UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Marcelo Fernando Faicán Guamán
Tutor:
Mg. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: GUÍA PARA LA APLICACIÓN DE LLAVES CRIPTOGRÁFICAS EN TARJETAS CPA Y DE CRÉDITO

Elaborado por: MARCELO FERNANDO FAICAN GUAMAN, de C.I: 0102846037, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: GUÍA PARA LA APLICACIÓN DE LLAVES CRIPTOGRÁFICAS EN TARJETAS CPA Y DE CRÉDITO

Elaborado por: MARCELO FERNANDO FAICAN GUAMAN, de C.I: 0102846037, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, MARCELO FERNANDO FAICAN GUAMAN con C.I: 0102846037, autor del proyecto de titulación denominado: GUÍA PARA LA APLICACIÓN DE LLAVES CRIPTOGRÁFICAS EN TARJETAS CPA Y DE CRÉDITO

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024

Firma

Tabla de contenidos

APROBACIÓN DEL TUTOR ii
APROBACIÓN DEL TUTOR iii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE iv
INFORMACIÓN GENERAL 1
Contextualización del tema 1
Problema de investigación 2
Objetivo general 3
Objetivos específicos 3
Vinculación con la sociedad y beneficiarios directos: 3
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO 5
1.1. Contextualización general del estado del arte 5
1.2. Proceso investigativo metodológico 6
1.3. Análisis de resultados 6
CAPÍTULO II: PROPUESTA 9
2.1 Fundamentos teóricos aplicados 9
2.2 Descripción de la propuesta 12
2.3 Validación de la propuesta 35
2.4 Matriz de articulación de la propuesta 37
CONCLUSIONES 39
RECOMENDACIONES 40
BIBLIOGRAFÍA 41
Anexos 44
Anexo 1: Formato de Encuesta 44
Anexo 2: Resultados de la Encuesta. 50
Anexo 3: Guía para la aplicación de llaves criptográficas en Tarjetas CPA y Tarjetas de Crédito 55
Anexo 4: Validación de especialistas. 56

Índice de tablas

Tabla 1. Cifrado de Llaves. 11
Tabla 2. Importancia del Cifrado de Llaves 12
Tabla 3. Tipos de llaves Criptográficas 15
Tabla 4. Matriz de Articulación 37

Índice de figuras

Figura 1. Tecnología chip EVM. 9
Figura 2. Esquema general de funcionamiento del algoritmo simétrico AES 10
Figura 3. Definición de Algoritmos de Cifrado DES/3DES/AES 10
Figura 4. Estructura General de la Guía para la aplicación de llaves criptográficas orientadas a tarjetas de débito y tarjetas con bandera. 13
Figura 5. Llave DPK 17
Figura 6. Llave DAT 18
Figura 7. Llave PPK 19
Figura 8. Llave PVK 20
Figura 9. Llave CVV 21
Figura 10. Llave CVV2 22
Figura 11. Llave iCVV 23
Figura 12. Llave IMKAC 25
Figura 13. Llave IWK 26
Figura 14. Ceremonia de entrega de llaves. 28
Figura 15. Llave Master Key 29
Figura 16. Cifrado Simétrico 32
Figura 17. Algoritmo de Cifrado Data Encryption Standard 32
Figura 18. Algoritmo de Cifrado Double Data Encryption Standard. 33
Figura 19. Double-Length 33
Figura 20. Triple-Length 34
Figura 21. Componentes Criptográficos 35

INFORMACIÓN GENERAL

En el contexto digital de hoy, proteger las transacciones financieras es esencial. Dado el crecimiento masivo de las transacciones en línea y el uso generalizado de tarjetas de pago, es crucial asegurar la información confidencial de los usuarios.

Contextualización del tema

En la era digital, las empresas se encuentran en un entorno en constante cambio, donde la tecnología es un elemento fundamental para el funcionamiento y el éxito.

En la sociedad moderna, el uso de tarjetas de crédito para transacciones financieras se ha vuelto común, ya sea para compras en locales comerciales o en línea, o para retirar dinero de cajeros automáticos.

Zelada y Frank (2023) establecen que el uso de claves de cifrado es esencial para cualquier institución financiera que procese o envíe datos confidenciales, como números de identificación personal de titulares de tarjetas (PIN) o números de cuenta primaria (PAN).

La criptografía no solo preserva la confidencialidad e integridad de los datos del tarjetahabiente durante las transacciones, sino que también verifica las identidades de los participantes involucrados. En el ámbito de las tarjetas de débito y de marca, la criptografía facilita la adopción de tecnologías avanzadas como EMV (Europay, MasterCard y Visa), la tokenización, así como los HSM que representan el estándar más alto en la protección de claves privadas y las operaciones criptográficas relacionadas, y garantizan la implementación de la política establecida por la organización que las utiliza, determinando qué usuarios y aplicaciones pueden acceder a dichas claves vitales para minimizar el fraude y fortalecer la confianza de los consumidores en el entorno financiero digital.

"Cada transacción de pago electrónico tiene datos sensibles que necesitan ser protegidos al momento de ser impresos en registros de aplicación y/o almacenados. La forma de protegerlos es mediante una encriptación de los datos utilizando alguna llave criptográfica digital" (Higonet, 2022, págs. 7,8).

> La seguridad de los datos es un aspecto crucial de cualquier transacción en línea, especialmente cuando se trata de información financiera confidencial, como números de tarjetas de crédito, cuentas bancarias o identificación personal. Las violaciones de datos pueden tener graves consecuencias tanto para los consumidores como para las empresas, como robo de identidad, fraude, pérdida de confianza y responsabilidad legal. (FasterCapital, 2024)

Problema de investigación

En el ámbito de la seguridad financiera, tanto las tarjetas CPA (Common Payment Application) como las tarjetas con bandera (tarjetas con franquicia Master Card, VISA, etc) utilizan avanzados sistemas criptográficos para asegurar tanto la transmisión como la gestión de datos confidenciales.

Un HSM (Módulo de seguridad de hardware) se utiliza para procesar tarjetas de débito y tarjetas de crédito, cuya función principal es la autenticación de llaves, es decir llaves preconfiguradas por el gestor de seguridad.

Hay diferentes tipos de llaves criptográficas, entre las más usadas en las transacciones financieras esta las llaves IMKAC IMKSMC, IMKSMI para la gestión EMV, para la validación de la autenticación de las tarjetas están las CVV, CVV2 e ICVV, las llaves de transporte utilizadas para enviar tanto pines cifrados como llaves de un sitio a otro están las PPK (KEK), KIS, KIR o conocidas como ZCMK, también se utilizan las llaves de terminal que van en los terminales de pago, atms o POS estas son las llaves KTM, finalmente las llaves que se utilizan para validar los pines de las tarjetas en una transacción son las PVK3624.

En este contexto se observa la ausencia de una guía para la aplicación de llaves criptográficas orientadas para tarjetas CPA y tarjetas con bandera, la cual se pueda utilizar en los diferentes HSM.

Las entidades financieras a menudo emplean métodos variados que, aunque cumplen con los estándares de seguridad básicos, no maximizan ni la seguridad ni la eficiencia operativa. La evolución acelerada de las amenazas cibernéticas también provoca que los sistemas de gestión de llaves se vuelvan obsoletos rápidamente, elevando los riesgos de seguridad que pueden comprometer innumerables transacciones diariamente.

Este problema se intensifica por la falta de claridad en los procedimientos para generar y/o almacenar las llaves de cifrado. Sin una guía clara, las instituciones financieras enfrentan no solo aumentos en los riesgos de seguridad, sino también dificultades en cumplimiento normativo y eficiencia operativa, ya que se ha tenido casos en los cuales los colaboradores de alguna Institución Financiera, encargados de realizar este proceso no documentan el proceso que se realiza al momento de desarrollar algún proyecto de pago con tarjetas, el cual después de algún tiempo en el que se desee realizar algún proceso de configuración en el HSM no se cuenta con la información de las llaves criptográficas, llegando a ser un problema crítico para la Institución Financiera y más aún cuando el colaborador ya no se encuentra laborando en la Institución.

La investigación que se propone tiene como objetivo formular una guía eficaz y flexible para la aplicación de estas llaves, que no solo potencie la seguridad de las tarjetas CPA y de marca,

sino que también responda a las regulaciones y a las necesidades operativas cambiantes del sector financiero.

Con la presente guía lo que se pretende responder es:

¿Como generar el conocimiento general para aplicar de una manera adecuada las llaves criptográficas que intervienen en un proyecto de pago con tarjetas?

Objetivo general

Desarrollar una guía integral que analice e identifique los diferentes tipos de llaves criptográficas, específicamente en tarjetas CPA y tarjetas con bandera, proporcionando un proceso para su aplicación en el ámbito financiero.

Objetivos específicos

- Analizarlos los diferentes tipos de llaves criptográficas que se utilizan en el ámbito financiero.
- Identificar las llaves criptográficas que intervienen en tarjetas CPA y tarjetas con bandera, para ser aplicadas durante el proceso de generación de criptogramas resultantes para los diferentes tipos de tarjetas.
- Desarrollar una guía que proporcione la aplicación de llaves criptográficas para tarjetas CPA y tarjetas con bandera.
- Valorar la propuesta por medio del criterio de especialistas.

Vinculación con la sociedad y beneficiarios directos:

En un entorno digital, asegurar la seguridad de las transacciones financieras es crucial para preservar la confianza y la estabilidad económica. La investigación que se plantea tiene como objetivo desarrollar una guía sólida para la aplicación de llaves criptográficas en tarjetas CPA y tarjetas con marca, que son fundamentales para la protección de la información financiera. Este enfoque no solo fortalece la seguridad de las transacciones, sino que también asegura que las prácticas estén en conformidad con las normativas internacionales actuales, ofreciendo beneficios tangibles a diversos sectores de la comunidad.

Este estudio está alineado con el Objetivo de Desarrollo Sostenible (ODS) número 9: "Industria, Innovación e Infraestructura", que busca construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible, y fomentar la innovación.

Específicamente, la aplicación de tecnologías avanzadas en la seguridad financiera contribuye a la meta de desarrollar infraestructuras sostenibles, resilientes y robustas, que apoyen el crecimiento económico y el desarrollo tecnológico. La implementación de estas prácticas de seguridad es esencial para garantizar la integridad y la confianza en las operaciones financieras, lo cual es crucial para el desarrollo de una infraestructura de calidad y la promoción de la innovación en el sector financiero.

Este enfoque contribuye a la sostenibilidad del sistema financiero, mejorando la seguridad de las transacciones y, por ende, la confianza de los usuarios en los servicios financieros, lo cual es un elemento clave para el progreso económico y social.

El propósito de esta guía es ofrecer a empleados de una institución financiera las orientaciones y procedimientos esenciales para generar el conocimiento adecuado de llaves criptográficas empleadas en las transacciones con tarjetas de débito y crédito. La adecuada aplicación de estas llaves es crucial para asegurar la protección y confidencialidad de la información financiera.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En el entorno de las instituciones financieras, es importante considerar una guía que nos permita adquirir el conocimiento necesario de las llaves criptográficas que intervienen en un proyecto de pagos con tarjeta, generando así que la aplicación de dichas llaves criptográficas con ayuda de esta guía conlleve una implementación adecuada para asegurar la integridad y la confianza en las transacciones financieras, lo que resulta indispensable para el desarrollo de una infraestructura sólida y el fomento de la innovación en el ámbito financiero.

1.1. Contextualización general del estado del arte

> La gestión de claves criptográficas es un reto para la mayoría de las organizaciones. Muchas de las personas que realizan actividades de Key management lo hacen de forma ad hoc y con poca o ninguna formación. En la mayoría de los casos, cada función requerida supone una interrupción de sus responsabilidades laborales normales a tiempo completo. Además, el mantenimiento de claves criptográficas requiere una inversión sustancial en hardware y tecnología de aplicaciones de apoyo que se utiliza con poca frecuencia. (Utimaco, 2024)

Redtrust (2024) establece que el HSM es un dispositivo de hardware especializado, diseñado específicamente para proporcionar alta seguridad en la confidencialidad y disponibilidad de las claves criptográficas mediante la ejecución de rutinas de cifrado y descifrado.

En el aspecto de la seguridad de las llaves criptográficas hay que tener en cuenta la funcionalidad que proporciona un HSM.

Según Higonet (2022) “la función más importante de un módulo HSM es la de autenticación de llaves. Es decir, asegurarse de que sus operaciones solo se puedan realizar con llaves que hayan sido previamente autorizadas por un administrador de seguridad” (p. 11).

En el ámbito de la criptografía, se denomina "texto en claro" o "texto plano" a la información original que se desea proteger.

WordPress (2023) establece que el cifrado es el proceso de transformar texto legible en un formato ininteligible llamado texto cifrado, utilizando un algoritmo que se adapta mediante una clave secreta.

“El uso de criptografía en las tarjetas bancarias es conseguido debido al “chip” que se integra en las tarjetas bancarias y que es "leído" por la terminal bancaria. Esto se conoce como tecnología chip EVM” (Morales et al., 2022).

Acosta (2023) establece que el Estándar de seguridad PIN (o PCI PIN) de la industria de tarjetas de pago (PCI) es un estándar de seguridad que define los requisitos para el

manejo, procesamiento y transmisión seguros de números de identificación personal (PIN) durante el procesamiento de pagos en línea y fuera de línea, así como en terminales POS atendidos y desatendidos.

Zelada y Frank (2023) describen que actualmente, marcas como TRACK2 y PINBLOCK reconocen las claves de cifrado simétricas para el cifrado de datos y son esenciales para mantener seguros a los titulares de tarjetas durante las transacciones.

Centellas et al. (2022) establece que los algoritmos de cifrado de bloques como AES y 3DES están diseñados para cifrar información de un tamaño de byte específico, pero la información generalmente no cumple con esta condición. La solución a este problema es dividir la información en bloques, cuyo tamaño es necesario para aplicar un algoritmo de cifrado a cada bloque. Si no hay suficientes bytes en el último bloque, se llena con una determinada cadena de bytes, que se excluye durante el descifrado.

1.2. Proceso investigativo metodológico

En el desarrollo de esta guía para la implementación de llaves criptográficas en tarjetas de débito y tarjetas con bandera, se utilizará una metodología cuantitativa. Este enfoque metodológico se distingue por medir cuantitativamente las características específicas de las llaves criptográficas utilizadas en proyectos de pagos con tarjeta y su rendimiento en diferentes contextos, lo que facilita un análisis estadístico. Mediante la recopilación de datos a través de encuestas, se evaluarán variables como la seguridad y la eficiencia de las llaves criptográficas aplicadas. (Rodríguez, 2019)

El uso de encuestas permitirá recopilar datos de una amplia muestra de participantes de manera eficiente y sistemática.

Esto facilitará la comparación y el análisis de las respuestas, asegurando la validez y confiabilidad de los resultados.

1.3. Análisis de resultados

Para realizar el análisis de resultados, se llevó a cabo una encuesta utilizando una muestra no probabilística, enfocado a un grupo de especialistas, especialmente del área de Tecnología. El propósito de esta encuesta fue recolectar información relevante para examinar cuatro aspectos fundamentales: Conocimiento y Preparación, Percepción de Seguridad, Implementación y Sugerencias. Los resultados obtenidos se presentan en el Anexo 1 y 2.

Esta guía está diseñada para ser accesible, asegurando que los usuarios puedan implementarla fácilmente en sus configuraciones de Proyectos de pagos con tarjetas, optimizando así la seguridad y la gestión de sus sistemas criptográficos. Así pues, se ofrece un análisis detallado de los resultados para cada uno de estos grupos.

Conocimiento y Preparación

Los formularios completados para recopilar datos de los participantes contenían un componente distintivo de "conocimiento y preparación", que ayudó en el desarrollo de esta investigación.

El propósito de esta sección fue evaluar el conocimiento previo y la experiencia de los participantes en el manejo de los aspectos cruciales de la implementación y administración de llaves criptográficas en tarjetas de débito y crédito, así como su preparación para manejar los desafíos asociados en este ámbito.

El análisis de los resultados obtenidos en esta sección proporcionó información valiosa sobre las posibles brechas en el conocimiento y preparación de los participantes, lo que a su vez contribuyó a orientar las recomendaciones y conclusiones de esta tesis. Este enfoque permitió no solo evaluar el estado actual del conocimiento en la materia, sino también identificar áreas donde podría ser necesaria una mayor formación o apoyo.

Percepción de Seguridad

El objetivo principal de esta sección es evaluar cómo los participantes perciben la seguridad en el contexto de la implementación de claves criptográficas en tarjetas de débito y crédito.
La “conciencia de la seguridad” es un aspecto importante porque influye en la confianza del usuario y la aceptación de las tecnologías de seguridad implementadas.

A través de esta sección buscamos recoger las opiniones y sentimientos de los participantes sobre la efectividad de las medidas de seguridad actuales y su confianza en los sistemas de protección criptográfica.

Las preguntas de esta sección cubren aspectos como la confianza en la tecnología de cifrado utilizada, la percepción de los riesgos asociados con las transacciones con tarjeta y la sensación de seguridad debido a las medidas de cifrado adoptadas. El análisis de las respuestas nos permitió identificar tendencias y patrones en las percepciones de seguridad de los participantes, lo cual es esencial para comprender las actitudes hacia la adopción de una guía para la aplicación de llaves criptográficas.

Los hallazgos de esta sección brindan una perspectiva valiosa que complementa el análisis técnico y objetivo del estudio, brindando una visión más integral de cómo los usuarios finales perciben la seguridad. Esta información es esencial para desarrollar una guía que no solo

mejoren la seguridad técnica, sino que también mejoren la confianza a la hora de realizar proyectos relacionados con tarjetas de pagos.

Implementación y Mejoras

Esta sección tiene como objetivo extraer las experiencias, de ser el caso, de los encuestados en la implementación de soluciones criptográficas y explorar temas como los desafíos encontrados durante la adquisición de conocimientos para la implementación, las estrategias adoptadas para superar estos desafíos y la efectividad de las soluciones implementadas.

Además, se pidió a los participantes que sugirieran mejoras, según sea el caso, que podrían mejorar la seguridad y el rendimiento en una guía para aplicar llaves criptográficas en tarjetas de débito y tarjetas con bandera.

Los resultados obtenidos en la sección "Implementación y mejora" brindan una visión detallada y práctica que complementa el análisis técnico de esta guía y proporciona una base para desarrollar recomendaciones específicas y viables. Estas recomendaciones tienen como objetivo mejorar la implementación de claves criptográficas y mejorar la seguridad de las transacciones en el sector financiero.

Opiniones y Sugerencias

Esta sección es importante ya que a través de preguntas abiertas se recogen opiniones sobre la efectividad de la solución, desafíos no resueltos y posibles mejoras.

La retroalimentación de las respuestas complementa los datos cuantitativos y proporciona información única para una guía enfocada en cubrir conocimientos aun no adoptados para la aplicación de llaves criptográficas en tarjetas de pagos.

Estas contribuciones han sido cuidadosamente analizadas e integradas en las conclusiones y recomendaciones de esta guía.

CAPÍTULO II: PROPUESTA

Este capítulo describe el desarrollo de una guía orientada a la aplicación de llaves criptográficas en tarjetas de débito y tarjetas con bandera.

2.1 Fundamentos teóricos aplicados

Criptogramas

Los criptogramas son mensajes cifrados que solo pueden ser entendidos por aquellos que logran descifrar la clave en cuestión. Uno los métodos más usuales y simples para crear un criptograma es el llamado cifrado por sustitución, que consiste en reemplazar cada letra por otra o por un número. (Pérez et al., 2019)

Criptografía

"La Criptografía es la ciencia que se ocupa de crear algoritmos para ocultar mensajes y de este modo, evitar que sean leídos por personas no autorizadas" (Bernstein, 2021, pág. 5).

El uso de criptografía en las tarjetas bancarias es conseguido debido al "chip" que se integra en las tarjetas bancarias y que es "leído "por la terminal bancaria. Esto se conoce como tecnología chip EVM. El chip ya integra una pareja de llaves pública y privada desde su fabricación, y se personaliza cuando dicha tarjeta se asigna a una persona en particular. (Morales et al., 2022)

En la Figura 1, se muestra un ejemplo de la tecnología chip EVM.

Figura 1.
Tecnología chip EVM.

Nota: Figura tomada del trabajo de investigación sobre Criptografía: una tecnología antigua en aplicaciones modernas de alto impacto (Morales et al., 2022).

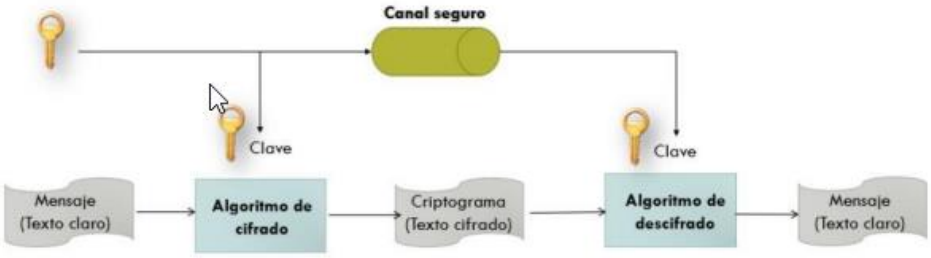
Cifrado AES

Según González et al. (2021) describe que:

> El Estándar de cifrado avanzado (AES) o también conocido como "Rjandael", es el cifrado simétrico más utilizado en la actualidad. Por definición, este tipo de algoritmos aplican la misma clave tanto para cifrar como descifrar; y para su intercambio requieren de un canal de comunicación seguro, el algoritmo de cifrado recibe como entradas: un mensaje o texto claro y una clave, y genera como salida un criptograma o texto cifrado. (p. 147)

En la Figura 2, se muestra el grafico de la Estructura del algoritmo AES.

