Identificación y bloqueo de rastreadores:** La base de datos integrada puede detectar SDK publicitarios y de análisis comunes en las aplicaciones y alertar al usuario de los posibles riesgos de privacidad de la conexión. El usuario puede optar por bloquear estos rastreadores de terceros.
- **Auditoría de conexiones:** El cortafuegos registra todas las solicitudes de conexión de red de las aplicaciones en tiempo real y las presenta al usuario de forma clara y fácil de entender, incluyendo el nombre de dominio de destino, la IP y el protocolo. Esto evita las cargas de datos encubiertasy saca a la luz comportamientos de filtración de datos ocultos tras las aplicaciones. El usuario puede optar por bloquear las conexiones de red para determinadas aplicaciones o servidores de destino.
- **Modo de lista blanca:** Para situaciones que impliquen datos altamente confidenciales, los usuarios pueden habilitar un estricto El modo «lista blanca», que por defecto bloquea todas las conexiones de red y solo permite el acceso a nombres de dominio o direcciones IP específicos aprobados manualmente por el usuario. En situaciones en las que el acceso a la

red es totalmente innecesario, los usuarios pueden desactivar todos los permisos de red con un solo clic, eliminando así cualquier posibilidad de fuga de información.

7. Aplicación complementaria del host

La aplicación complementaria del host es la aplicación complementaria de PlugOS en dispositivos móviles u ordenadores. Su función principal es permitir que PlugOS utilice los periféricos del host —como la pantalla y el teclado— para la interacción y la visualización. En esta sección se aclarará, desde el punto de vista de su función, responsabilidades y límites, que esta aplicación no se convertirá en un vector de riesgo de seguridad para PlugOS.

7.1. Función principal: un «proxy de E/S»limitado

La aplicación complementaria del host estádiseñada para cumplir estrictamente los principios de privilegios mínimos y confianza cero. Dentro del modelo de seguridad de PlugOS, se clasifica explícitamente en la «Zona no confiable» (véase la sección 4.3). Su función principal es la de un «proxy de E/S» limitado, que sirve de puente entre el usuario y el dispositivo de hardware de PlugOS. En otras palabras, incluso si la aplicación complementaria del host contiene vulnerabilidades, es manipulada por un hacker o queda totalmente comprometida, no puede acceder ni descifrar los datos almacenados en PlugOS.

7.2. Responsabilidades y limitaciones: lo que puede y no puede Hacer

Para definir claramente sus capacidades, la siguiente tabla enumera las responsabilidades permitidas y los comportamientos restringidos por la arquitectura de la aplicación complementaria:

Responsabilidades permitidas (Lo que puede hacer)	Comportamientos restringidos por la arquitectura (Lo que no puede hacer)
1. Reenvío de entradas: Recibe señales deteclado, ratón, táctiles y otras entradas delhost y las reenvía sin modificaciones alhardware de PlugOS a través de un canalcifrado de extremo a extremo.	1. Descifrar datos: Todas las claves de cifrado se almacenan de forma segura en el TEE/SE del hardware de PlugOS y nunca salen del hardware. Laaplicación no puede obtener las claves, por lo que nopuede descifrar ningún dato que transmita.
2. Representar la salida: Recibe la pantallarecibe flujos de datos de fotogramas desde el hardware de PlugOS y los muestra en de la pantalla del host para su visualización.	2. Acceder a datos en texto plano: La aplicación solosirve como un canal para que PlugOS se comunique con el mundo exterior. No puede conocer el contenido específico de las comunicaciones de red.

3. Red de proxy cifrada: Actúa como salida de red, reenviando el tráfico de red cifrado desde PlugOS a Internet.	3. Ejecutar la lógica central: Todas las tareas informáticas básicas, como la autenticación de usuarios, el cifrado y descifrado de datos, la lectura yescritura del sistema de archivos y la ejecución deaplicaciones, se completan de forma independientedentro del hardware de PlugOS. La aplicación noparticipa en ningún proceso de toma de decisiones.
4. Comprobación de sus propias actualizaciones: Se conecta al servidoroficial para comprobar si hay nuevasversiones de la aplicación, sin implicarninguna interacción con los datos del Usuario.	4. Almacenamiento de datos de usuario: La aplicación no almacena ningún dato de usuario, configuración o estado de PlugOS en el host. Su diseño es sin estado.