Figura 2.
Esquema general de funcionamiento del algoritmo simétrico AES



Nota: Figura tomada de (González et al., 2021)

Es necesario citar los conceptos de los algoritmos de cifrado utilizados en los criptogramas de las diferentes llaves criptográficas para las tarjetas de débito y de marca, para esto se lo presenta en la siguiente Figura 3.

Figura 3.
Definición de Algoritmos de Cifrado DES/3DES/AES

Algoritmo	Definición
DES	El Estándar de Cifrado de Datos es un cifrado de bloques de clave simétrica. El DES fue creado en 1972 por IBM utilizando el algoritmo de encriptación de datos. Fue adoptado por el gobierno de Estados Unidos como algoritmo de cifrado estándar. Es vulnerable a los ataques de clave cuando se utiliza una clave débil.
3DES	Algoritmo de Cifrado de Datos Triple, que es un cifrado de bloques. El estándar de cifrado de datos triple se publicó por primera vez en 1998 y recibe su nombre porque aplica el cifrado DES tres veces a cada bloque de datos, cifrado - descifrado - cifrado utilizando DES.
AES	El algoritmo Advance Encryption Standard fue desarrollado en 1998 por Joan Daemen y Vincent Rijmen, este algoritmo permite una combinación de longitud de datos y clave de 128, 192 y 256 bits. Este algoritmo es cifrado por bloques de clave simétrica.

Nota: Tomado de (Ahumada-Urquijo et al., 2022).

HSM.

Según Lang (2022) describe que:

> Un módulo de seguridad por hardware es un dispositivo de hardware resistente a la manipulación de externos, que se utiliza principalmente en la industria financiera para proporcionar altos niveles de protección a las claves criptográficas y a la información de las tarjetas de los clientes. Generalmente, estos módulos se emplean para proporcionar llaves para funciones críticas como encriptación, desencriptación y autenticación. (p.10)

Cifrado de Llaves Criptográficas

El cifrado de llaves criptográficas es el proceso de usar una llave de cifrado (a menudo llamada llave de envoltura o llave maestra) para cifrar otras llaves criptográficas. Este método se utiliza para proteger las llaves cuando se almacenan en un medio no seguro o cuando se transmiten a través de una red insegura. La importancia de estas llaves se lo describe en la Tabla 1.

Tabla 1.
Cifrado de Llaves.

Proceso	Descripción
Selección de la Llave de Maestra	Primero, se selecciona una llave de cifrado robusta, conocida como llave Maestra. Esta llave será utilizada para cifrar y descifrar las llaves criptográficas de menor nivel.
Cifrado	Las llaves que necesitan ser protegidas son cifradas con la llave Maestra. Este proceso convierte las llaves originales en una forma cifrada que solo puede ser interpretada o devuelta a su forma original mediante la aplicación de la llave de envoltura correcta.
Almacenamiento o Transmisión	Las llaves cifradas pueden almacenarse de manera segura o transmitirse a través de redes inseguras sin el riesgo de que sean comprometidas, dado que cualquier actor malicioso necesitaría la llave de envoltura para acceder a las llaves protegidas.

Importancia del Cifrado de Llaves

El cifrado de llaves criptográficas es un componente vital en una estrategia de seguridad robusta, asegurando que incluso si se compromete la seguridad periférica, las llaves criptográficas, y por ende los datos que protegen, permanezcan seguros. Este nivel de protección es fundamental para mantener la integridad y la confidencialidad de los sistemas de información en todas las Instituciones Financieras. La importancia del cifrado de llaves se lo presenta en la Tabla 2.

Tabla 2.
Importancia del Cifrado de Llaves

Proceso	Descripción
Seguridad Mejorada	El cifrado de llaves ayuda a proteger contra el acceso no autorizado a las llaves criptográficas, un elemento esencial en la protección de datos sensibles.
Cumplimiento Normativo	Muchas normas de seguridad de datos, como el PCI DSS de la producción de las tarjetas de pago, exigen el cifrado de claves como medida de seguridad necesaria.
Gestión de Llaves	Facilita una gestión más segura y eficiente de llaves criptográficas, especialmente en entornos donde las llaves deben ser distribuidas o gestionadas a lo largo del tiempo.

Códigos de Verificación de Claves (KVC)

Un Código de Verificación de Clave (KVC) se utiliza para verificar, sin comprometer el secreto, que una clave o un componente de clave se ha ingresado correctamente o para confirmar que el valor de una clave almacenada es el esperado.

2.2 Descripción de la propuesta

En el contexto actual, la seguridad de las transacciones financieras se ha vuelto cada vez más preocupante debido al aumento de fraudes y ciberataques dirigidos a los sistemas de pago.

Las tarjetas de débito y de marca (tarjetas de marca compartida) se utilizan ampliamente en el comercio global, lo que las convierte en objetivos principales para actividades maliciosas.

Para mitigar estos riesgos, el cifrado es una herramienta esencial para proteger los datos confidenciales.

A medida que las transacciones electrónicas se convierten en el núcleo de la economía moderna, la seguridad en los pagos electrónicos ha adquirido una importancia crítica. Sin embargo,

en el ámbito financiero, se observa una falta de conocimiento generalizado sobre los distintos tipos de llaves criptográficas que son fundamentales para asegurar estas transacciones.

La implementación de llaves criptográficas es esencial para garantizar la confidencialidad, integridad, y autenticidad de la información intercambiada durante las transacciones con tarjetas de pago. A pesar de su importancia, muchos profesionales del sector financiero no están familiarizados con los diferentes tipos de llaves criptográficas que intervienen en este proceso, ni con las mejores prácticas para su implementación.

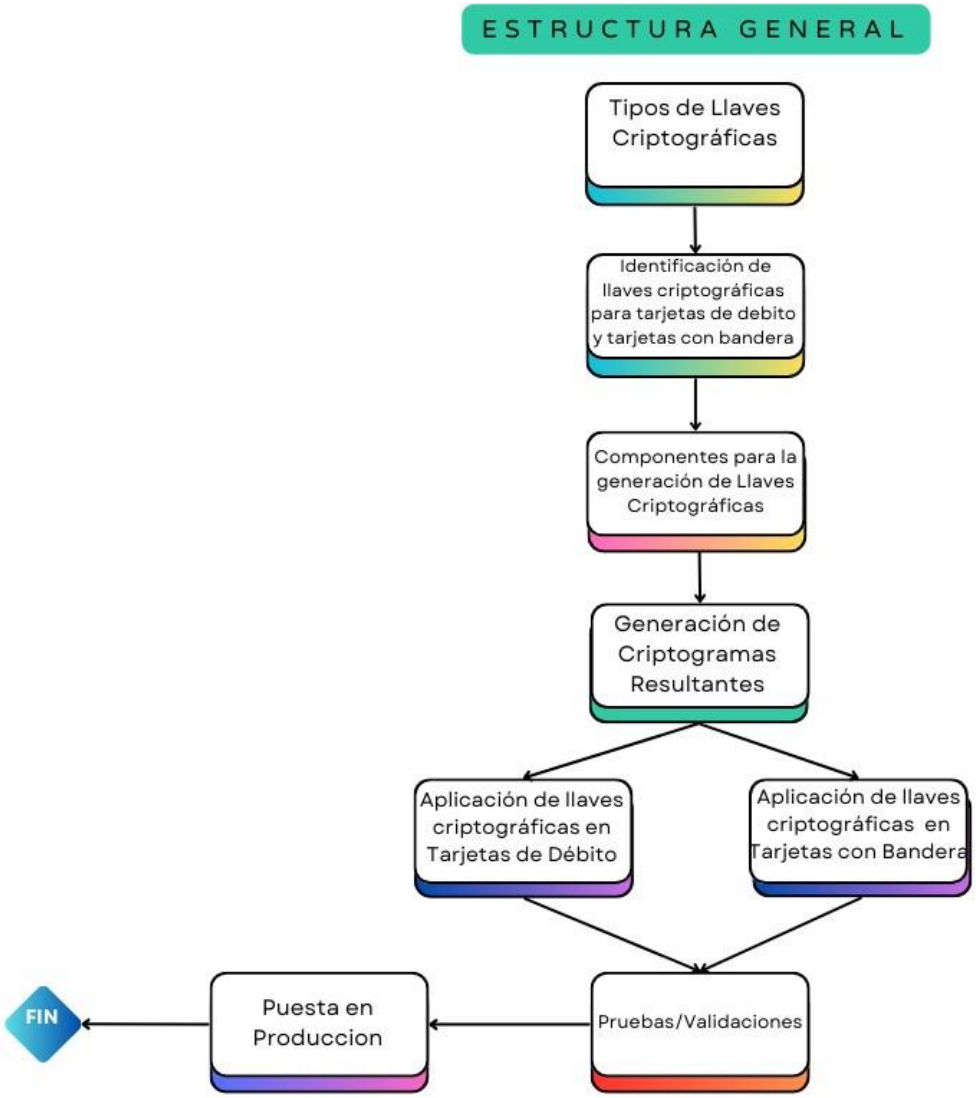
Desde esta perspectiva la propuesta de este estudio es elaborar una guía exhaustiva que explique de manera clara y detallada los tipos de llaves criptográficas utilizados en tarjetas de débito y tarjetas con bandera, así como su correcta implementación en proyectos de pago con tarjetas. Esta guía servirá como un recurso valioso para los profesionales del sector financiero y de la seguridad informática, brindándoles el conocimiento necesario para llevar a cabo proyectos de implementación de sistemas de pago seguros y eficientes.

a. Estructura general

Para realizar la propuesta de esta guía se basó en la ausencia de información de la aplicabilidad de llaves criptográficas para tarjetas de débito y tarjetas con bandera, de manera que se consideró importante investigar el procedimiento a seguir, por lo que en la Figura 4 se presenta la estructura de la propuesta para resolver el problema, orientándose en generar el conocimiento necesario para profesionales de Instituciones Financieras.

Figura 4.

Estructura General de la Guía para la aplicación de llaves criptográficas orientadas a tarjetas de débito y tarjetas con bandera.



La aplicación de llaves criptográficas es un desafío para la mayoría de las organizaciones. Muchas personas involucradas en esta actividad lo hacen de manera improvisada y reciben poca o ninguna capacitación.

Por lo tanto, surge la necesidad de desarrollar una guía que permita aplicar las llaves criptográficas que intervienen en el proceso de protección de datos en tarjetas de débito y de marca. Esta guía proporcionará el conocimiento fundamental necesario para configurar adecuadamente las llaves criptográficas en cualquier HSM, lo que facilitará un flujo más eficiente de actividades. Al contar con una base sólida, se podrá llevar a cabo la configuración de llaves criptográficas de manera más ágil y efectiva en proyectos relacionados con pagos mediante tarjetas.

b. Explicación del aporte

En el ámbito financiero, la criptografía presenta varias llaves criptográficas que intervienen en el proceso de proteger la información del tarjetahabiente, a continuación, en la Tabla 3, se presenta los diferentes tipos de estas llaves.

Tabla 3.
Tipos de llaves Criptográficas

Tipos de Llaves	Descripción
KM (Master Key)	Es una llave de longitud doble/triple para almacenar de forma segura otras claves en un HSM
KIR (Key Identification Response)	Es un conjunto de llaves criptográficas que se usa para probar la identidad de otras claves.
KIS (Key Identification Signature)	Permiten que el HSM identifique de manera única y segura cada llave criptográfica dentro del sistema
DPK (Data Protection Key)	Para cifrar datos sensibles que se deben almacenar o transmitir de forma segura.
DAT(Data Authentication Token)	Es una llave criptográfica creada para un fin especial, generar MACs o firmas digitales que autentican los datos en una transacción financiera.
PEK (Pin Encryption Key)	Su función principal es cifrar y proteger los números de identificación personal (PIN) de los usuarios durante las transacciones para prevenir el acceso no autorizado y el fraude.
PPK (Pin Protection Key)	Se utiliza con el propósito de proteger el PIN de los usuarios.
PVK (PIN Verification Key)	Es una llave criptográfica utilizada para verificar PIN (Personal Identification Number)r. más a menudo, el PIN de los usuarios en sistemas de pago, tales como tarjetas de crédito.
CVV (Card Verification Value)	Es utilizada para generar el código CVV que se imprime en la tarjeta de crédito o débito.
CVV2 (Card Verification Value 2)	Se utiliza para generar el código CVV2 que se imprime en el reverso de la tarjeta

iCVV (Integrated Circuit Card Verification Value)	Se utiliza para producir un código iCVV el cual se guarda en el chip interno de la tarjeta de pago. iCVV es el nombre de la versión del CVV el cual es utilizado en el caso de tarjetas con chip.
IMKAC (Issuer Master Key for Application Cryptogram)	Una llave maestra utilizada por los emisores de tarjetas para generar y verificar criptogramas en aplicaciones de pago.
IWK (Issuer Working Key)	La IWK se utiliza para derivar otras llaves necesarias para operaciones particulares, como llaves de cifrado de PIN, llaves de autenticación de mensajes, o llaves de sesión para transacciones individuales.
KTP (Key Transport Protection)	Se utilizan para cifrar otras llaves de cifrado antes de transferirlas de un sistema a otro.
KEK (Key Encryption Key)	Se utiliza para cifrar otras llaves, como llaves de cifrado de datos, claves de sesión, claves de PIN, entre otras.
ZCMK (Zone Control Master Key)	Es una llave maestra utilizada para asegurar las comunicaciones y operaciones criptográficas dentro de una "zona" de seguridad específica dentro de una infraestructura financiera.

IDENTIFICACIÓN DE LLAVES CRIPTOGRÁFICAS PARA TARJETAS CPA Y TARJETAS CON BANDERA

TARJETAS CPA (DEBITO)

En esta parte del documento se identifica las llaves criptográficas que intervienen en las tarjetas con bandera, siendo las que se describen a continuación:

Llave DPK (Data Protection Key)

Es una llave criptográfica utilizada específicamente para proteger datos sensibles.

Protección de Datos Sensibles

La DPK se utiliza para cifrar datos sensibles que necesitan ser almacenados o transmitidos de forma segura. Esto incluye, por ejemplo, información personal identificable (PII), datos de transacciones financieras, números de tarjetas de crédito, y otros datos críticos en el contexto financiero.

El uso de la DPK asegura que incluso si los datos cifrados son interceptados o accedidos sin autorización, no puedan ser interpretados sin la clave correcta.

Ejemplo de Uso

Supongamos que una institución financiera almacena datos de transacciones de tarjetas de crédito. Para proteger estos datos, utiliza una DPK dentro de su HSM para cifrar la información antes de almacenarla en su base de datos. Cuando sea necesario acceder a los datos, el HSM utilizará la DPK para descifrar la información de manera segura y permitir su uso por aplicaciones autorizadas, sin que la clave salga del HSM en ningún momento.

Las llaves DPK que se muestra en la Figura 5, también pueden usarse cuando se genera lotes de tarjetas que van a ir donde los proveedores de plásticos (creación de tarjetas), estas llaves cifran el lote de datos para que no sean expuestas ya que los números de tarjetas y datos CVV podrían comprometerse.

Figura 5.
Llave DPK

Nota: Creada por la IA

Llave DAT (Data Authentication Key)

Es una llave criptográfica utilizada específicamente para la generación de MACs (Message Authentication Codes) o firmas digitales que autentican los datos en una transacción financiera.

Verificación de Integridad y Autenticidad

La llave DAT juega un papel crucial en la verificación de la integridad y autenticidad de los datos. Cuando se utiliza para crear un token o una firma, cualquier alteración en los datos puede ser detectada, ya que el DAT generado a partir de los datos modificados no coincidirá con el esperado.

Dentro de un HSM, la generación y uso de la llave DAT se realiza en un entorno seguro, protegiendo la clave de cualquier intento de acceso no autorizado o manipulación.

Ejemplo de Uso

En un sistema de pago con tarjeta, cuando se realiza una transacción, se puede utilizar una llave DAT para generar un MAC (Message Authentication Code) que se envía junto con los datos de la transacción. El receptor de la transacción utiliza la misma llave DAT para verificar el MAC y asegurarse de que los datos no han sido alterados durante la transmisión, validando así la autenticidad de la transacción. En la Figura 6, se muestra la utilización de esta llave.

Figura 6.

Llave DAT

Nota: Creada por la IA

Llave PPK (Pin Protection Key)

Es una llave que se utiliza específicamente para proteger el PIN (Personal Identification Number) de los usuarios.

Protección del PIN

La Pin Protection Key (PPK) se utiliza para cifrar y proteger los PINs de los usuarios durante el proceso de generación, almacenamiento, y verificación. Esto asegura que el PIN no sea expuesto en ningún momento en texto claro y que solo sea accesible dentro del entorno seguro del HSM.

Cifrado del PIN

Cuando un usuario ingresa su PIN, este es cifrado utilizando la PPK antes de ser transmitido o comparado. El PIN cifrado es lo que se maneja dentro del sistema, protegiendo el valor real del PIN de posibles interceptaciones o accesos no autorizados.

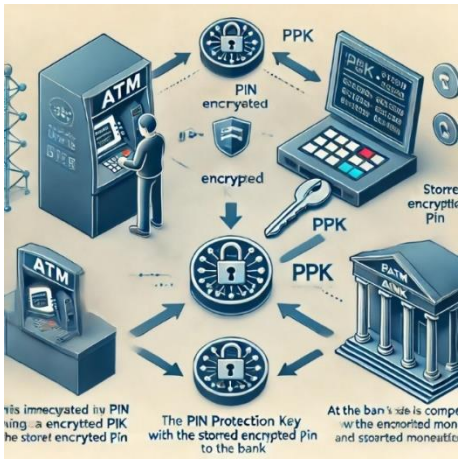
Verificación del PIN

Durante una transacción, como un retiro de efectivo en un cajero automático, el PIN ingresado por el usuario es cifrado usando la PPK y luego comparado con el PIN cifrado almacenado en la base de datos o enviado para verificación. Si los valores coinciden, la transacción es autorizada. Este proceso asegura que solo el titular de la tarjeta, que conoce el PIN correcto, pueda realizar la transacción.

Ejemplo de Uso

En un cajero automático, cuando un usuario ingresa su PIN, el PIN es cifrado inmediatamente usando la PPK antes de ser transmitido al banco para la verificación. Si el PIN cifrado coincide con el PIN cifrado almacenado en el banco, la transacción se autoriza, permitiendo al usuario retirar dinero o realizar otras operaciones. En la Figura 7, se muestra la utilización de esta llave.

Figura 7.
Llave PPK



Nota: Creada por la IA

Llave PVK (PIN Verification Key)

Es una llave utilizada para verificar el **PIN (Personal Identification Number)** de los usuarios en sistemas de pago, como transacciones con tarjetas de crédito o débito. La PVK juega un papel crucial en garantizar que el PIN ingresado por un usuario durante una transacción sea correcto y corresponda al PIN asociado con la cuenta o tarjeta.

Verificación del PIN

La PIN Verification Key (PVK) Se utiliza para verificar que el PIN ingresado por el usuario coincida con el PIN almacenado o esperado por el sistema. Esto es esencial en operaciones donde se necesita autenticar a un usuario antes de aprobar una transacción, como retiros de cajeros automáticos, pagos en puntos de venta, o accesos a cuentas bancarias.

Proceso de Verificación

Cuando un usuario ingresa su PIN, el HSM utiliza la PVK para realizar una comparación segura. Dependiendo del sistema, esto puede implicar la generación de un valor de referencia (por ejemplo, un PIN offset) que se compara con la información almacenada.

Generación de Valores de Verificación

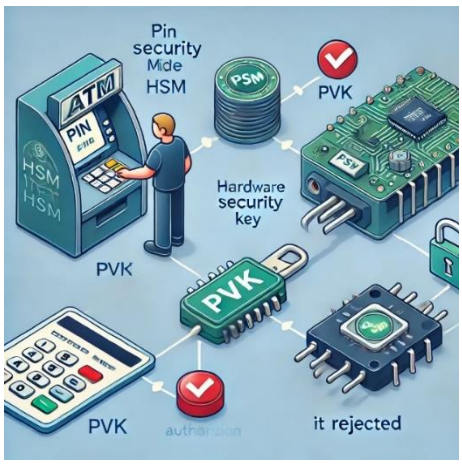
La PVK puede ser utilizada para generar un valor de verificación (como un PIN offset o un PIN block) que se almacena de forma cifrada y se utiliza en futuras comparaciones. Esto asegura que los datos del PIN no se almacenen en texto claro, aumentando la seguridad.En sistemas donde

los PINs no se almacenan directamente, la PVK ayuda a calcular y verificar estos valores derivados del PIN, permitiendo la autenticación sin comprometer la seguridad.

Ejemplo de Uso

Durante una transacción en un cajero automático, cuando un usuario ingresa su PIN, el sistema envía el PIN al HSM, donde se utiliza la PVK para verificarlo. El HSM compara el PIN ingresado con el valor de verificación generado previamente. Si coinciden, la transacción es autorizada, de lo contrario, se rechaza. En la Figura 8, se muestra la utilización de esta llave.

Figura 8.
Llave PVK



Nota: Creada por la IA

Llave CVV (Card Verification Value)

Se refiere a una llave utilizada para generar y verificar el **CVV** de una tarjeta de crédito o débito. El CVV es un código de seguridad impreso en la tarjeta que se utiliza para verificar que la persona que realiza la transacción tiene físicamente la tarjeta.

Generación del CVV

La llave CVV es utilizada dentro del HSM para generar el código CVV que se imprime en la tarjeta de crédito o débito. Este código suele ser de 3 o 4 dígitos y se genera a partir de un algoritmo que toma como entrada la llave CVV, el número de la tarjeta (PAN), y otros datos como la fecha de expiración de la tarjeta.

El CVV generado es único para cada combinación de PAN y fecha de vencimiento, lo que lo convierte en una medida de seguridad efectiva para validar transacciones.

Verificación del CVV

Durante una transacción en línea o por teléfono (donde la tarjeta no está presente), el sistema de pago utiliza la llave CVV en el HSM para verificar que el CVV ingresado por el usuario coincide con el CVV generado originalmente y almacenado en el sistema. Esta verificación

asegura que el cliente que realiza la transacción tiene en su posesión la tarjeta física, ya que el CVV no es almacenado en el chip de la tarjeta ni en el sistema del comerciante.

Ejemplo de Uso

Cuando un usuario realiza una compra en línea, se le solicita que ingrese el número de la tarjeta, la fecha de vencimiento y el CVV. El comerciante envía estos datos al banco emisor, que utiliza la llave CVV almacenada en su HSM para verificar que el CVV ingresado coincide con el CVV generado originalmente. Si coincide, la transacción es aprobada. En la Figura 9, se muestra la utilización de esta llave.

Figura 9.

Llave CVV

Nota: Creada por la IA

Llave CVV2 (Card Verification Value 2)

Es una llave utilizada para generar y verificar el CVV2 de una tarjeta de crédito o débito. El CVV2 es un código de seguridad impreso en el reverso de las tarjetas de pago, que se utiliza principalmente en transacciones en las que la tarjeta no está presente físicamente, como las compras en línea o por teléfono.

Generación del CVV2

La llave **CVV2** en el HSM se utiliza para generar el código CVV2 que se imprime en el reverso de la tarjeta. Este código suele ser de 3 dígitos en las tarjetas Visa y MasterCard, y de 4 dígitos en las tarjetas American Express. El CVV2 se genera a partir de un algoritmo criptográfico que utiliza la llave CVV2, el número de la tarjeta (PAN), la fecha de vencimiento de la tarjeta, y posiblemente otros datos como entradas. Este proceso asegura que el CVV2 es único para cada tarjeta.

Verificación del CVV2

Durante una transacción sin tarjeta presente (por ejemplo, compras en línea), el CVV2 ingresado por el titular de la tarjeta se compara con el valor que fue generado y almacenado

utilizando la llave CVV2 en el HSM. Si el CVV2 ingresado coincide con el valor esperado, la transacción es aprobada. Esto confirma que la persona que realiza la transacción posee la tarjeta física, ya que el CVV2 es un dato que no se almacena ni en la banda magnética ni en el chip de la tarjeta.

Diferencia entre CVV y CVV2

CVV (Card Verification Value) **g**eneralmente se refiere al código impreso en la banda magnética o en el chip de la tarjeta, que se utiliza en transacciones donde la tarjeta está físicamente presente.

CVV2 (Card Verification Value 2) específicamente se refiere al código de seguridad impreso en el reverso de la tarjeta, utilizado en transacciones donde la tarjeta no está presente físicamente (por ejemplo, en línea o por teléfono).

Ejemplo de Uso

Cuando un cliente realiza una compra en línea, se le solicita que ingrese el número de la tarjeta, la fecha de vencimiento y el CVV2. El comerciante envía estos datos al procesador de pagos, que utiliza la llave CVV2 en su HSM para verificar que el CVV2 ingresado coincide con el CVV2 generado y almacenado originalmente. Si la verificación es exitosa, la transacción es aprobada. En la figura 10, se muestra la utilización de esta llave. En la Figura 10, se muestra la utilización de esta llave.

Figura 10.

Llave CVV2

Nota: Creada por la IA

Llave iCVV (Integrated Circuit Card Verification Value)

Se refiere a una llave utilizada para generar y verificar el **iCVV**, que es un código de verificación utilizado en las tarjetas de pago con chip (tarjetas EMV). El iCVV es similar al CVV (Card Verification Value) estándar, pero está específicamente diseñado para tarjetas con chip y se utiliza para proteger las transacciones realizadas con estas tarjetas.

Generación del iCVV

La llave iCVV es utilizada dentro del HSM para generar el código iCVV, que se almacena en el chip de la tarjeta de pago. El iCVV es una versión del CVV que ha sido adaptada para su uso en el entorno de tarjetas con chip, asegurando que las transacciones sean seguras y que la tarjeta no haya sido clonada. El iCVV se genera utilizando un algoritmo que toma como entrada la llave iCVV, el número de la tarjeta (PAN), la fecha de vencimiento de la tarjeta, y otros datos específicos de la tarjeta. Este código se almacena en el chip de la tarjeta y se utiliza en transacciones para verificar la autenticidad de la tarjeta.

Verificación del iCVV

Durante una transacción en la que se utiliza una tarjeta con chip, el sistema verifica que el iCVV generado por el chip de la tarjeta coincide con el iCVV esperado que fue previamente generado y almacenado en el HSM del emisor.

Este proceso de verificación asegura que la tarjeta no ha sido clonada y que la transacción es legítima, ya que un iCVV válido solo puede ser generado por el chip original de la tarjeta en combinación con la llave iCVV.

Diferencia entre CVV, CVV2 y iCVV

CVV (Card Verification Value) utilizado en la banda magnética de las tarjetas para verificar transacciones en las que se utiliza la banda magnética.

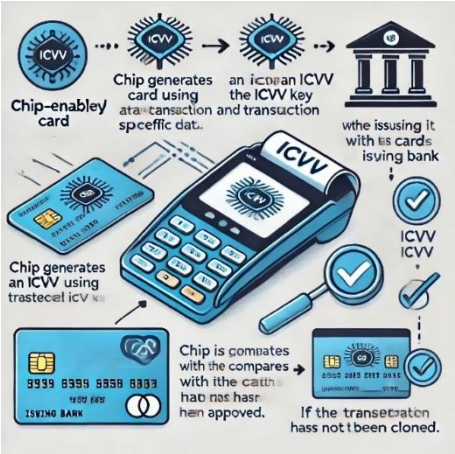
CVV2 (Card Verification Value 2) código de seguridad impreso en la tarjeta, utilizado en transacciones donde la tarjeta no está presente físicamente (en línea o por teléfono).

iCVV (Integrated Circuit Card Verification Value) específicamente diseñado para tarjetas con chip (EMV), el iCVV protege las transacciones realizadas con el chip de la tarjeta, asegurando que la tarjeta no ha sido clonada.

Ejemplo de Uso

Cuando un cliente realiza una compra utilizando una tarjeta con chip en un terminal de punto de venta (POS), el chip genera un iCVV utilizando la llave iCVV y otros datos específicos de la transacción. El iCVV es enviado al banco emisor, que lo compara con el iCVV almacenado para verificar la autenticidad de la tarjeta. Si el iCVV coincide, la transacción es aprobada, garantizando que la tarjeta no ha sido clonada. En la Figura 11, se muestra la utilización de esta llave.

Figura 11.
Llave iCVV



Nota: Creada por la IA

Llave IMKAC (Issuer Master Key for Application Cryptogram)

Es una llave maestra utilizada por el emisor de la tarjeta para la generación y verificación de criptogramas en aplicaciones de pago, especialmente en el entorno de tarjetas de pago EMV (Europay, MasterCard, and Visa). Los criptogramas son códigos de seguridad generados durante las transacciones para autenticar y proteger los datos involucrados en la transacción.

Generación de Criptogramas

La Issuer Master Key for Application Cryptogram (IMKAC) es utilizada dentro del HSM para generar las claves derivadas necesarias para la creación de criptogramas en transacciones EMV. Un criptograma es un código criptográfico que se genera utilizando datos específicos de la transacción, como el número de la tarjeta, la fecha de vencimiento, el monto de la transacción, y otros datos. El criptograma generado es enviado al emisor de la tarjeta como parte de la transacción y se utiliza para autenticar la transacción y verificar la integridad de los datos.

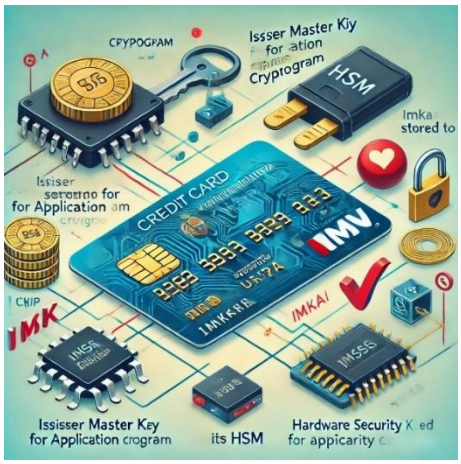
Verificación de Criptogramas

Durante una transacción, la IMKAC también se utiliza para verificar que el criptograma generado por la tarjeta es válido y coincide con lo que se espera según los datos de la transacción. Esta verificación asegura que la transacción no ha sido manipulada y que la tarjeta es legítima. El proceso de verificación implica utilizar la IMKAC para regenerar el criptograma y compararlo con el criptograma enviado. Si coinciden, la transacción es aprobada

Ejemplo de Uso

Cuando un cliente utiliza una tarjeta de crédito EMV para realizar una compra, el chip de la tarjeta genera un criptograma utilizando una clave derivada de la IMKAC. Este criptograma es enviado al banco emisor durante la transacción. El banco, utilizando la IMKAC en su HSM, verifica el criptograma para asegurarse de que la transacción es auténtica y que no ha sido manipulada. Si la verificación es exitosa, la transacción es aprobada. En la Figura 12, se muestra la utilización de esta llave.

Figura 12.
Llave IMKAC



Nota: Creada por la IA

LLAVES CRIPTOGRÁFICAS PARA TARJETAS CON BANDERA

En esta parte del documento se identifica las llaves criptográficas que intervienen en las tarjetas con bandera, siendo las mismas que se utilizan en las tarjetas CPA, con la diferencia que las franquicias como por ejemplo VISA llaman ciertas llaves con diferentes nombres pero que al final, realizan el mismo proceso.

Las llaves para tarjetas con bandera se describen a continuación:

- DPK
- PPK
- PVK
- CVV
- CVV2
- ICVV
- PVV
- IMKAC

Este tipo de llaves se explica su concepto, funcionalidad y ejemplo de uso en las tarjetas con bandera, ya que tienen la misma funcionalidad

Además de este tipo de llaves, en las tarjetas con bandera se utiliza la llave IWK.

Llave IWK (Issuer Working Key)

Es una llave utilizada por el emisor de tarjetas para realizar diversas operaciones criptográficas relacionadas con la seguridad y la autenticación de transacciones. La IWK es una llave derivada de una llave maestra y es utilizada en operaciones específicas como el cifrado de datos, la generación de criptogramas, y la verificación de autenticidad en transacciones financieras.

Derivación de Claves

La Issuer Working Key (IWK) es generalmente derivada de una llave maestra, como la IMK (Issuer Master Key), y está diseñada para usarse en operaciones criptográficas específicas dentro de un entorno seguro, como un HSM. La IWK se utiliza para derivar otras llaves necesarias para operaciones particulares, como claves de cifrado de PIN, claves de autenticación de mensajes, o claves de sesión para transacciones individuales.

Ejemplo de Uso

Durante una transacción con tarjeta en un punto de venta, el HSM del emisor utiliza la IWK para cifrar el PIN ingresado por el cliente y para generar un criptograma que se envía junto con los datos de la transacción al banco emisor. El banco utiliza la misma IWK para verificar el criptograma y asegurar que la transacción es legítima y que el PIN no ha sido comprometido. En la Figura 13, se muestra la utilización de esta llave.

Figura 13.
Llave IWK

Nota: Creada por la IA

Componentes para Llaves Criptográficas

Intercambio de Información de Llaves

El intercambio de información de llaves criptográficas se lo realizara de acuerdo a los procesos establecidos entre la entidad Financiera y la red de pagos, previamente acordada entre las empresas de realizar el proyecto de tarjetas de débito y tarjetas con bandera.

Custodios de Componentes de Llaves Criptográficas

Los custodios de claves criptográficas son individuos o entidades encargados de la administración y protección de las claves criptográficas dentro de una organización. Su función es esencial para garantizar que estas claves, vitales para el cifrado y descifrado de datos, se mantengan seguras y no sean accesibles por personas no autorizadas.

La red de pagos envía los tres componentes de la clave de cifrado a los custodios la Empresa Procesadora de Pagos en sobres sellados y seguros que no deben manipularse durante el transporte. Los componentes deben transportarse a través de 3 empresas de mensajería diferentes para garantizar entregas separadas. Si se utiliza la misma empresa de mensajería para enviar los 3 componentes, el cliente debe enviar los 3 paquetes en fechas diferentes. Cada componente solo se puede enviar después de que se haya recibido y verificado el componente anterior.

Para realizar la ceremonia de llaves entre la Institución Financiera y la Empresa Procesadora de Pagos, la Institución financiera que desarrollará el proyecto de pago con tarjetas, deberá contar con al menos tres componentes, lo que requiere tres custodios responsables de la custodia, el transporte y el manejo de cada componente. Nadie que no sea un custodio puede ver el componente respectivo, estos custodios deben ser asignados por la misma Institución, mediante la asignación de algún proceso interno, para ser los responsables del resguardo de dichas llaves, para precautelar la seguridad de dicha información.

En criptografía, una ceremonia de Llaves se refiere a un evento en el cual se genera o utiliza una llave criptográfica.

La ceremonia propiamente dicha, puede tomar un tiempo considerable según la cantidad de llaves involucradas, este proceso puede realizarse en persona o por mensajería.

Para cumplir con los requisitos de la industria de tarjetas de pago (PCI), las llaves deben estar compuesta por al menos 3 componentes hexadecimales, de longitud doble (32 caracteres) con un algoritmo de cifrado 3-DES.

Los componentes de las llaves criptográficas deben transportarse físicamente (no por medios digitales) y por separado, es por esto que los custodios pueden acudir personalmente a las oficinas de la empresa certificadora de tarjetas y realizar la ceremonia de entrega de los componentes de cada llave criptográfica que serán custodios individualmente o pueden llegar

los componentes de las llaves criptográficas a través de diferentes empresas de mensajería en un sobre cerrado identificado, serializado y numerado. Los componentes criptográficos no pueden (bajo ninguna circunstancia) enviarse por el mismo método, es decir, si uno se envía por correo ordinario, los demás deben hacerlo por otro método. A menudo se utilizan 3 empresas de mensajería diferentes para transportar los componentes de forma individual y totalmente separada para reducir el riesgo de vulneración.

Este proceso se debe decidir entre las dos empresas que van a realizar el proyecto de pago con tarjetas, el método a realizar el intercambio de información.

Si surge algún problema y se pierden uno o más componentes, el criptograma resultante está comprometido y se deben generar nuevos componentes para preservar la integridad y confidencialidad de la información sensible. En este escenario, será necesario reiniciar el proceso.

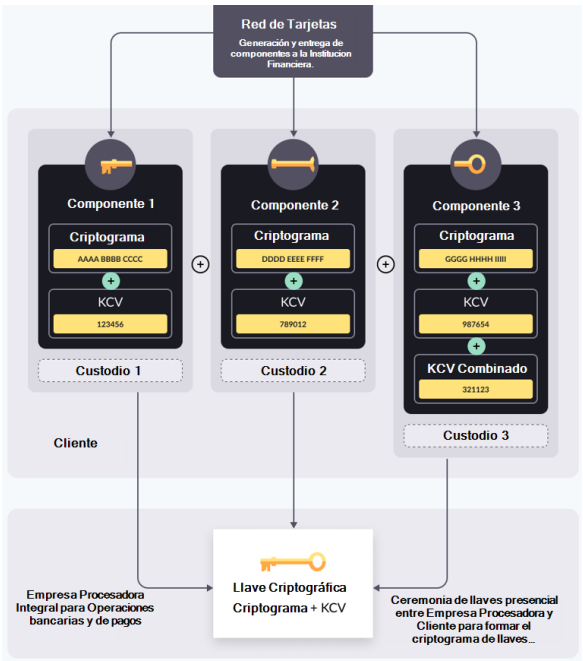
La ceremonia de entrega de llaves se lleva a cabo en las oficinas de la Empresa Procesadora Integral para Operaciones bancarias y de Pago, en una sala segura con miembros encargados de la custodia de las llaves (uno por cada componente) y al menos un conductor de ceremonia y un testigo.

En ese momento, los responsables de la custodia de los componentes de las llaves criptográficas pueden ser empleados de la Institución Financiera que visiten las oficinas, o bien empleados de la Empresa Procesadora Integral para Operaciones Bancarias y de Pago, quienes tienen la custodia delegada de los componentes que el cliente ha proporcionado para su uso.

En la Figura 14, se presenta un diagrama de los pasos a seguir en una ceremonia de llaves.

Figura 14.

Ceremonia de entrega de llaves.



La ceremonia se lleva a cabo en una sala segura con miembros custodios de las llaves (uno por cada componente) y al menos un conductor ceremonial y un testigo.

Los responsables de la custodia de las llaves criptográficas y los testigos firman un acuerdo de confidencialidad relacionado con la información, la asistencia y las actas de la ceremonia.

No se les permite ingresar a la sala de seguridad con dispositivos electrónicos de audio y video, como teléfonos celulares, teléfonos inteligentes, grabadoras, computadoras, entre otros.

Ingreso y Configuración de llaves Criptográficas

En esta fase se identifica los tipos de llaves criptográficas que se utilizaran para interactuar tanto en las tarjetas de débito, como en las tarjetas con bandera, para luego realizar la generación de los criptogramas resultantes de cada llave criptográfica.

Llave Master Key

MK es la llave de cifrado maestra, utilizada por un HSM para proteger otras llaves de cifrado. Normalmente, la MK posee todas las claves de la organización.

Las claves MK no se utilizan para cifrar datos, se utilizan para cifrar/descifrar otras llaves de cifrado que se utilizan para realizar operaciones en el HSM.

La Llave Maestra (MK) garantiza que incluso si se interrumpe el tráfico entrante y saliente, el verdadero valor de la llave no se verá comprometido.

Cuando un dispositivo recibe una operación MK, sabe internamente que debe usar MK para descifrar el contenido y acceder al valor de llave real.

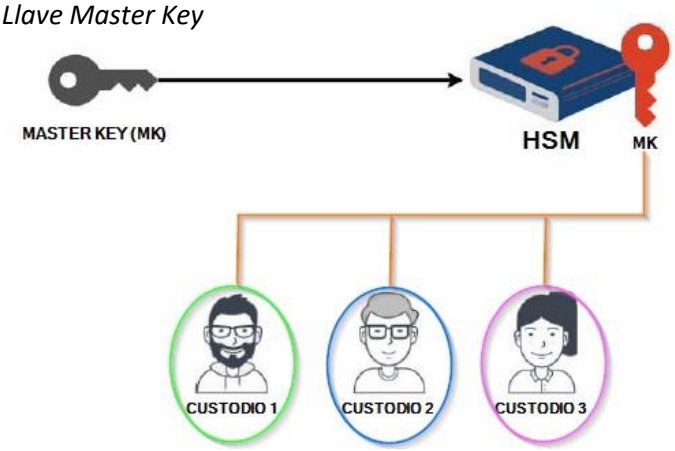
Ésta es la única forma de acceder al valor original, razón por la cual los dispositivos HSM son tan seguros.

Además, MK se instala según el procedimiento previsto, tras lo cual se pierde el acceso a su valor.

La Llave MK como se muestra en la Figura 15, generalmente se divide en 3 componentes (componentes principales) que son conservados por diferentes titulares. Para almacenar cada componente se suele utilizar una tarjeta con chip, que almacena automáticamente el valor.

Figura 15.

Llave Master Key



Si no dispone de tarjeta con chip, se recomienda hacerlo manualmente, escribir el valor del componente en una plantilla que servirá como base para poderlo replicar y documentar todas las llaves criptográficas, que funcionaran en un HSM para procesar transacciones enfocadas a tarjetas de pago.

Validación y Pruebas

El objetivo de la fase de pruebas es garantizar que las llaves de encriptación aplicadas en las tarjetas con bandera (tarjetas de crédito y débito) funcionen correctamente, asegurando la confidencialidad y autenticidad de los datos almacenados en la tarjeta y transmitidos durante las transacciones. Estas pruebas también buscan verificar la resistencia de las llaves criptográficas frente a intentos de acceso no autorizado. 2. Entorno de Pruebas Las pruebas se realizarán en un entorno controlado que simula un ecosistema de pagos típico, incluyendo:

- **Emuladores de Tarjetas:** Para simular tarjetas con bandera.
- **HSM (Hardware Security Module):** Para la gestión segura de las llaves criptográficas.
- **Terminales de Punto de Venta (POS):** Para realizar transacciones con las tarjetas simuladas.
- **Servidores de Autorización:** Que replican el comportamiento de los servidores de una entidad financiera.