7.3. Límite de seguridad: no puede suponer una amenaza para PlugOS aunque se vea comprometida

La aplicación complementaria se encuentra fuera del límite de confianza de PlugOS; pertenece a la zona no confiable. Incluso si la aplicación host es manipulada maliciosamente o controlada por completo por un hacker, no puede descifrar ni robar ningún dato dentro de PlugOS. La seguridad de PlugOS se deriva del hardware independiente, el cifrado del sistema y los límites estrictos, no de la dependencia del comportamiento de la aplicación complementaria. Este diseño elimina los riesgos de confianza asociados con las aplicaciones host de código cerrado.

8. Organización de la seguridad y gestión del personal

La seguridad de PlugOS no solo se debe a su arquitectura técnica, sino también a un sólido sistema organizativo y de gestión. Hemos creado equipos especializados en I+D de seguridad, pruebas, cumplimiento normativo y respuesta ante emergencias para formar un ciclo de seguridad completo, desde el desarrollo hasta la puesta en marcha.

- **I+D y pruebas de seguridad**: Exploramos continuamente tecnologías de seguridad de vanguardia, combinando pruebas multidimensionales con verificaciones de penetración para garantizar que el rendimiento de seguridad de PlugOS evolucione constantemente.
- **Cumplimiento normativo y gobernanza**: Cumplimos estrictamente con las normativas globales y los estándares del sector , y llevamos a cabo revisiones estrictas de las actividades de tratamiento de datos para cumplir con normativas como el RGPD y la PIPL.
- **Respuesta ante emergencias**: Hemos establecido un mecanismo de respuesta rápida que abarca la prevención, la gestión y el seguimiento de incidentes de seguridad.

- **Gestión de personal**: desde la contratación y la incorporación hasta el empleo continuo, losempleados se someten a estrictas verificaciones de antecedentes, firman acuerdos de confidencialidad, empleados se someten a estrictas verificaciones de antecedentes, firman acuerdos de confidencialidad,se les asignan permisos por niveles y reciben formación en seguridad. Esto garantiza que las responsabilidades en materia de seguridad de la información se asignen a personas concretas.

9. Gestión del ciclo de vida de desarrollo seguro

PlugOS integra los requisitos de seguridad y privacidad a lo largo de todo el proceso de desarrollo de software, formando un sistema de gestión del ciclo de vida de desarrollo (SDL) que cumple con las normas internacionales:

- **Requisitos y diseño**: Realización de modelos de amenazas de seguridad y evaluaciones de cumplimiento, dando prioridad a las métricas de seguridad para garantizar que los riesgos se eviten a nivel arquitectónico.
- **Desarrollo seguro**: Seguimiento de las normas internacionales de codificación segura (NIST, ETSI, OWASP, etc.), combinando herramientas automatizadas con revisiones manuales para eliminar vulnerabilidades comunes.
- **Pruebas de seguridad**: Realización de pruebas multinivel y verificación de cumplimiento por terceros, incluyendo la solidez del cifrado, los mecanismos de protección de datos y las pruebas de penetración, para generar informes de seguridad profesionales.
- **Garantía continua**: tras el lanzamiento del producto, se implementan continuamente actualizaciones de seguridad, se supervisan las vulnerabilidades y se corrigen rápidamente para garantizar que PlugOS siga siendo seguro y controlable a lo largo de todo su ciclo de vida.

10. Operaciones y mantenimiento de seguridad

La seguridad de PlugOS se refleja no solo en su arquitectura y mecanismos técnicos, sino también en su seguridad operativa continua, el cumplimiento normativo y las certificaciones externas, lo que garantiza los más altos estándares de seguridad del sector. Entendemos que la base de la confianza de los usuarios no reside en la autoproclamación, sino en un sistema de gestión de operaciones de seguridad y mantenimiento que sea verificable, auditable y certificable.

10.1. Actualizaciones y mantenimiento seguros

PlugOS ha creado un mecanismo de actualización seguro, transparente y trazable:

- **Paquetes de actualización firmados y cifrados**: Todas las actualizaciones están firmadas oficialmente y se distribuyen a través de un canal cifrado. Antes de su instalación, deben superar la verificación de la firma digital y los controles de integridad.
- **Mecanismo de actualización diferencial**: además de garantizar la seguridad, este mecanismo reduce el tamaño de los paquetes de actualización, minimizando el impacto de las actualizaciones en la experiencia del usuario.
- **Capacidad de reversión rápida**: si se detecta que una actualización presenta problemas de compatibilidad o riesgos potenciales, el usuario puede revertir a la versión estable anterior con un solo clic.
- **Ejecución con privilegios mínimos**: El proceso de actualización opera estrictamente con privilegios mínimos, lo que evita que el propio servicio de actualización se convierta en un vector de ataque.