Procedimiento de Pruebas

Generación y Asignación de Llaves

- **Generación de Llaves Maestras:** Utilizando el HSM, se generarán las llaves maestras que se utilizarán para derivar otras claves como la CVV, iCVV, KEK, etc.
- **Asignación de Llaves a Tarjetas:** Las llaves criptográficas serán asignadas a las tarjetas simuladas en el emulador, incluyendo llaves para la protección del PIN (PIN Encryption Key) y llaves para la verificación de la autenticidad de la tarjeta (CVV, iCVV).

Pruebas de Cifrado y Descifrado

- **Cifrado de Datos Sensibles:** Se cifrarán datos como el número de tarjeta (PAN), el PIN del usuario y la información del titular. Posteriormente, se realizará el descifrado en diferentes escenarios para asegurar que el proceso es reversible y seguro.

- **Verificación del CVV/iCVV:** Se generarán CVV e iCVV utilizando las llaves asignadas y se verificarán durante transacciones simuladas para asegurar su correcta implementación y funcionalidad.

Pruebas de Autenticación

- **Autenticación de Transacciones:** Se simularán transacciones de compra donde se verificará la autenticidad de la tarjeta a través de la verificación del CVV/iCVV y el uso del PIN. Se comprobará que las transacciones solo se autorizan cuando las claves criptográficas se utilizan correctamente.
- **Verificación de la Integridad de los Datos:** Se realizarán pruebas para asegurar que cualquier modificación no autorizada de los datos cifrados sea detectada e impida la autorización de la transacción.

c. Estrategias y/o técnicas

Luego de haber identificado las llaves, es importante conocer el tipo de configuración criptográfica que se debe establecer para todo el grupo de llaves que deberán precautelar la información sensible de datos y transacciones de los usuarios que utilicen las tarjetas de pago.

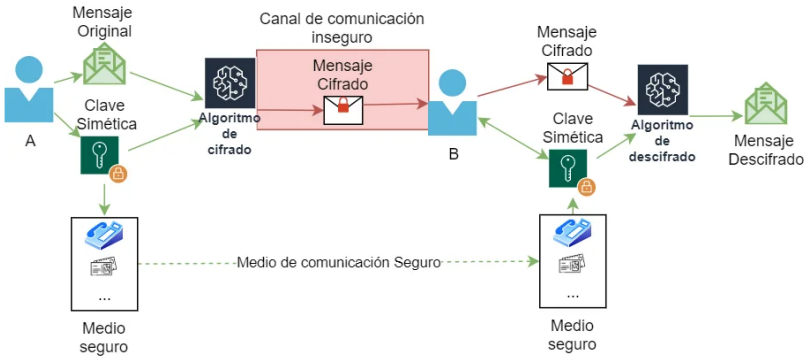
Para la generación de Criptogramas Resultantes, se propone utilizar las configuraciones que a continuación se describen.

Criptografía simétrica o criptografía de una clave

> La criptografía simétrica es la técnica criptográfica más antigua que existe, pero sigue ofreciendo un alto nivel de seguridad. Se basa en la utilización de una única clave secreta que se encargará de cifrar y descifrar la información, ya sea información en tránsito con protocolos como TLS, o información en un dispositivo de almacenamiento extraíble. La criptografía simétrica fue el primer método empleado para el cifrado de la información, se basa en que se utilizará la misma contraseña tanto para el cifrado como el descifrado, por tanto, es fundamental que todos los usuarios que quieran cifrar o descifrar el mensaje, tengan esta clave secreta, de lo contrario, no podrán hacerlo. (Lopez, 2023)

En la Figura 16, nos presenta el proceso de un cifrado Simétrico.

Figura 16.
Cifrado Simétrico



Nota: Imagen tomada de "Criptografía Simétrica y Asimétrica". (Ibero, 2023)

Algoritmos de Cifrado Utilizado

> El algoritmo DES (Data Encryption Standard), también conocido como DEA (Data Encryption Algorithm), era uno de los algoritmos de cifrado por bloques más utilizados en el sector financiero. Este algoritmo, que se seleccionó por primera vez como norma FIPS en 1976, se considera actualmente inseguro debido a la longitud extremadamente corta de su clave (56 bits reales de clave y 8 bits de paridad), que se ve fácilmente comprometida con las técnicas computacionales existentes. (Acosta, 2022)

En la Figura 17, nos presenta el algoritmo de cifrado DES.

Figura 17.
Algoritmo de Cifrado Data Encryption Standard

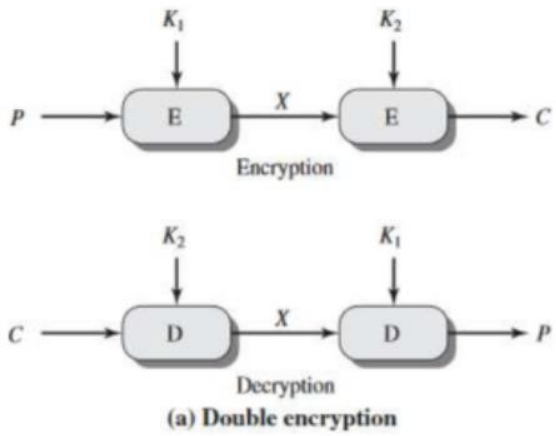
$$8\left\{\begin{matrix} * & * & * & * & * & * & * & p_1 \\ * & * & * & * & * & * & * & p_2 \\ * & * & * & * & * & * & * & p_3 \\ * & * & * & * & * & * & * & p_4 \\ * & * & * & * & * & * & * & p_5 \\ * & * & * & * & * & * & * & p_6 \\ * & * & * & * & * & * & * & p_7 \\ * & * & * & * & * & * & * & p_8 \end{matrix}\right\}$$

Nota: Imagen tomada de "La guía definitiva de Key Blocks" (Acosta, 2022).

Para resolver este problema, se implementaron dos algoritmos que, basados en el DES, incrementaban la complejidad del proceso al incorporar repeticiones adicionales y claves adicionales.

"Double-DES (2DES o 2DEA) Usa dos instancias de DES en el mismo bloque de texto en claro. En cada instancia usa diferentes claves de encriptación. Actualmente, este algoritmo está obsoleto" (Acosta, 2022). En la Figura 18, se muestra el tipo de cifrado doble DES.

Figura 18.
Algoritmo de Cifrado Double Data Encryption Standard.

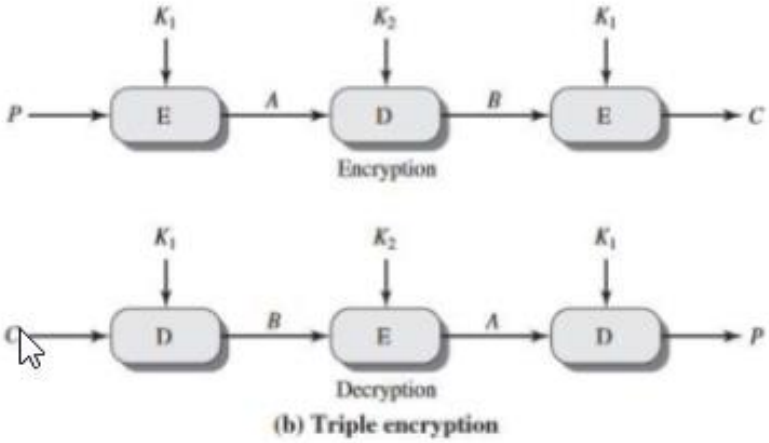


Nota: Imagen tomada de “La guía definitiva de Key Blocks”. (Acosta D. , 2022)

“Triple-DES (3DES o TDEA) Tres instancias de DES en el mismo texto en claro, pudiendo emplear dos claves (Double-length TDEA) o tres claves diferentes de encriptación (Triple-length TDEA)” (Acosta, 2022).

En la Figura 19, se muestra el cifrado 3DES de tamaño doble.

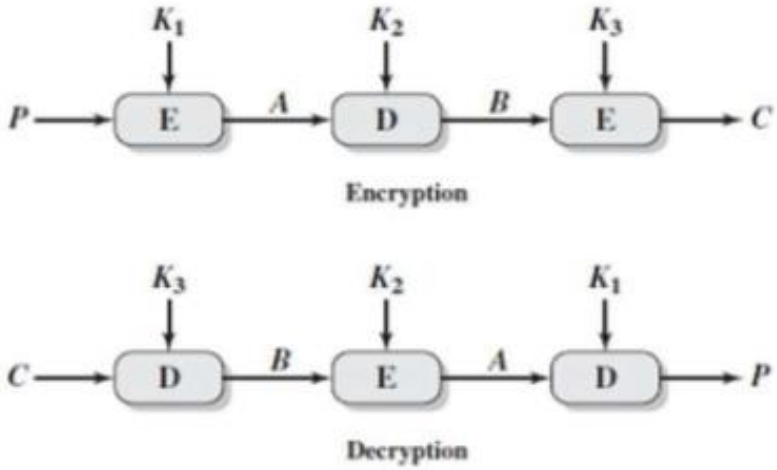
Figura 19.
Double-Length



Nota: Imagen tomada de “La guía definitiva de Key Blocks”. (Acosta D. , 2022)

En la Figura 20, se muestra el cifrado 3DES de tamaño doble.

Figura 20.
Triple-Length



Nota: Imagen tomada de "La guía definitiva de Key Blocks". (Acosta D. , 2022)

Triple DES es un algoritmo de cifrado de clave simétrica que realiza por tres ocasiones el cifrado de DES.

En los sistemas financieros, especialmente en el uso de HSMs, es habitual emplear estas configuraciones de llaves para proteger transacciones y otros datos sensibles. Las llaves de doble y triple longitud son preferidas en escenarios donde la seguridad es crítica, como en la protección de PINs(Personal Identification Number), la generación de MACs (Códigos de Autenticación de Mensajes), y el cifrado de datos financieros

En la industria financiera actualmente se invierten millones de dólares en dispositivos que sólo soportan la tecnología 3DES, como los cajeros automáticos.

Componentes

Los componentes que se utilizan para la generación de los criptogramas resultantes de las diferentes llaves pueden ser dos o tres componentes. Esto se define de acuerdo al número de componentes que se entregaron al momento de la entrega de los mismos cuando se realiza el protocolo de entrega de llaves criptográficas.

Por ejemplo, generar dos componentes criptográficos de 128 bits se refiere al proceso de crear dos segmentos o partes de una clave criptográfica, donde cada componente tiene una longitud de 128 bits. Estos componentes pueden ser utilizados en conjunto para formar una llave completa, o bien pueden ser usados por separado dependiendo de la aplicación criptográfica específica.

Propósito de los Componentes Criptográficos

En muchos sistemas criptográficos, una llave maestra se puede dividir en varios componentes por razones de seguridad. Esto es común en sistemas de key management donde se requiere que varias partes (por ejemplo, administradores o dispositivos) colaboren para reconstruir la llave original. Cada componente por sí solo no es suficiente para reconstruir la llave completa, lo que incrementa la seguridad al requerir la presencia de múltiples componentes para utilizar la clave.

En la Figura 21, se presenta un ejemplo de componentes criptográficos.

Figura 21.
Componentes Criptográficos

Nota: Figura tomada de “emvlab.org” (Emvlab, 2022)

Ingreso de Llaves Criptográficas en Modulo de Seguridad de Hardware (HSM)

El proceso de ingreso y generación de criptogramas resultantes para las llaves criptográficas que se aplican en tarjetas de débito y tarjetas pago con bandera se lo presenta en el Anexo 3, en el cual se muestra el ingreso de las llaves criptográficas en diferentes HSM, demostrando así que los tipos de llaves se utilizan con la misma configuración para las diferentes marcas de HSM.

2.3 Validación de la propuesta

Para realizar este estudio, se ha contado con la colaboración de expertos en el sector financiero que ocupan puestos en distintas instituciones del ámbito.

Los resultados obtenidos de esta validación son esenciales para ajustar la presente guía, garantizando su eficacia en la implementación de llaves criptográficas en tarjetas de débito y tarjetas con bandera.

La evaluación fue realizada por dos especialistas que laboran en entidades financieras y un especialista en el ámbito de manejo y Administración de cajas Criptográficas para el ámbito financiero.

• Especialista #1. Enrique Jimbo, Especialista en Infraestructura

• Especialista #2. Byron Molina, Especialista en Manejo y Administración Cajas Criptográficas HSM

• Especialista #3. Paul Zhañay, responsable del Departamento de Seguridad Informática.

La validación de los especialistas se adjunta en el Anexo 4.

2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 4.

Matriz de Articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Investigación Llaves Criptográficas	Teoría de Seguridad Informática	Metodología Bibliográfica	Revisión en tesis, artículos, libros	Utilizar las ventajas de la investigación en llaves criptográficas para aplicarlas en proyectos de pago de tarjetas de débito y tarjetas con bandera.	Fuente Bibliográfica
Algoritmos	Algoritmos de protección segura 3DES	Metodología Bibliográfica	Investigación de Algoritmos de encriptación	Nivel de protección del algoritmo de encriptación utilizado	Fuente Bibliográfica

Encuestas dirigidas a grupos basadas en criterios determinados.	Proceso de Investigación Cuantitativa	Encuestas, revisión documental	Elaboración de encuestas	El resultado de las encuestas es que la mayoría de los encuestados tienen un conocimiento medio-bajo sobre llaves criptográficas	Encuestas
Aplicación de Llaves Criptográficas en tarjetas de débito y tarjetas con bandera	Conceptos teóricos sobre cada llave que interviene en el proceso	Metodología Bibliográfica	Ingreso de componentes en Dispositivo de Módulo de Seguridad.	Generación de Criptogramas resultantes de las diferentes llaves criptográficas	HSM

CONCLUSIONES

En este trabajo, se ha abordado con detalle la identificación de llaves criptográficas para tarjetas de débito y tarjetas de marca, destacando la función específica que cada llave desempeña en el proceso de generación de estas tarjetas. A través de una investigación exhaustiva y el desarrollo de una guía que pueda abordar este tema, el presente estudio contribuye al entendimiento de estas llaves de seguridad, esenciales en el ámbito de las transacciones financieras.

Primordialmente, la investigación ha revelado la complejidad y la importancia crítica de una guía adecuada de las llaves criptográficas, demostrando que la seguridad de las tarjetas no solo depende de las tecnologías utilizadas, sino también del conocimiento y la implementación estratégica de dichas tecnologías. La guía propuesta ofrece un camino claro para la integración efectiva de las llaves criptográficas, asegurando que cada llave cumpla su función específica para fortalecer la integridad y la confidencialidad de los datos del usuario.

Además, se ha destacado la importancia de la educación y la capacitación continua en el campo de la criptografía financiera. Comprender para qué sirve cada llave en el proceso no solo mejora la implementación de las medidas de seguridad, sino que también prepara el terreno para innovaciones futuras que puedan responder a amenazas emergentes en el panorama de la ciberseguridad.

En conclusión, esta investigación no solo enriquece el conocimiento existente sobre la aplicación de llaves criptográficas en tarjetas de pago, sino que también proporciona una herramienta para profesionales y académicos interesados en la seguridad financiera. A medida que avanzamos hacia una era aún más digitalizada, la relevancia de esta investigación continuará creciendo, subrayando la necesidad de enfoques de seguridad cada vez más sofisticados y adaptados a los desafíos del futuro.

RECOMENDACIONES

Se recomienda fomentar programas de capacitación continua para los profesionales que trabajan con tecnologías de tarjetas de pago. Estos programas deben incluir módulos especializados en criptografía aplicada, con un enfoque particular en la función y gestión de las llaves criptográficas, asegurando que los profesionales estén siempre al tanto de las últimas prácticas y tecnologías de seguridad. Esto debido a cómo evolucionan las amenazas cibernéticas, también lo debe hacer nuestro entendimiento y habilidades para combatirlas eficazmente.

Alentar y financiar la investigación continua en el campo de la criptografía aplicada a tarjetas de débito y de marca para explorar nuevas técnicas y tecnologías de cifrado que puedan ofrecer mejores niveles de seguridad puesto que la innovación continua es crucial para mantenerse un paso adelante de los actores maliciosos en el ámbito de la ciberseguridad.

BIBLIOGRAFÍA

Acosta, D. (14 de Diciembre de 2022). *PCI Hispano*. https://www.pcihispano.com/la-guia-definitiva-de-bloques-de-claves-criptograficas-key-blocks/

Acosta, D. (25 de Enero de 2023). *PCI Hispano*. PCI Hispano: https://www.pcihispano.com/que-es-pci-pin/

adastra. (20 de 05 de 2021). https://thehackerway.com/2021/05/20/post-explotacion-en-sistemas-windows-con-ghostpack-parte-3-de-3/#:~:text=Rubeus,ataques%20contra%20el%20protocolo%20Kerberos.

Ahumada-Urquijo, L. X., Valencia-Ortiz, J., Velandia-Beltrán, M. F., Y Mendoza-Calderón, J. B. (2022). *geox.udistrital.edu.co.* geox.udistrital.edu.co: https://geox.udistrital.edu.co/index.php/vinculos/article/view/19224/19134

Arango, O. (2023). *El ABC de la seguridad informática: guía práctica para entender la seguridad digital.* https://doi.org/http://repositorio.itm.edu.co/handle/20.500.12622/5901

Bernstein, S. (2021). Algoritmo criptográfico para descifrar el protocolo de intercambio de claves HK17. 5. https://dspaceapi.uai.edu.ar/server/api/core/bitstreams/0302ab91-494c-43f9-992e-ee859f6e51c7/content

Centellas, L., Blanco, L., Y Sandoval, J. (10 de Enero de 2022). *Estudio comparativo de los algoritmos de* . Scielo.org.bo: http://www.scielo.org.bo/pdf/ran/v10n3/1683-0789-ran-10-03-283.pdf?cv=1

Codina, L. (01 de 06 de 2020). CÓMO HACER REVISIONES BIBLIOGRÁFICAS TRADICIONALES O SISTEMÁTICAS UTILIZANDO BASES DE DATOS ACADÉMICAS. pág. 15. https://doi.org/https://doi.org/10.14201/orl.22977

Emvlab. (2022). *EMVLAB*. EMVLAB: https://emvlab.org/

FasterCapital. (2024). *FasterCapital.com*. https://fastercapital.com/es/tema/la-importancia-de-la-seguridad-de-los-datos-en-las-transacciones-financieras.html

García, M. (2013). El método Delphi para la consulta a expertos en la. *Revista Cubana de Salud Pública, 39(2), 253-267*, pág. 15. https://doi.org/253-267

González, M. S., Roldán, G., D'Angiolo, F. G., Y Asteasuain, F. (2021). *sedici.unlp.edu.ar*. sedici.unlp.edu.ar: https://sedici.unlp.edu.ar/handle/10915/141782

Gutierrez, N. (17 de 02 de 2022). https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Haran, J. (06 de 02 de 2023). https://prensa.ec/2022/06/22/ecuador-es-uno-de-los-paises-mas-vulnerables-para-los-ciberdelincuentes/

Harán, J. M. (14 de 10 de 2021). https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Higonet Lang, R. (2022). *API de seguridad de hardware HS-API.* https://repo.unlpam.edu.ar/handle/unlpam/8288

Ibero, J. (2023). *IberAsync*. IberAsync: https://iberasync.es/clave-simetrica-y-asimetrica/

isecom. (14 de 12 de 2010). https://www.isecom.org/OSSTMM.3.pdf

KeepCoding. (10 de 04 de 2023). *keepcoding.oi*. https://keepcoding.io/blog/que-es-blackarch-linux/

Lang, R. (8 de Abril de 2022). Hardware Security API. https://repo.unlpam.edu.ar/bitstream/handle/unlpam/8288/itg-highsa022.pdf?sequence=1&isAllowed=y

Léon, C. (02 de 05 de 2016). MÉTODO COMPARATIVO. http://eprints.uanl.mx/9943/

Lopez, A. (18 de 06 de 2023). *RZ Redes Zone*. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-.

Malagon, J. (10 de 07 de 2023). Análisis de las técnicas de ingeniería social que amenazan la seguridad informática de usuarios de entidades financieras. https://doi.org/https://repository.unad.edu.co/handle/10596/55080

Morales, M., y De la Fuente José, D. l. (2022). *www.tamps.cinvestav.mx.* https://www.tamps.cinvestav.mx/~mmorales/divulg/JD06.pdf

Morales, M., Molina de la Fuente, J., Y Héctor, D. l. (2022). *Criptografía: una tecnología antigua en aplicaciones modernas de.* https://www.tamps.cinvestav.mx/~mmorales/divulg/JD06.pdf

Pérez, J., y Merino, M. (24 de Enero de 2019). *Criptograma - Qué es, definición y concepto.* Definicion.de: https://definicion.de/criptograma/

redtrust. (2024). *redtrust*. https://redtrust.com/hsm-claves-certificados-digitales/

Rodriguez, A. (2020). Herramientas fundamentales para el hacking ético. https://doi.org/2020:12(1)116-131

Rodríguez, P. (2019). *www.revistaespacios.com*. www.revistaespacios.com: https://www.revistaespacios.com/a19v40n37/19403702.html#:~:text=Para%20Rodr%C3%ADguez%20Pe%C3%B1uelas%20(2010)%2C,pueden%20ser%20analizados%20estad%C3%ADsticamente%20para

Rubio, J. (2019). Técnicas de ciberataque y su relación con el espionaje industrial y económico. https://doi.org/https://repository.unad.edu.co/handle/10596/31843

SEPS. (2022). *www.seps.gob.ec.* www.seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

Suarez, J. L. (2020). Importancia de la seguridad informática y ciberseguridad en el mundo actual.

Utimaco. (2024). *Utimaco*. https://utimaco.com/es/servicio/ayuda/servicio-de-intercambio-y-custodia-de-llaves-keestm

WordPress. (26 de Agosto de 2023). *SEGURIDADENREDESGJA*. https://seguridadenredesgjsa.wordpress.com/criptografia/

Zelada, S., y Frank, A. (2023, 16 de Noviembre). Propuesta de diseño de un sistema de inyección de llaves criptográficas de manera remota en terminales de pago, para las empresas procesadoras de medios de pagos, utilizando el estándar PCI PIN v3.1. *Rrepositorioacademico.upc.edu.pe*, 1.

https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/672554/Zelada_SF.pdf?sequence=1&isAllowed=y

Anexos

Anexo 1: Formato de Encuesta

Encuesta

La siguiente encuesta tiene como objetivo recopilar datos sobre el conocimiento que se tiene sobre llaves criptográficas en una Institución Financiera.

Su participación nos ayudará a mejorar la seguridad y eficiencia de nuestras operaciones. No es necesario tener conocimiento previo sobre metodologías específicas para responder a esta encuesta, la información que se recopile se usaran únicamente con fines investigativos.

Gracias por su colaboración.

Cambiar de cuenta

No compartido

Sección 1: Conocimiento y Preparación

1. En una escala del 1 al 5, donde 1 es 'Nada' y 5 es 'Bastante' ¿Está familiarizado con el concepto de llaves criptográficas?

1	2	3	4	5
○	○	○	○	○

2. ¿Cual es tu conocimiento sobre el tipo de llaves criptográficas que se utilizan en una Institución Financiera, para tarjetas de débito y crédito?

- ◯ Pésima
- ◯ Mala
- ◯ Regular
- ◯ Buena
- ◯ Excelente

3. ¿Tiene conocimiento si el rol que posee un custodio de llaves criptográficas es importante?

- ◯ Muy importante
- ◯ Importante
- ◯ Neutral
- ◯ Poco importante
- ◯ Nada importante

4. En una escala del 1 al 5, donde 1 es 'Ninguna' y 5 es 'Muchas' ¿Cuantas veces ha recibido alguna capacitación en criptografía, en su lugar de trabajo?

1	2	3	4	5
◯	◯	◯	◯	◯

5. En una escala del 1 al 5, donde 1 es 'Nada' y 5 es 'Bastante' ¿Esta familiarizado con el concepto de criptograma?

1	2	3	4	5
○	○	○	○	○

6. En una escala del 1 al 5, donde 1 es 'Nada' y 5 es 'Bastante' ¿Tiene conocimiento sobre el tipo de llave criptográfica, que se utiliza para la generación del chip de las tarjetas de débito y/o crédito?

1	2	3	4	5
○	○	○	○	○

Sección 2: Percepción de Seguridad

1. En una escala del 1 al 5, donde 1 es 'Nada seguro' y 5 es 'Muy seguro', ¿cómo calificaría la seguridad actual de nuestras transacciones con tarjetas de débito y crédito?

	1	2	3	4	5	
Nada Seguro	○	○	○	○	○	Muy Seguro

2. En su opinión, ¿cuáles son los mayores riesgos asociados con la aplicación de llaves criptográficas? (Seleccione todas las ud. crea que apliquen)

- [ ] Robo de llaves
- [ ] Pérdida de llaves
- [ ] Uso indebido de llaves
- [ ] Fallos en la generacion de llaves
- [ ] Otros

3. ¿Qué tan seguro considera el proceso actual de generación de llaves criptográficas en su institución financiera?

- ○ Muy Seguro
- ○ Seguro
- ○ Neutral
- ○ Inseguro
- ○ No lo sé

4. En una escala del 1 al 5, donde 1 es 'Nada seguro' y 5 es 'Muy seguro' ¿Es seguro delegar a varios custodios los componentes, con las que se genera una llave criptográfica ?

1	2	3	4	5
○	○	○	○	○

5. ¿Considera importante la guía adecuada de llaves criptográficas para la seguridad de las transacciones?

- ○ Muy importante
- ○ Importante
- ○ Neutral
- ○ Poco Importante
- ○ Nada Importante

Sección 3: Implementación y Mejoras

1. ¿Qué factores cree que son más importantes para mejorar la aplicación de llaves criptográficas? (Seleccione todas las que apliquen)

- ☐ Capacitación del personal
- ☐ Actualización tecnológica
- ☐ Políticas y procedimientos claros
- ☐ Auditorías y monitoreo continuo
- ☐ Otros

Sección 4: Opiniones y Sugerencias

¿Tiene alguna sugerencia específica para mejorar la aplicación de llaves criptográficas en la institución?

Tu respuesta

¿Desea añadir algún comentario adicional?

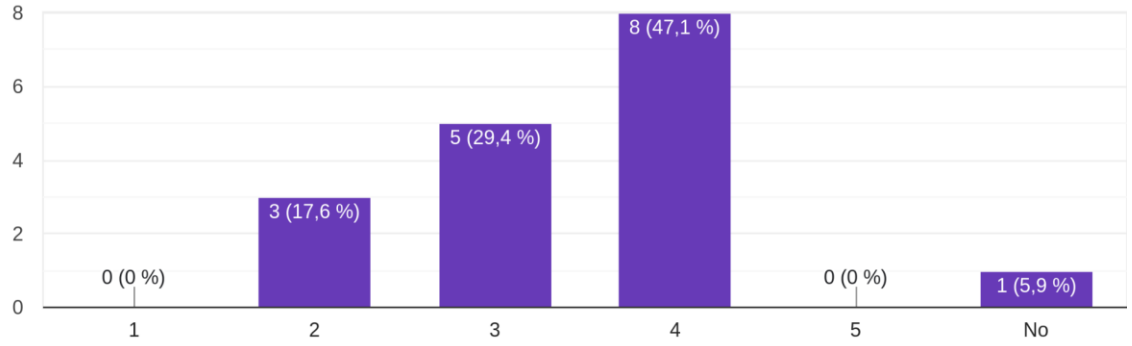
Tu respuesta

Anexo 2: Resultados de la Encuesta.

Sección 1: Conocimiento y Preparación

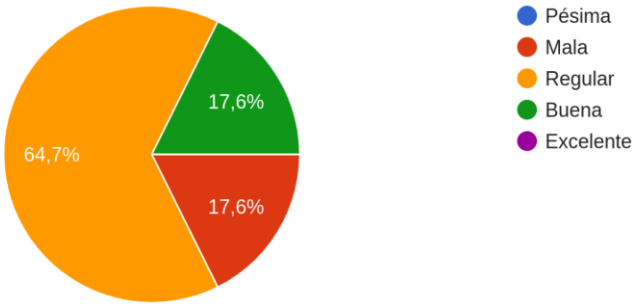
1. En una escala del 1 al 5, donde 1 es 'Nada' y 5 es 'Bastante' ¿Está familiarizado con el concepto de llaves criptográficas?

17 respuestas



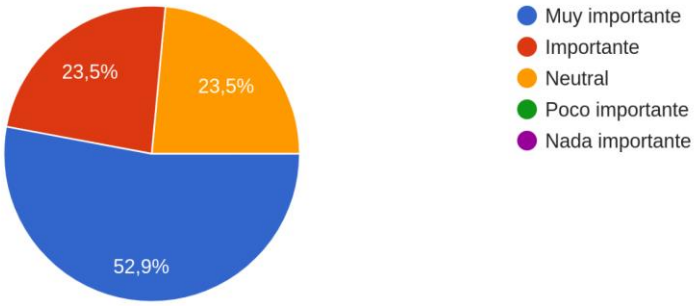
2. ¿Cual es tu conocimiento sobre el tipo de llaves criptográficas que se utilizan en una Institución Financiera, para tarjetas de débito y crédito?

17 respuestas



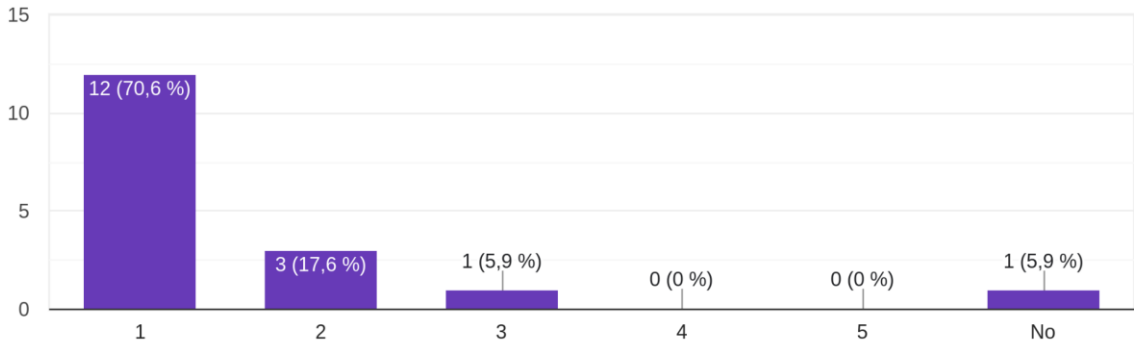
3. ¿Tiene conocimiento si el rol que posee un custodio de llaves criptográficas es importante?

17 respuestas



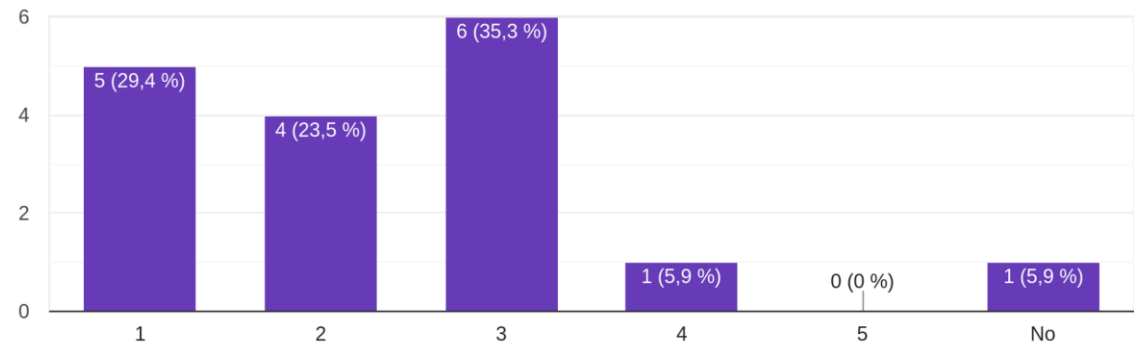
4. En una escala del 1 al 5, donde 1 es 'Ninguna' y 5 es 'Muchas' ¿Cuantas veces ha recibido alguna capacitación en criptografía, en su lugar de trabajo?

17 respuestas



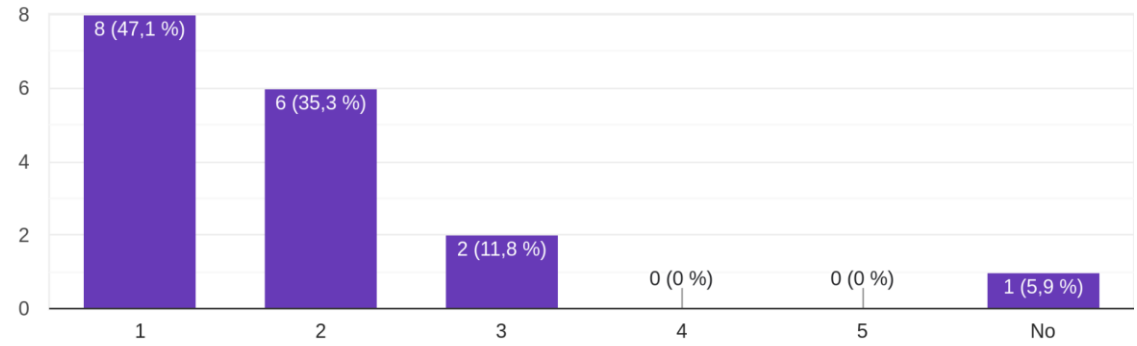
5. En una escala del 1 al 5, donde 1 es 'Nada' y 5 es 'Bastante' ¿Esta familiarizado con el concepto de criptograma?

17 respuestas



6. En una escala del 1 al 5, donde 1 es 'Nada' y 5 es 'Bastante' ¿Tiene conocimiento sobre el tipo de llave criptográfica, que se utiliza para la generación del chip de las tarjetas de débito y/o crédito?

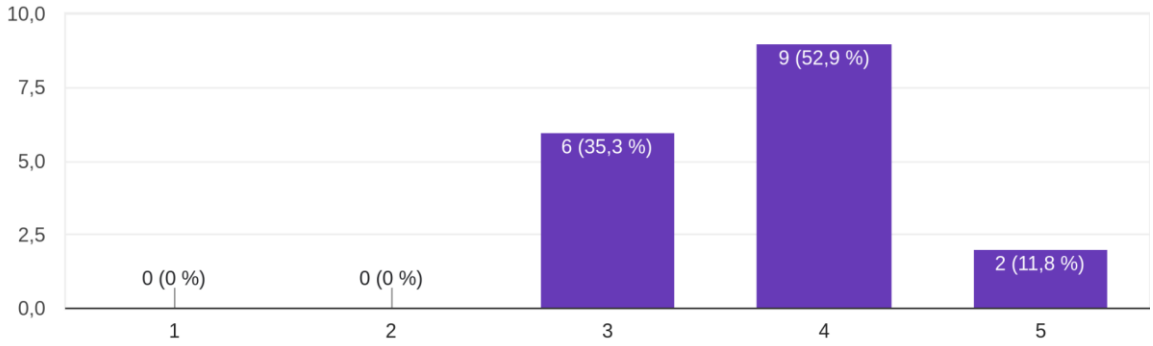
17 respuestas



Sección 2: Percepción de Seguridad

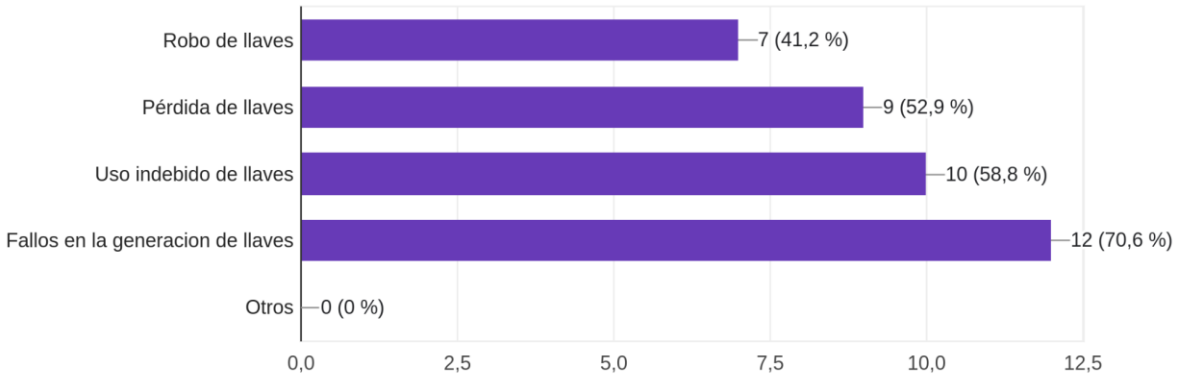
1. En una escala del 1 al 5, donde 1 es 'Nada seguro' y 5 es 'Muy seguro', ¿cómo calificaría la seguridad actual de nuestras transacciones con tarjetas de débito y crédito?

17 respuestas



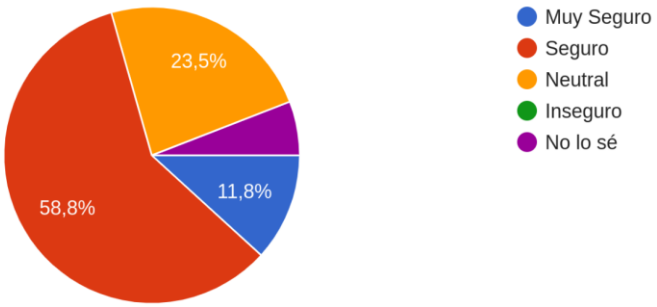
2. En su opinión, ¿cuáles son los mayores riesgos asociados con la aplicación de llaves criptográficas? (Seleccione todas las ud. crea que apliquen)

17 respuestas



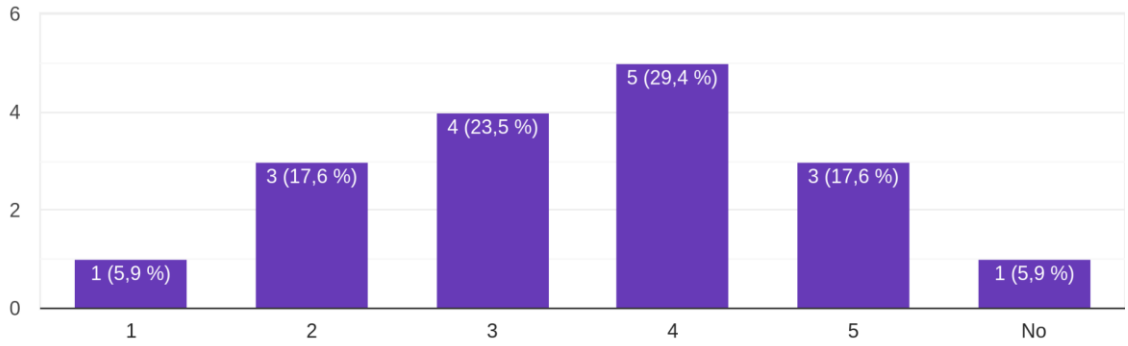
3. ¿Qué tan seguro considera el proceso actual de generación de llaves criptográficas en su institución financiera?

17 respuestas



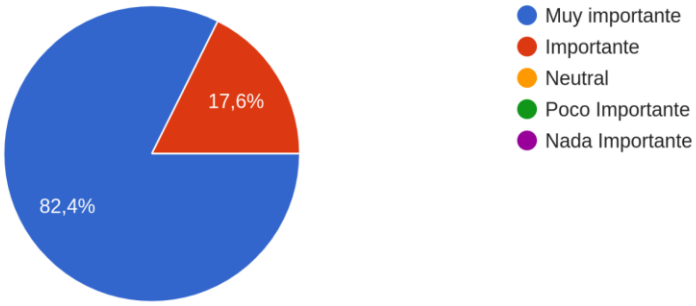
4. En una escala del 1 al 5, donde 1 es 'Nada seguro' y 5 es 'Muy seguro' ¿Es seguro delegar a varios custodios los componentes, con las que se genera una llave criptográfica ?

17 respuestas



5. ¿Considera importante la guía adecuada de llaves criptográficas para la seguridad de las transacciones?