10.2. Centro de respuesta a emergencias de seguridad

Creemos que la colaboración abierta con la comunidad de seguridad es clave para mejorar la seguridad del producto. Por ello, hemos establecido un Centro de Respuesta a Emergencias de Seguridad de Productos estandarizado para proporcionar a los usuarios una respuesta de seguridad durante todo el ciclo de vida:

- **Soporte técnico de seguridad**: Ofrecemos respuesta y soluciones en tiempo real a los problemas de seguridad que encuentran los usuarios durante el uso (por ejemplo, la protección de datos tras la pérdida del dispositivo), creando un ciclo de colaboración entre las operaciones de seguridad del producto y la gestión de seguridad de los usuarios.
- **Programa de recompensa por errores**: Animamos y recompensamos activamente a investigadores de seguridad, académicos y hackers de sombrero blanco de todo el mundo para que realicen pruebas de seguridad en PlugOS. Nosotros

Hemos puesto en marcha un programa de recompensas por errores que ofrece recompensas económicas a las personas y equipos que descubran y nos comuniquen de forma responsable vulnerabilidades de seguridad válidas.

- **Política de divulgación pública de vulnerabilidades**: Hemos elaborado y hecho pública una política detallada de divulgación de vulnerabilidades, que ofrece un canal claro y seguro para que la . Nos comprometemos a reconocer y evaluar rápidamente los informes, a mantener la comunicación con el informante y a agradecerle públicamente una vez que se haya solucionado la vulnerabilidad.
- **Colaboración intersectorial**: Establecemos continuamente canales de colaboración con proveedores de seguridad, instituciones de investigación y comunidades de código abierto para mantenernos al día sobre la información sobre amenazas y responder con rapidez.

11. Lista de verificación de seguridad para el usuario

Para ayudar a los usuarios a aprovechar al máximo las capacidades de seguridad de PlugOS, recomendamos que revisen periódicamente la siguiente lista de verificación de seguridad:

- **Mantenga su clave de producto segura**: Los usuarios deben almacenar su clave de producto de forma segura. Si le te preocupa una posible filtración de tu clave de producto, puedes restablecerla en la configuración de PlugOS.
- **Compruebe los hosts vinculados**: revise periódicamente la lista de hosts vinculados en la configuración y elimine cualquier dispositivo que ya no se utilice o que no sea de confianza.
- **Reducir al mínimo los permisos**: Siga el principio de «bajo demanda», concediendo permisos sensibles (por ejemplo, cámara, micrófono, ubicación) a las aplicaciones solo cuando sean necesarios.
- **Configurar listas blancas de red**: Para las aplicaciones que manejan datos altamente sensibles, utilice la función de cortafuegos para restringir su acceso a la red.
- **Habilita la protección contra ataques de fuerza bruta**: en función de tu evaluación de riesgos, habilita la función que activa automáticamente la autodestrucción tras N intentos fallidos de contraseña. Asegúrate de hacer una copia de seguridad de tus datos de antemano.
- **Establezca una contraseña de coacción**: para mitigar el riesgo de una posible coacción física, preconfigure una contraseña para el modo señuelo.
- **Copia de seguridad periódica de los datos**: Sus datos son inestimables y debe realizar copias de seguridad periódicas para evitar su pérdida.
- **Mantenga el sistema actualizado**: Instale las actualizaciones de seguridad oficiales sin demora para garantizar que el sistema se mantenga en un estado de protección óptimo.

12. Conclusión

PlugOS es más que un simple producto, es la encamación practica de una filosofia de seguridadProporciona a los usuarios una verdadera caja fuerte digital al anclar la raiz de confianza en hardwareindependiente y verificable, y al combinar una arguitectura de defensa multicapa con un diseno deprotección de la privacidad con visión de futuro.

Con una cadena de confianza de hardware verificable, certificaciones de seguridad de tercerosindependientes, una aruitectura unica de confianza cero y un mecanismo de autodestrucción de datosPlugOS ofrece una soluci'n fiable, robusta y transparente para los usuarios con las más altas exigenciasen materia de soberania de datos y privacidad personal. Creemos que, al devolver el control total a losusuarios, PlugOS está estableciendo un nuevo punto de referencia para el futuro de la seguridad movil.