17 respuestas

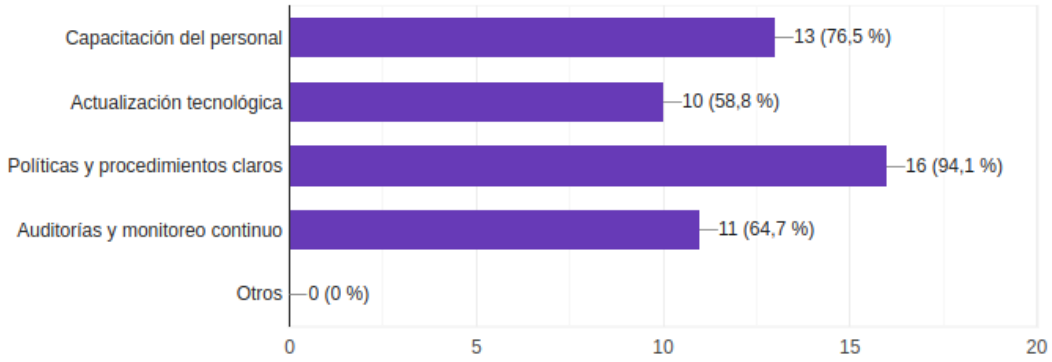


Sección 3: Implementación y Mejoras

Copiar

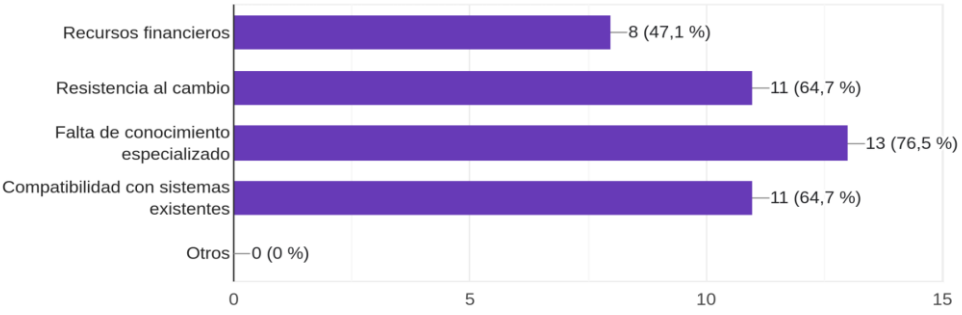
1. ¿Qué factores cree que son más importantes para mejorar la aplicación de llaves criptográficas? (Seleccione todas las que apliquen)

17 respuestas



2. ¿Cuáles cree que serían los principales desafíos en la implementación de nuevas metodologías para la gestión de llaves criptográficas? (Seleccione todas las que apliquen)

17 respuestas



Anexo 3: Guía para la aplicación de llaves criptográficas en Tarjetas CPA y Tarjetas de Crédito

GUÍA PARA LA APLICACIÓN DE LLAVES CRIPTOGRÁFICAS EN TARJETAS CPA Y TARJETAS DE CRÉDITO

Responsable: Marcelo Faicán septiembre 2024

Tabla de contenidos

INTRODUCCIÓN: ……2
OBJETIVO: ……2
CONCEPTOS BASICOS: ……3
PRINCIPALES LLAVES CRIPTOGRAFICAS: ……4
NORMAS ESTANDARES INTERNACIONALES: ……5
LISTA DE LLAVES CRIPTOGRAFICAS UTILIZADAS PARA TARJETAS CPA: ……5
LISTA DE LLAVES CRIPTOGRAFICAS UTILIZADAS PARA TARJETAS CON BANDERA: ……5
PREREQUISITOS: ……6
PASOS PARA GENERAR LOS CRIPTOGRAMAS RESULTANTES DE LAS DISTINTAS LLAVES CRIPTOGRÁFICAS PARA TARJETAS CPA Y TARJETAS CON BANDERA (VISA), EN UN HSM GEMALTO, LUNA SAFENET Y ATALLA: ……7
HSM GEMALTO: ……7
Pasos para realizar el Login en el HSM: ……7
Comandos Utilizados: ……7
Configuración para tarjetas CPA: ……7
Configuración para tarjetas VISA: ……7
HSM LUNA SAFENET: ……18
HSM ATALLA: ……20

INTRODUCCIÓN

En el contexto actual de la digitalización y el aumento de las transacciones electrónicas, la seguridad en los sistemas de pago se ha convertido en una prioridad esencial para las instituciones financieras. Las tarjetas de débito y crédito, como instrumentos fundamentales para las transacciones financieras, requieren una protección robusta contra amenazas cibernéticas y fraudes. La criptografía, en este sentido, juega un papel crucial al proporcionar mecanismos seguros para la autenticación, integridad y confidencialidad de los datos durante las transacciones.

Sin embargo, la implementación efectiva de criptografía en tarjetas de pago, como las tarjetas de débito y de crédito, depende del conocimiento que se posee para la aplicación de las llaves criptográficas involucradas en el proceso. Estas llaves, que varían según su función y aplicación, son esenciales para garantizar la seguridad en cada etapa, desde la emisión de la tarjeta hasta su uso en transacciones cotidianas.

Esta guía ha sido desarrollada con el objetivo de proporcionar un conocimiento inicial claro y accesible sobre los diferentes tipos de llaves criptográficas utilizadas en tarjetas de débito y crédito. A través de este documento, los especialistas que carecen de experiencia previa en criptografía podrán comprender el rol y la importancia de cada tipo de llave en el ecosistema de seguridad de las tarjetas. Además, la guía incluye un ejemplo práctico detallado, que ilustra cómo implementar estas llaves en un entorno real utilizando un Hardware Security Module (HSM), permitiendo a los profesionales aplicar este conocimiento de manera efectiva en sus entornos laborales.

OBJETIVO

El objetivo principal de esta guía es proporcionar un recurso comprensible y práctico para los profesionales del sector financiero y de la seguridad informática, enfocado en la aplicación de llaves criptográficas en tarjetas de débito y crédito.

CONCEPTOS BÁSICOS

Tipos de Tarjetas

- **Tarjetas CPA. -** Las tarjetas CPA son tarjetas de débito o crédito emitidas por cooperativas de ahorro y crédito. Estas tarjetas permiten a los miembros de la cooperativa acceder a sus fondos o a una línea de crédito, similar a las tarjetas emitidas por bancos tradicionales.
    - **Características Claves**
        - **Emisión Local**: Generalmente son emitidas por cooperativas locales, que ofrecen servicios financieros a sus miembros en un ámbito más restringido que los bancos comerciales.
        - **Beneficios Comunitarios**: Las tarjetas CPA suelen estar diseñadas para beneficiar a la comunidad de miembros, ofreciendo tasas de interés más bajas, menores comisiones y otros beneficios específicos para sus socios.
        - **Limitaciones Geográficas**: A menudo, su uso puede estar limitado geográficamente o tener restricciones en comparación con las tarjetas de bancos comerciales, aunque muchas cooperativas se han modernizado para ofrecer funcionalidades similares a las de las tarjetas bancarias tradicionales.
    - **Uso**
        - **Transacciones Cotidianas**: Se utilizan para retiros en cajeros automáticos, compras en puntos de venta y pagos en línea, similares a las tarjetas bancarias tradicionales.
- **Tarjetas con Bandera**: Estas son tarjetas de crédito o débito que llevan la marca (o "bandera") de una red global de pagos, como Visa, Mastercard, American Express o Discover. Estas tarjetas son emitidas por bancos o instituciones financieras, pero son aceptadas globalmente gracias a la red de la marca.
    - **Características Claves**
        - **Aceptación Global**: Una de las principales ventajas de las tarjetas con bandera es que son aceptadas en millones de establecimientos y cajeros automáticos en todo el mundo, gracias a la red global de la marca.
        - **Servicios Asociados**: Estas tarjetas suelen venir con servicios adicionales como programas de recompensas, protección contra fraudes,

seguros de viaje y otros beneficios que son proporcionados o respaldados por la red de la marca.

- **Seguridad**: Las tarjetas con bandera utilizan tecnologías avanzadas de seguridad, como EMV (Europay, Mastercard y Visa), que incluye chips integrados para reducir el fraude y aumentar la seguridad en las transacciones.

- **Uso**
  - **Transacciones Internacionales**: Se utilizan ampliamente para compras y retiros a nivel internacional, siendo una herramienta esencial para viajeros y personas que realizan transacciones fuera de su país de origen.

Criptograma

Los criptogramas son mensajes encriptados que solo pueden ser comprendidos por quienes consiguen descifrar la clave correspondiente.

Códigos de Verificación de Claves (KVC)

Un Código de Verificación de Clave (KVC) se utiliza para verificar, sin comprometer el secreto, que una clave o un componente de clave se ha ingresado correctamente o para confirmar que el valor de una clave almacenada es el esperado.

PRINCIPALES LLAVES CRIPTOGRÁFICAS

Entre las principales llaves criptográficas para la aplicación en tarjetas CPA y de crédito se tiene las siguientes:

- **MK (Master Key):** Llave maestra usada para derivar otras llaves.
- **KIR (Key Identification Response): S**e usa para probar la identidad de otras claves.
- **CVV/CVV2 (Card Verification Value):** Códigos de seguridad para validar transacciones.
- **iCVV (Integrated Card Verification Value):** Similar al CVV, pero usado internamente.
- **PVV (PIN Verification Value):** Llave usada para verificar el PIN.
- **DPK (Data Protection Key):** Llave para proteger la integridad de los datos.
- **IMKAC IMKSMC, IMKSMI**: Para la gestión EMV.
- **PPK (KEK), KIS, KIR:** Son llaves de transporte utilizadas para enviar tanto pines cifrados como llaves de un sitio a otro, conocidas también como llaves **ZCMK.**

- **KTM**: Llaves de terminal que van en los terminales de pago, atms o POS.
- **PVK3624** Se utilizan para validar los pines de las tarjetas en una transacción.
- **DPK (Data Protection Key):** Para cifrar datos sensibles que se deben almacenar o transmitir de forma segura
- **PEK (Pin Encryption Key):** Esta llave cifrar y proteger los números de identificación personal (PIN).
- **IWK (Issuer Working Key):** Se utilizan para crear llaves de cifrado de PIN, llaves de autenticación de mensajes, o llaves de sesión para transacciones individuales.

NORMAS Y ESTÁNDARES INTERNACIONALES

- **PCI DSS (Payment Card Industry Data Security Standard):** Requisitos para la protección de datos de tarjeta.
- **EMV (Europay, MasterCard, and Visa):** Estándares para transacciones con tarjeta usando chips.

LISTA DE LLAVES CRIPTOGRÁFICAS UTILIZADAS PARA TARJETAS CPA

- KIR
- PEK
- DAT
- PPK
- CVV
- CVV2
- iCVV
- PVK
- PVV
- IMKAC

LISTA DE LLAVES CRIPTOGRÁFICAS UTILIZADAS PARA TARJETAS CON BANDERA

- IWK
- CVV
- CVV2
- iCVV
- ZCMK

- IMKAC
- PVV
- PVK

PREREQUISITOS

Antes de proceder con la implementación de las llaves criptográficas en tarjetas CPA y de crédito, es fundamental asegurarse de que se cuenta con todos los componentes necesarios para la generación de estas llaves. Estos componentes deben ser coordinados y acordados entre la institución financiera y la red de pagos con la que se está trabajando.

Específicamente, se requiere lo siguiente:

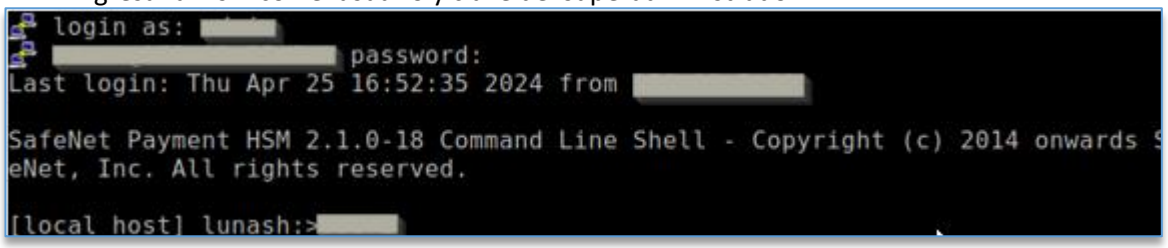
1. **Componentes de Llave Criptográfica**:
    - Cada llave criptográfica que se utilizará en el proceso debe estar compuesta por uno o más componentes criptográficos, los cuales pueden estar en forma de claves parciales que, al combinarse, forman la llave completa.
    - Estos componentes pueden ser generados por la institución financiera, la red de pagos, o una combinación de ambos, dependiendo de las políticas de seguridad y acuerdos específicos.
2. **Acuerdo entre las Partes Involucradas**:
    - Es necesario que exista un acuerdo formal entre la institución financiera y la red de pagos que defina claramente cómo se generarán, manejarán, y compartirán estos componentes criptográficos.
    - Dicho acuerdo debe incluir procedimientos para la distribución segura de los componentes, así como los métodos para combinarlos dentro del Hardware Security Module (HSM).
3. **Almacenamiento Seguro de Componentes**:
    - Los componentes criptográficos deben ser almacenados de manera segura tanto en la institución financiera como en la red de pagos, garantizando que no puedan ser accedidos o comprometidos por terceros no autorizados.
    - Se recomienda que estos componentes sean almacenados en dispositivos seguros, como HSMs, y que su transferencia entre partes se realice bajo estrictos protocolos de seguridad.

PASOS PARA GENERAR LOS CRIPTOGRAMAS RESULTANTES DE LAS DISTINTAS LLAVES CRIPTOGRÁFICAS PARA TARJETAS CPA Y TARJETAS CON BANDERA (VISA), EN UN HSM GEMALTO, LUNA SAFENET Y ATALLA.

HSM GEMALTO

PASOS PARA REALIZAR EL LOGIN EN EL HSM

- Ingresar al hsm con el usuario y clave del superadministrador



El usuario es **xxxx**, la contraseña es **xxxxxxxxxxx.**

- Ingresar los tokens de color negro en el HSM y ejecutar el comando: login partitionOwner -partition “Ingresar el nombre de la partición que se tenga identificado en el HSM”.

- Se ingresa el primer usuario y la contraseña, luego de esto se ingresa el segundo usuario y la contraseña

COMANDOS UTILIZADOS

Para la generación de las llaves criptográficas se utilizan comando,s los cuales se listan a continuación:

keymgmt generate host encrypted "Tipo de llave a generar": Este comando indica que el HSM debe generar una nueva llave, por ejemplo, DPK, un Derived Pin Key (DPK). El DPK es comúnmente utilizado en sistemas de procesamiento de pagos para cifrar PINs de tarjetas de débito o crédito.

keyspec 11: El especificador de llave "11" Identifica el tipo y propósito de la llave que se está generando.

clearcomp 2: Indica que se están utilizando dos componentes en claro (sin cifrar) para formar la llave. En el manejo de llaves, a menudo se combinan múltiples componentes para formar una llave final, como una medida de seguridad adicional.

encryptedcomp 0: Señala que no se están utilizando componentes cifrados en la formación de la llave. Esto significa que todos los componentes involucrados son transparentes (en claro) para el proceso.

algo DES: Especifica que el algoritmo de cifrado utilizado para la generación de la llave es DES (Data Encryption Standard), un algoritmo criptográfico conocido por ser utilizado en muchos sistemas bancarios y financieros.

keylen 2: Esto indica que la longitud de la llave es doble. En el contexto de DES, que normalmente tiene una longitud de clave de 56 bits, esto podría implicar que se está utilizando una variante como el Triple DES, que usa una llave más larga para seguridad adicional, aunque normalmente se esperaría una clave de longitud 3 para Triple DES. Es importante verificar la documentación específica para detalles exactos.

eIndex 1: Se refiere a un índice de clave dentro del HSM, especificando dónde o cómo se debe almacenar o gestionar la clave generada. El número "1" es un identificador para ese almacenamiento específico o configuración de manejo.

p RANDOM: Indica que el proceso de generación de la llave debe utilizar una fuente de entropía aleatoria para asegurar que la llave generada sea única y segura.

encryptedMode ECB: Especifica que el modo de cifrado para operaciones que utilizan esta llave es ECB (Electronic Codebook). ECB es un modo de operación simple para algoritmos de cifrado en bloque, aunque es menos seguro en comparación con otros modos porque no introduce variabilidad en el cifrado de bloques de datos idénticos.

CONFIGURACIÓN PARA TARJETAS CPA

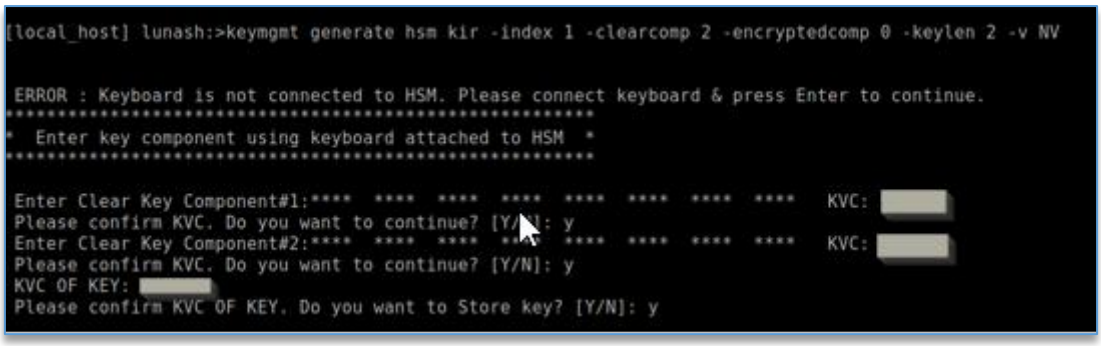
LLAVE KIR

La llave es Ingresada en el HSM en el índice “1”, se debe considerar que se toma el valor referencial de 1 ya que este HSM no tiene configurado ninguna información y se empezara desde el inicio todas las configuraciones. Con los componentes que se tiene documentado en el proceso de entrega de componentes entre la entidad financiera y la red de pagos, se procede a generar los criptogramas resultantes.

Cabe indicar que las únicas llaves que se ingresan en el HSM son las llaves de transporte como es este el caso, las demás llaves se tienen que generar criptogramas resultantes los cuales se enviaran a la red de pagos con la que se este realizando el intercambio de información de las llaves.

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



KVC RESULTANTE: XXXXXX

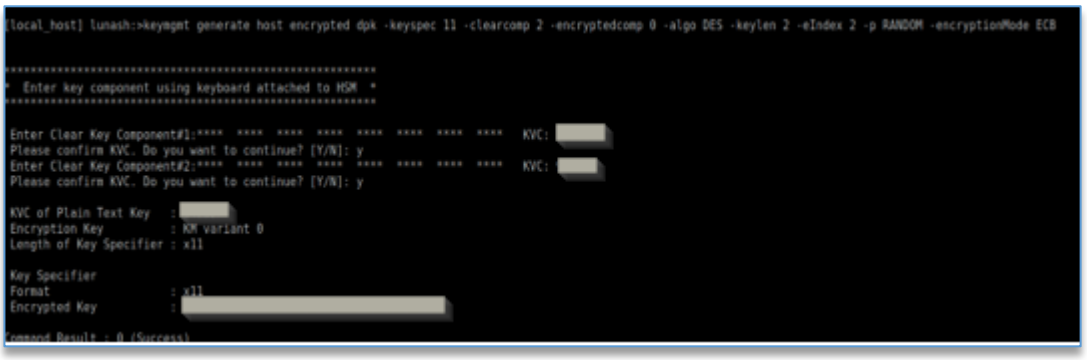
LLAVES DPK

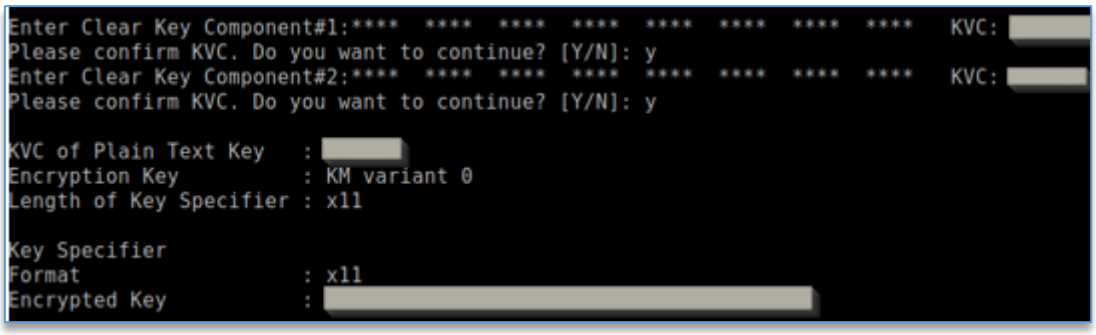
Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

KVC XXXXXX





Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

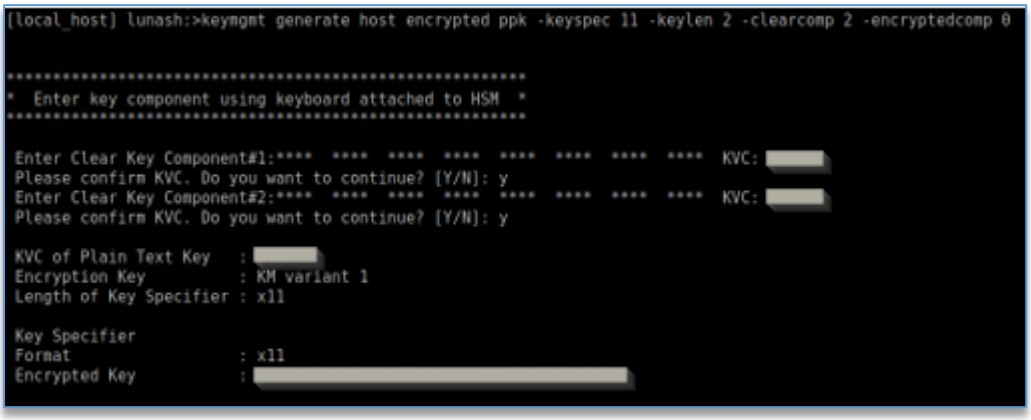
KVC:XXXXXX

LLAVE PEK EN EL HSM ES PPK

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

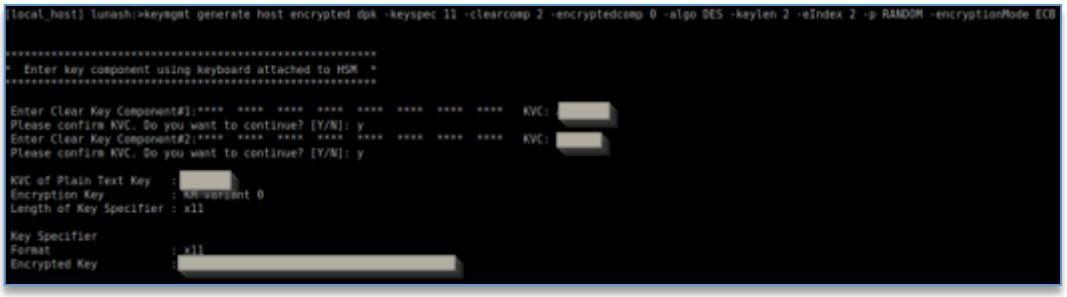
KVC:XXXXXX

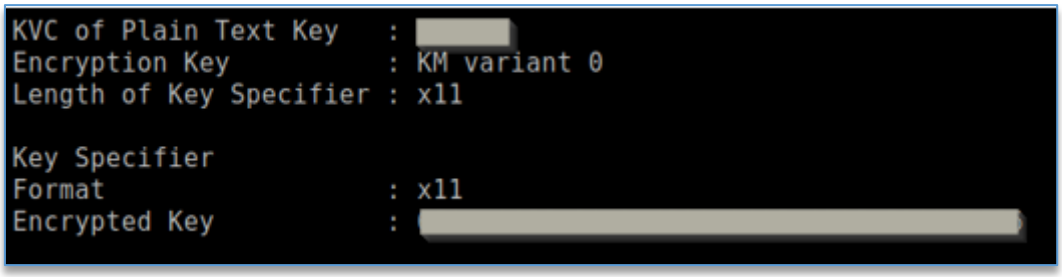
LLAVE DAT

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX





Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

LLAVES (PPK)

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

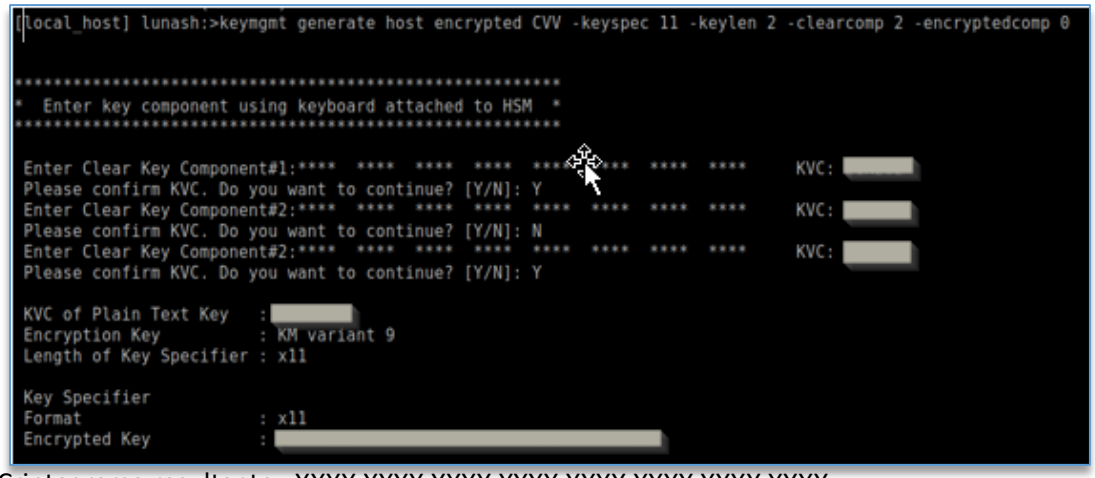
KVC:XXXXXX

LLAVES CVV

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

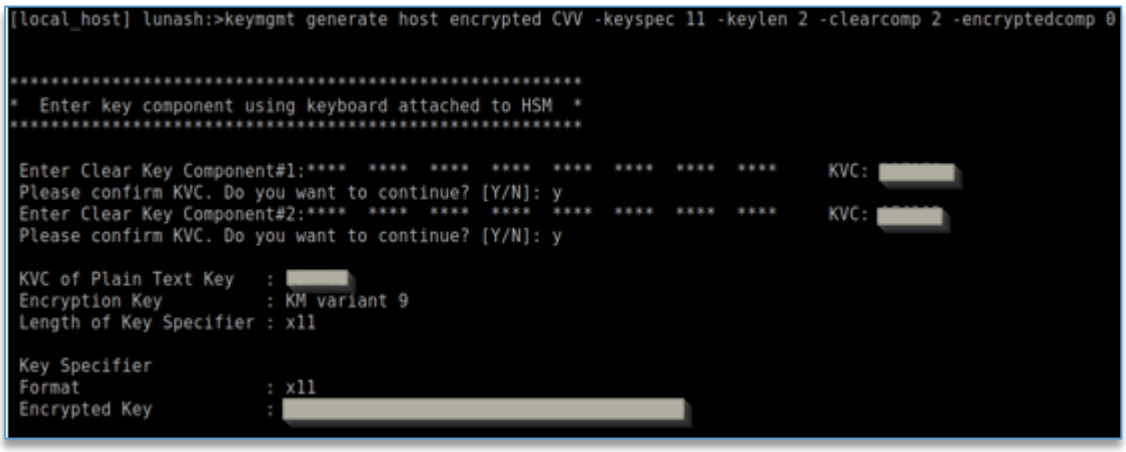
KVC:XXXXXX

LLAVE CVV2

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

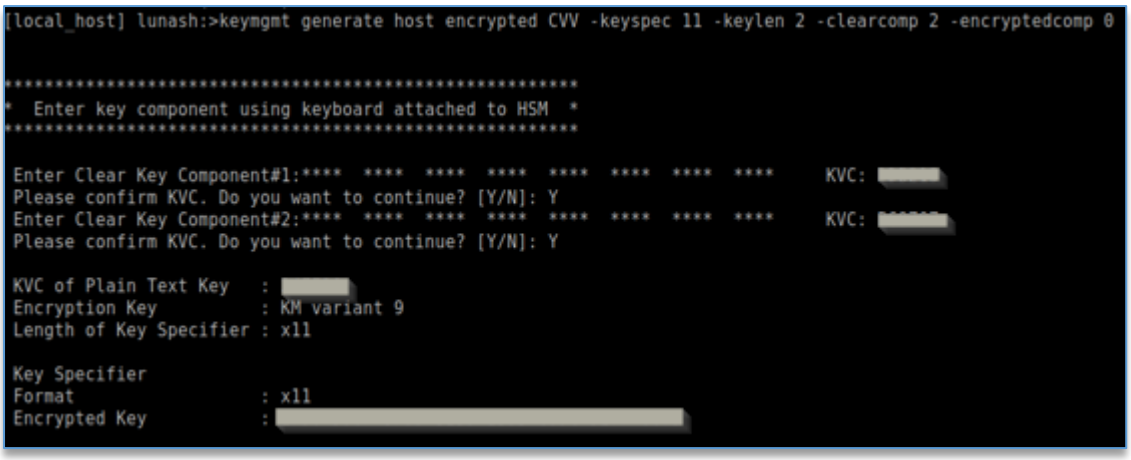
KVC:XXXXXX

LLAVE ICVV

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

LLAVE PVK (TIPO DPK)

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

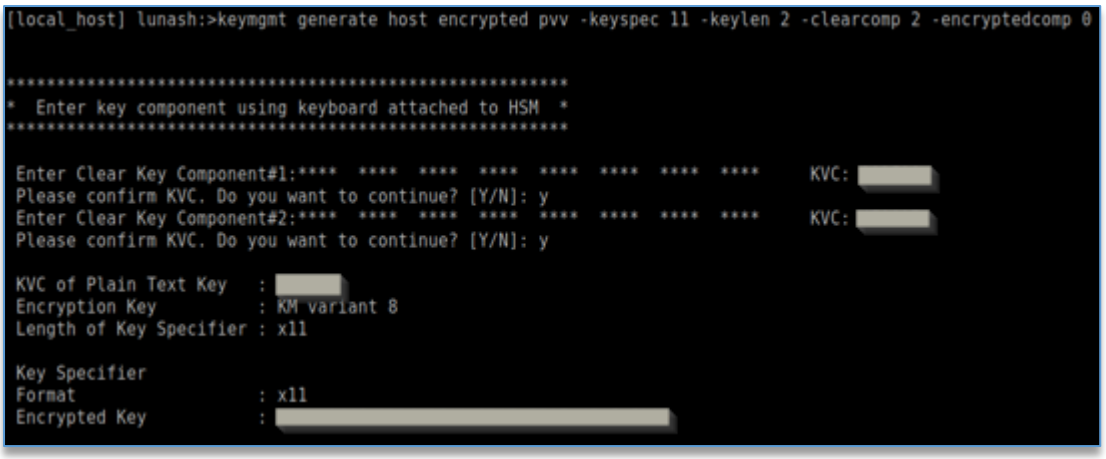
KVC:XXXXXX

LLAVE PVV

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

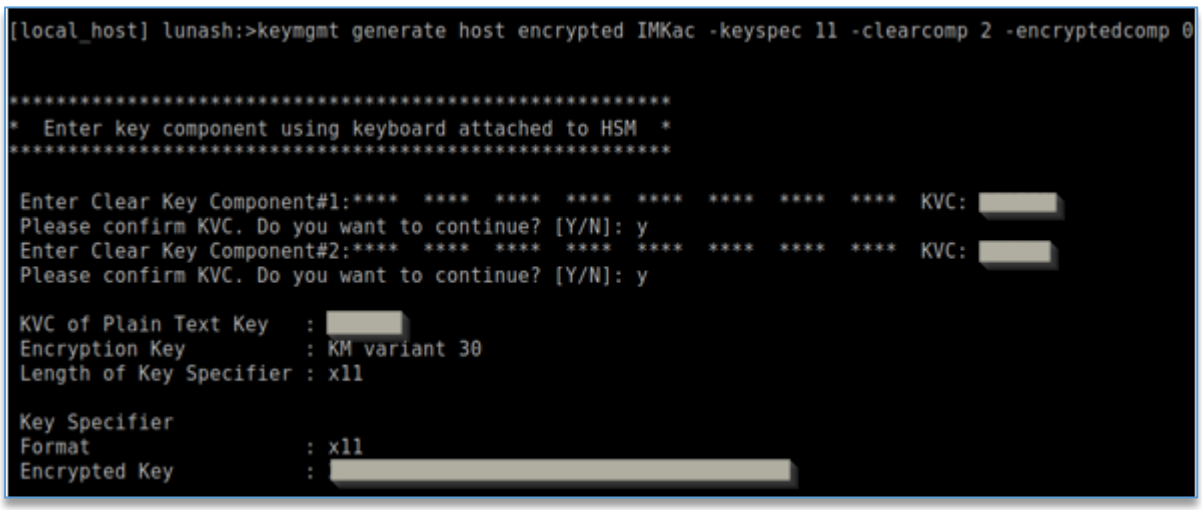
KVC:XXXXXX

LLAVE IMKAC

Estos componentes son ingresados en el HSM en el Índice 1

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

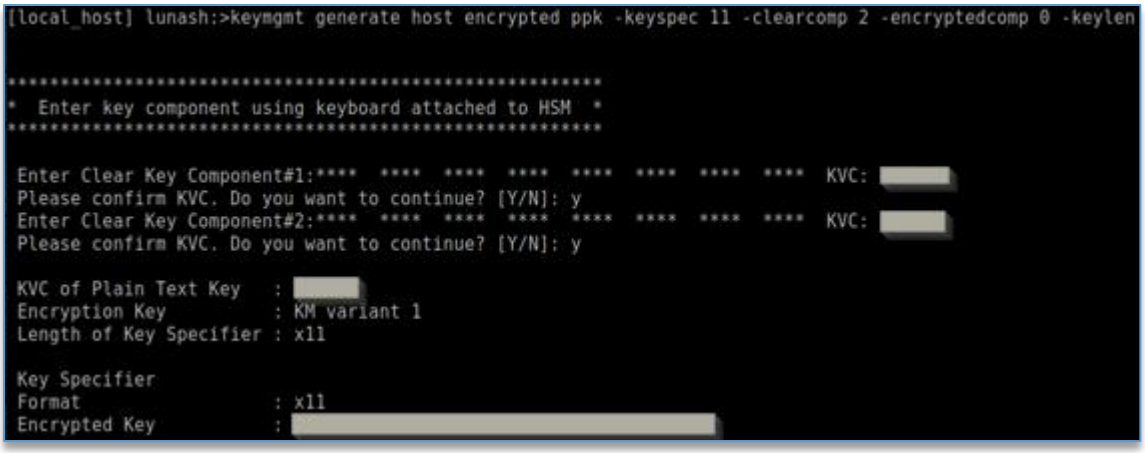
CONFIGURACIÓN PARA TARJETAS VISA

LLAVE IWK(MODO PPK)

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

LLAVE CVV

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

```
[local_host] lunash:>keymgmt generate host encrypted cvv -keyspec 11 -clearcomp 2 -encryptedcomp 0 -keylen 2


*****************************************************
*  Enter key component using keyboard attached to HSM  *
*****************************************************

 Enter Clear Key Component#1:****  ****  ****  ****  ****  ****  ****  ****     KVC: 0D11C5
 Please confirm KVC. Do you want to continue? [Y/N]: y
 Enter Clear Key Component#2:****  ****  ****  ****  ****  ****  ****  ****     KVC: 3AAF31
 Please confirm KVC. Do you want to continue? [Y/N]: y

 KVC of Plain Text Key   : 406007
 Encryption Key          : KM variant 9
 Length of Key Specifier : x11

 Key Specifier
 Format                  : x11
 Encrypted Key           : AC6C 5A40 F5C8 3323 CBB4 292B 4E4A 6CE3
```

Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

LLAVE ZCMK (TRANSPORTE)

Se realiza el ingreso de llave ZCMK en el HSM, Índice 2

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP3: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

```
[local_host] lunash:>keymgmt generate hsm kir -index 2 -clearcomp 3 -encryptedcomp 0 -keylen 2 -variantscheme NV


*****************************************************
*  Enter key component using keyboard attached to HSM  *
*****************************************************

 Enter Clear Key Component#1:****  ****  ****  ****  ****  ****  ****  ****   KVC:
 Please confirm KVC. Do you want to continue? [Y/N]: y
 Enter Clear Key Component#2:****  ****  ****  ****  ****  ****  ****  ****   KVC:
 Please confirm KVC. Do you want to continue? [Y/N]: y
 Enter Clear Key Component#3:****  ****  ****  ****  ****  ****  ****  ****   KVC:
 Please confirm KVC. Do you want to continue? [Y/N]: y
 KVC OF KEY:
 Please confirm KVC OF KEY. Do you want to Store key? [Y/N]: y

Command Result : 0 (Success)
```

Combined ZCMK Clear: **XX XX XX**

LLAVE IMKAC

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

```
[local_host] lunash:>keymgmt generate host encrypted imkac -keyspec 11 -clearcomp 2 -encryptedcomp 0


*******************************************************
*  Enter key component using keyboard attached to HSM  *
*******************************************************

 Enter Clear Key Component#1:****  ****  ****  ****  ****  ****  ****  ****  KVC: 91B6EE
 Please confirm KVC. Do you want to continue? [Y/N]: y
 Enter Clear Key Component#2:****  ****  ****  ****  ****  ****  ****  ****  KVC: 1EBF66
 Please confirm KVC. Do you want to continue? [Y/N]: y

 KVC of Plain Text Key   : F90060
 Encryption Key          : KM variant 30
 Length of Key Specifier : x11

 Key Specifier
 Format                  : x11
 Encrypted Key           : 9675 9B5B 71B8 BF1E 3028 26B7 34E5 E6EF
```

Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

LLAVE PVV

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

```
[local_host] lunash:>keymgmt generate host encrypted PVV -keyspec 11 -clearcomp 2 -encryptedcomp 0 -keylen 2


*******************************************************
*  Enter key component using keyboard attached to HSM  *
*******************************************************

 Enter Clear Key Component#1:****  ****  ****  ****  ****  ****  ****  ****     KVC:
 Please confirm KVC. Do you want to continue? [Y/N]: y
 Enter Clear Key Component#2:****  ****  ****  ****  ****  ****  ****  ****     KVC:
 Please confirm KVC. Do you want to continue? [Y/N]: y

 KVC of Plain Text Key   :
 Encryption Key          : KM variant 8
 Length of Key Specifier : x11

 Key Specifier
 Format                  : x11
 Encrypted Key           :
```

Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

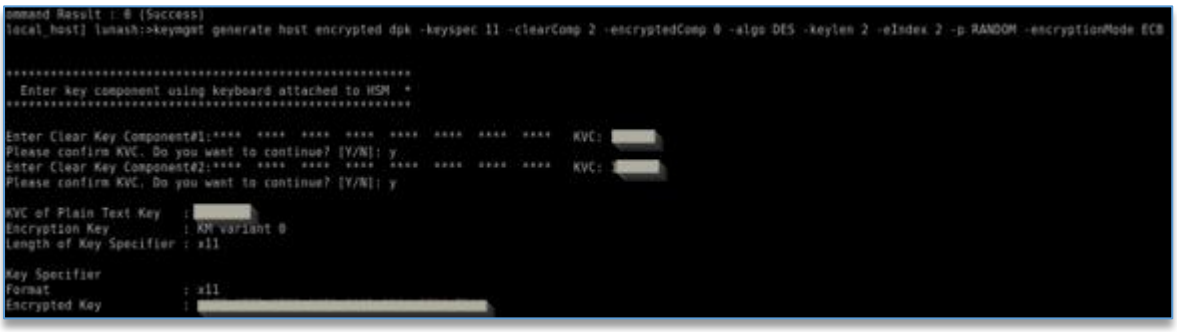
KVC:XXXXXX

LLAVE PVK(TIPO DPK)

Generación de Criptograma

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX

COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXXXX



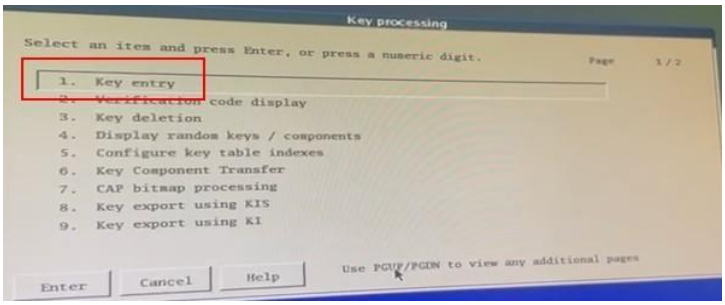
Criptograma resultante: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

KVC:XXXXXX

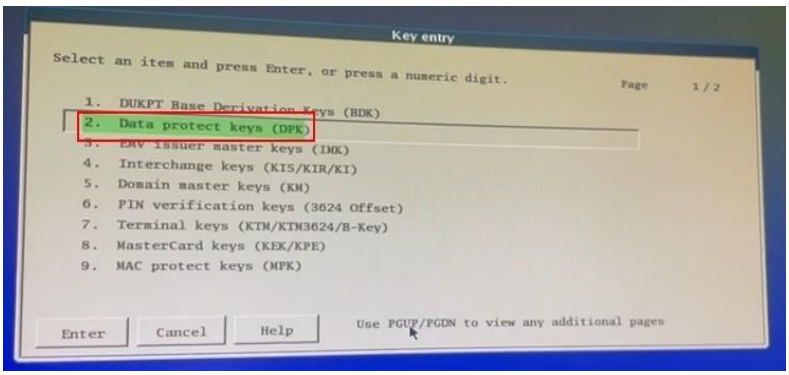
HSM LUNA SAFENET

LLAVE DPK

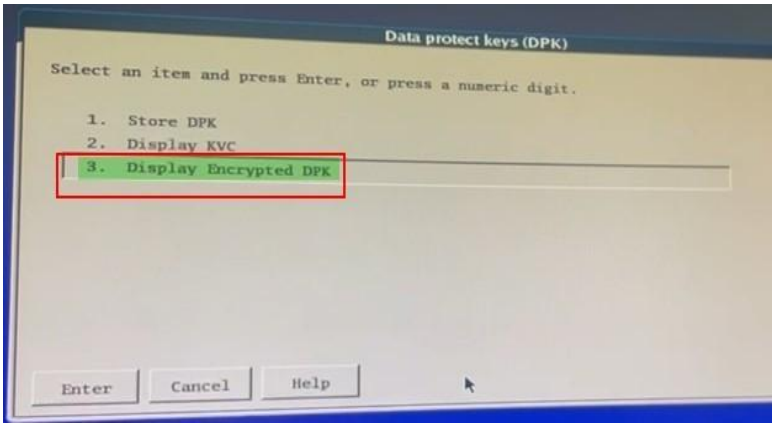
1.- Se ingresa a Key Proccesing → Key Entry



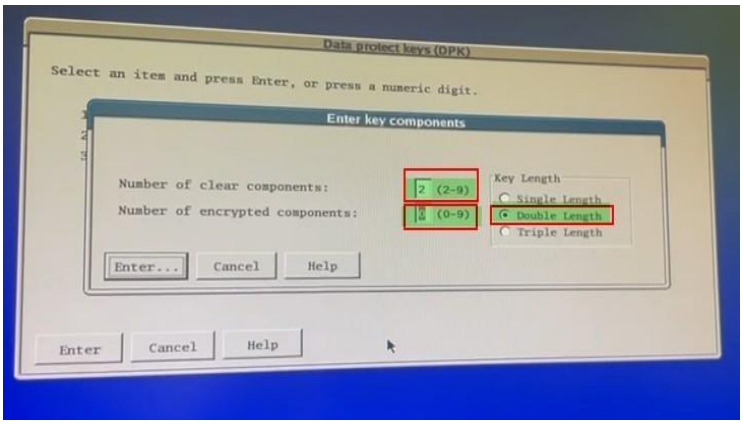
2.- Ingresamos a Data Protect Keys (DPK)



3.- Seleccionamos la opción de Display Encrypted DPK

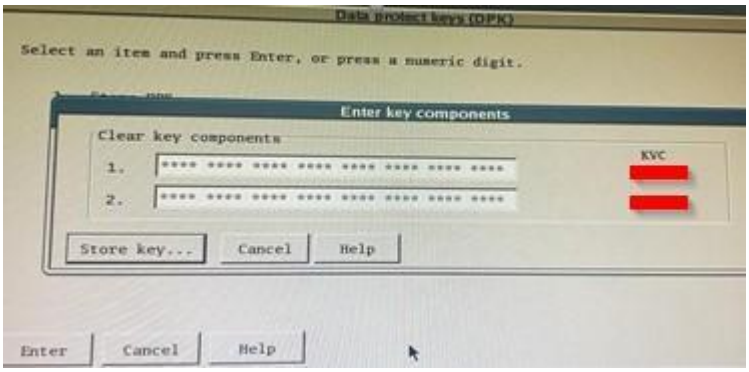


4.- Se debe ingresar los iguientes datos:
Number of clear components: **2**
Number of encrypted components: **0**
KeyLength: **Double Length**

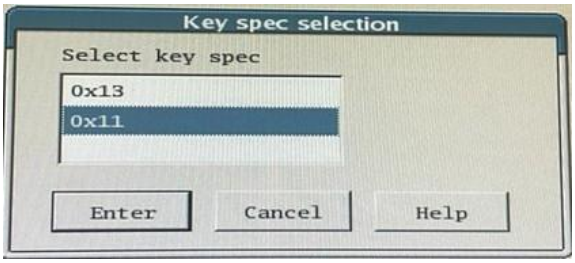


5.- Se genera el criptograma que se ingresará en el switch transaccional.

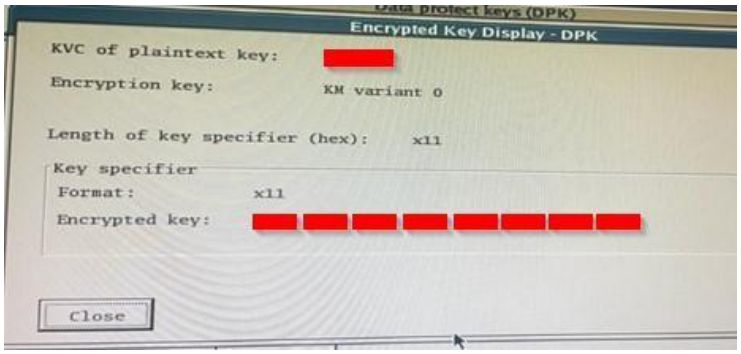
COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXX
COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXX



6.- En Key spec selection se selecciona la opción **0x11**



A continuación, se genera el criptograma resultante:



Nota: Se realiza el mismo procedimiento para todas las llaves que se vayan a configurar.

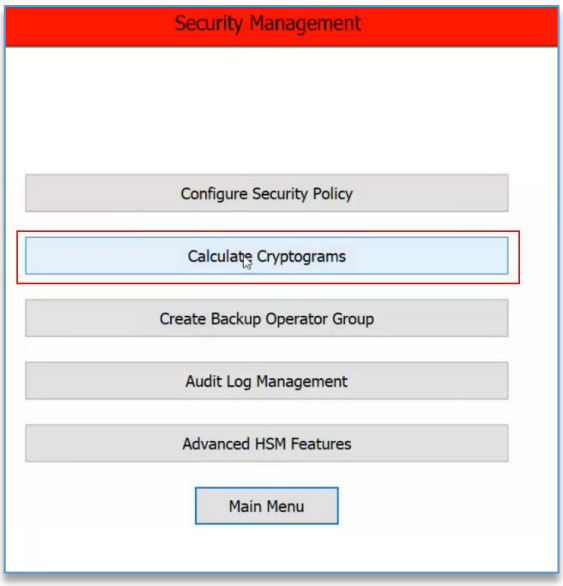
HSM ATALLA

Para realizar la generación de componentes resultantes en el HSM Atalla, se realiza el siguiente procedimiento.

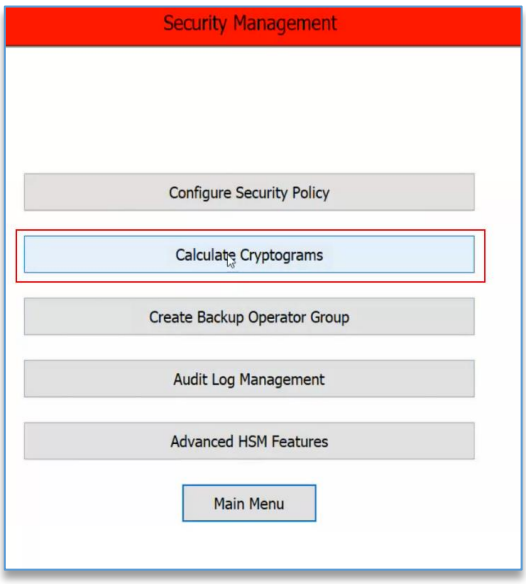
Se debe ingresar sesión con la tarjeta administrador para poder realizar este proceso, generalmente se configura tres tarjetas administradoras, para que con dicha autenticación se pueda acceder a la configuración que se necesita realizar.

Ahora ingresamos a la opción de Security Management

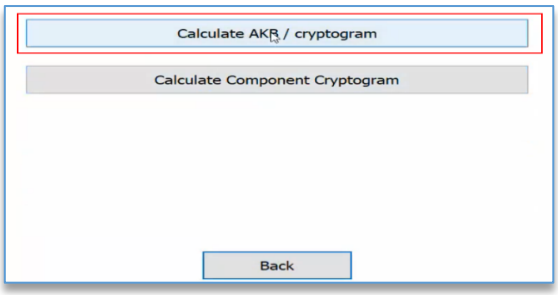
Click en Calculate Cryptograms



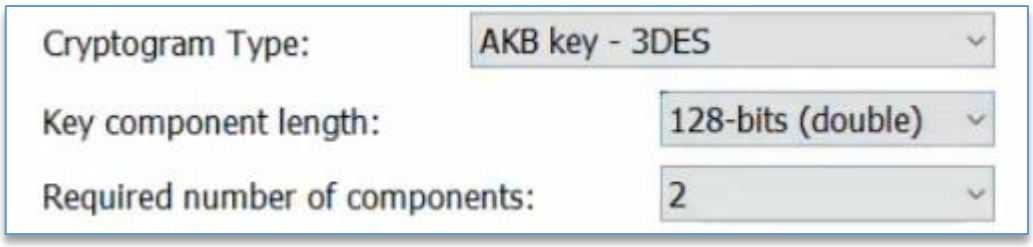
Click en Calculate Cryptograms



Click en Calculate AKB / cryptogram.



Se realiza la configuración, para el tipo de criptografía va a tener los componentes

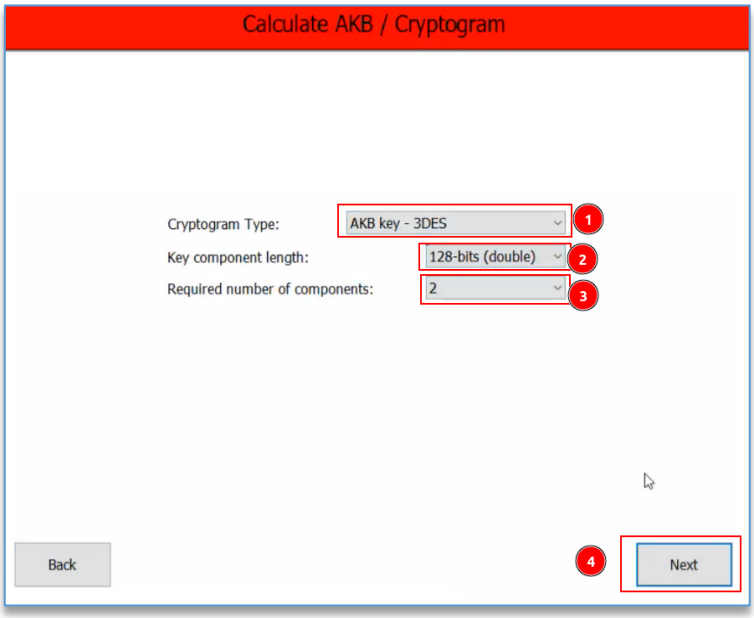


En esta parte se aplica lo siguiente:

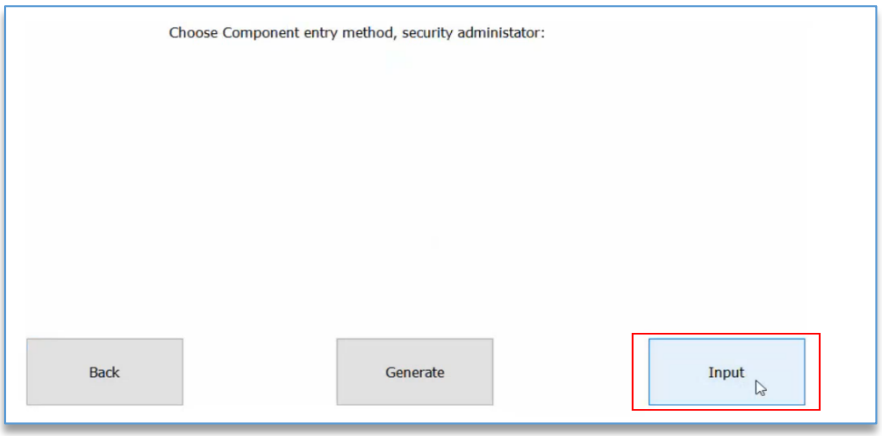
El tipo de criptograma: 3DES

El tamaño del componente será de tamaño doble.

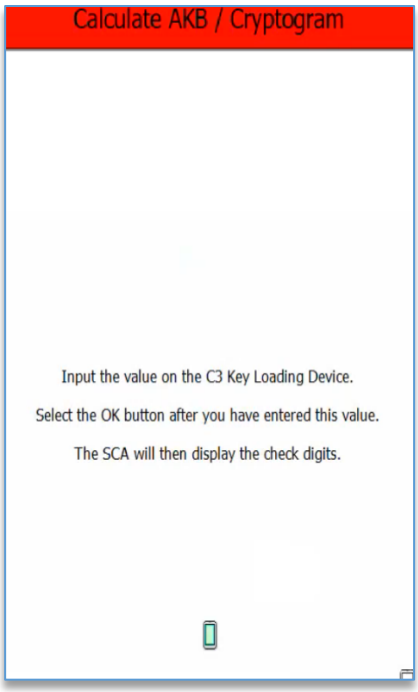
Componentes Requeridos: 2



Click en Input.



Ahora nos indica que se ingrese los componentes en el dispositivo C3.



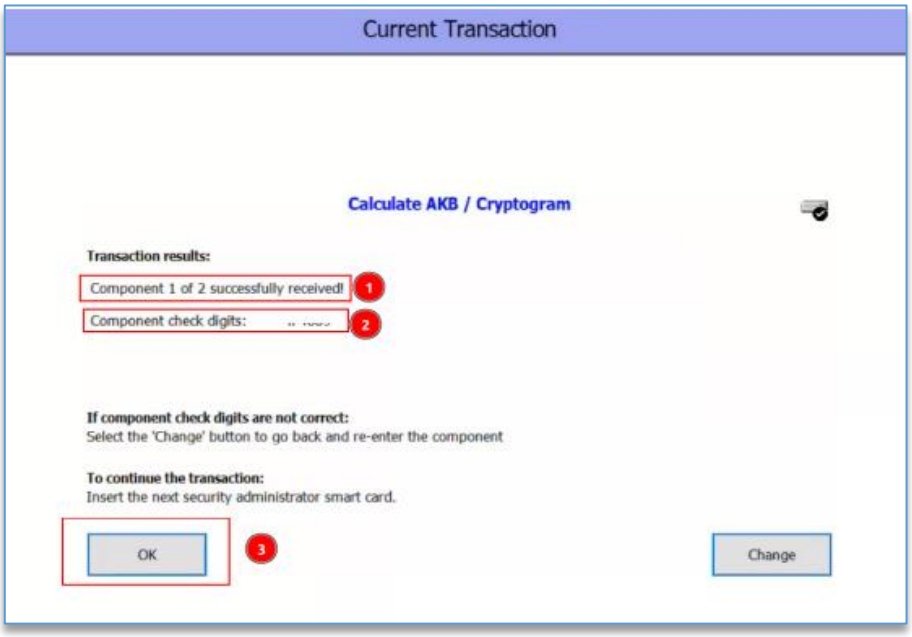
Para este ejemplo se va a utilizar los componentes de la llave PVK.

Entonces ingresamos los componentes en el dispositivo C3.

COMP1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXX
COMP2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX KVC XXXX

En la siguiente pantalla nos visualiza lo siguiente: Se ha recibido satisfactoriamente 1 de 2 componentes.

Se debe validar el dígito verificador.

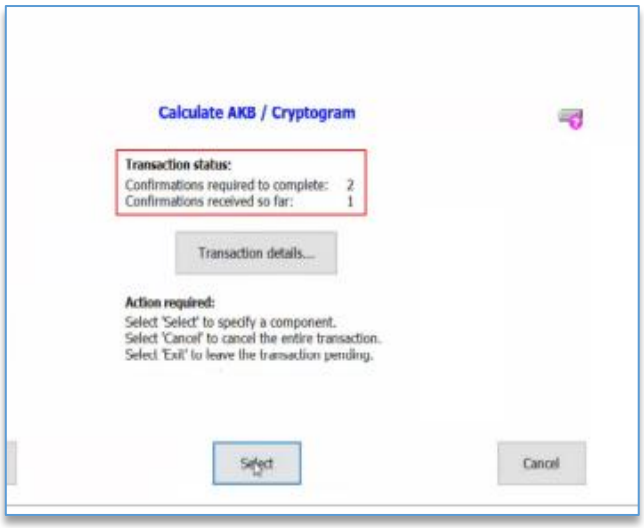


Si el dígito verificador no coincide se da click en Change para volver a ingresar el componente, en este caso sí coincide el dígito verificador por lo que se procede a dar click en Ok.

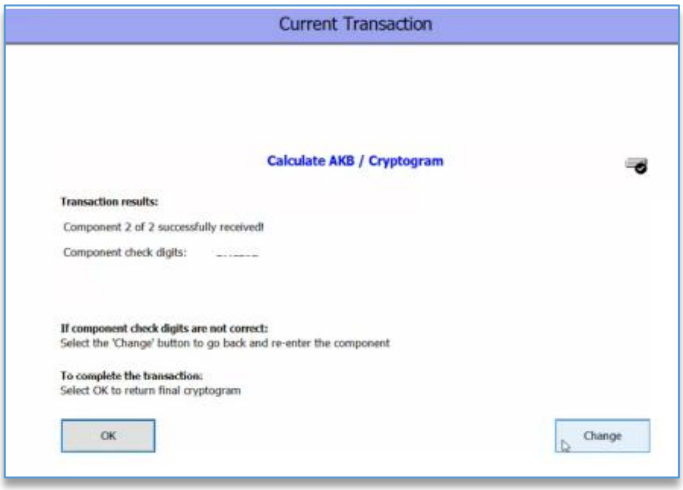
Ahora se procede a retirar la tarjeta Administrador que se esté utilizando y se inserta la siguiente tarjeta Administrador, se lo realiza de esta forma ya que al realizar la Asociación de las tarjetas en una configuración inicial del HSM se configura tres tarjetas administradoras, de preferencia para realizar cualquier proceso de configuración en el HSM.

Se necesita por los menos dos de las tarjetas administradoras que realicen esta actividad, es por esto que nos presenta el mensaje que se tiene ingresado un componente de los dos componentes a ingresar.

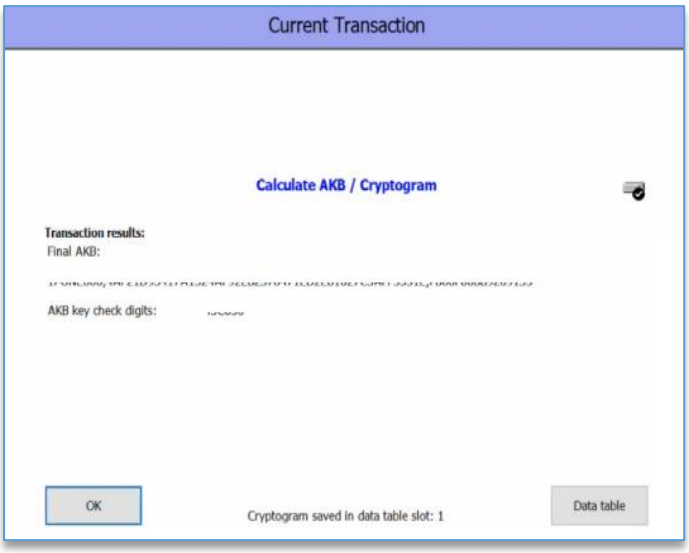
Nos aparece automáticamente la siguiente pantalla y procedemos a dar click en Select, para ingresar el segundo componente.



Ahora se repite el proceso de ingreso del segundo componente en el dispositivo C3.



Por último, se nos presenta el AKB resultante



Anexo 4: Validación de especialistas.

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Enrique Leonardo Jimbo Landi
Título obtenido: Ingeniero de Sistemas /Magister en Tecnologías de la Información
C.I.: 0104672712
E-mail: e.jimbo@jardinazuayo.fin.ec
Institución de Trabajo: COAC Jardín Azuayo Ltda.
Cargo: Especialista en Centro de Datos
Años de experiencia en el área: 16 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	35				

Observaciones: La guía propuesta es un recurso clave para las instituciones financieras, ya que mejora la comprensión de la criptografía y los criterios de seguridad en la implementación y operación de tarjetas de débito y crédito, y puede servir como base para desarrollar servicios más seguros en el futuro.

Recomendaciones: Se recomienda aplicar la guía propuesta en este estudio, asegurando la socialización y capacitación de todas las personas involucradas en la implementación y operación de tarjetas de débito y crédito, así como de aquellas responsables de los procesos de mejora continua, innovación y desarrollo de servicios.

Lugar, fecha de validación: Cuenca, 28 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

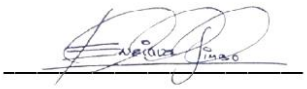
En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



Firma del especialista
Ing. Enrique Jimbo L. Mg

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Byron Javier Molina Quishpe
Título obtenido: Ingeniero en Sistemas Informáticos
C.I.: 17152158592
E-mail: bmolina@prosupply.ec
Institución de Trabajo: Proveedor de Tecnología PROSUPPLY SA.
Cargo: Especialista en Manejo y Administración Cajas Criptográficas HSM
Años de experiencia en el área: 15 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	35				

Observaciones: No se presentan observaciones, más bien la guía presentada es un recurso valioso para las instituciones financieras, ya que ofrece una comprensión general de las llaves criptográfica, esenciales para la implementación de tarjetas de débito y crédito

Recomendaciones: Para llevar a cabo una implementación efectiva de llaves criptográficas en tarjetas de débito y crédito, se recomienda seguir esta guía, ya que proporciona un punto de partida claro y enfocado para adquirir los conocimientos necesarios y desarrollar un proyecto relacionado con tarjetas de pago y tarjetas de débito

Lugar, fecha de validación: Cuenca, 28 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Prosupply
RUC. 1792[illegible]333001

Firma del especialista
Ing. Byron Molina

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Paúl Zhañay Ledesma
Título obtenido: Magister en Seguridad Informática
C.I.: 0102807807
E-mail: h.zhanay@jardinazuayo.fin.ec
Institución de Trabajo: COAC Jardín Azuayo
Cargo: Responsable de Seguridad Informática
Años de experiencia en el área: 7

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Universidad Israel
ESPOG | Escuela de Posgrados

Tema: "Guía para la Aplicación de Llaves Criptográficas en Tarjetas CPA y de Crédito"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad	**X**				
Novedad	**X**				
Fundamentación pedagógica	**X**				
Fundamentación tecnológica	**X**				
Indicaciones para su uso	**X**				
TOTAL	**35**				

Observaciones:

La aplicación de llaves criptográficas es crucial para mantener la seguridad y confianza durante las transacciones con tarjeta. La presente guía es de mucha ayuda ya que establece los pasos que deben aplicarse durante el proceso de obtención de criptogramas resultantes con el objetivo de proteger los datos y las transacciones de posibles fraudes y ataques, garantizando así un entorno seguro para los usuarios.

Recomendaciones:

Los pasos descritos en la presente guía están establecidos con marcas reconocidas y utilizadas por su tecnología. Sin embargo, es importante conforme se actualiza la tecnología analizar y actualizar de ser el caso la presente guía para garantizar el procedimiento a seguir y los tipos de llaves a utilizar.

Lugar, fecha de validación: Cuenca, 30 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firmado electrónicamente por:
HENRY PAUL
ZHANAY LEDESMA

Firma del especialista
Ing. Paúl Zhañay Ledesma, MSc