TECNOLOGIAS DE LA INFORMACION
HIPER S.A.
INTERNACIONAL

Córdova 1021 y 9 de Octubre
Ed. San Francisco 300 Piso 22 Of. 2
GUAYAQUIL - ECUADOR

Telefax (593-4) 2302975

PROYECTO MEDIANET

Especificaciones Mensaje de Seguridad
"Integración Ventanillas – Pinpad Verifone"

HIPER

Ciudad	:	Guayaquil
Documento Referencia	:	5.1
Versión del Documento	:	5.1 Revisión 4
Fecha	:	03 Junio del 2019
Responsabilidad HIPER S.A.	:	Sr. Pablo Moreira

CONFIDENCIAL

HIPER

	Autor	Fecha	Observación
Preparación	Pablo Moreira	03/Jun/2019	

EVOLUCION DEL DOCUMENTO			
Versión	**Fecha**	**Autor**	**Evolución**
Draft V5.1 R.4	03/Jun/2019	P. Moreira	Generación de Documentos para Proyecto Ventanilla-Pinpad Avance de Efectivo Banco Bolivariano
V5.1 R.5	30/Ago/2019	P. Moreira	Ya no es preliminar

Contenido

Objetivo del Documento

Especificar el proceso de seguridad para integración de los pinpads Verifone con las Cajas de la Cadena Departamental través de la infraestructura Ethernet; el cual permite comprobar la autenticidad del dispositivo y minimizar los riesgos de clonación o reemplazo de los pinpads.

Audiencia

Este documento está destinado únicamente al Personal Técnico que sea asignado por de Medianet para este Proyecto.

Confidencialidad

Especificaciones del Proceso

Para la implementación del proceso de seguridad entre cajas y pinpads; es necesario el desarrollo, como parte integral de la solución de Ventanilla del Banco, de código para Generaciones, Encripciones y Validaciones de elementos

El proceso de autenticación deberá realizarse para cualquier requerimiento de mensaje que enviará a la caja el pinpad.

Entre las funcionalidades básicas a cubrir detallamos las siguientes rutinas:

GENERADOR DE COMPONENTE

OBJETIVO
Generar Componente único

ENTRADAS		
CAMPO	**TIPO DATO**	**OBSERVACION**
N/A		

RETORNO		
REPUESTA	**TIPO**	**OBSERVACION**
Componente	String	Componente de 16 bytes Hexadecimales para el proceso de seguridad entre la Caja y el Pinpad.

ALGORITMO
Generación Aleatoria por cada invocación

ENCRIPTOR DE LLAVE

OBJETIVO
Encriptar la llave izquierda con el componente aleatorio

ENTRADAS		
CAMPO	**TIPO DATO**	**OBSERVACION**
Llave Izquierda	String	Key de 16 bytes Hexadecimales Generada por la Cadena (Aquí deberá enviarse el componente aleatorio)
Llave Derecha	String	Key de 16 bytes Hexadecimales (llave de PINPAD)
Data a Encriptar	String	Información a encriptar (Aquí deberá enviarse la Llave Izquierda o también denominada llave de la ventanilla)

RETORNO		
REPUESTA	**TIPO**	**OBSERVACION**
Criptograma C	String	Criptograma de 16 bytes Hexadecimales para el proceso de seguridad entre la Ventanilla y el Pinpad.

ALGORITMO
Criptograma C = 3DES(Llave Izquierda, Llave Derecha, Data)

VALIDADOR DE CRIPTOGRAMA P

OBJETIVO
Validar el Criptograma P devuelto por el PINPAD.

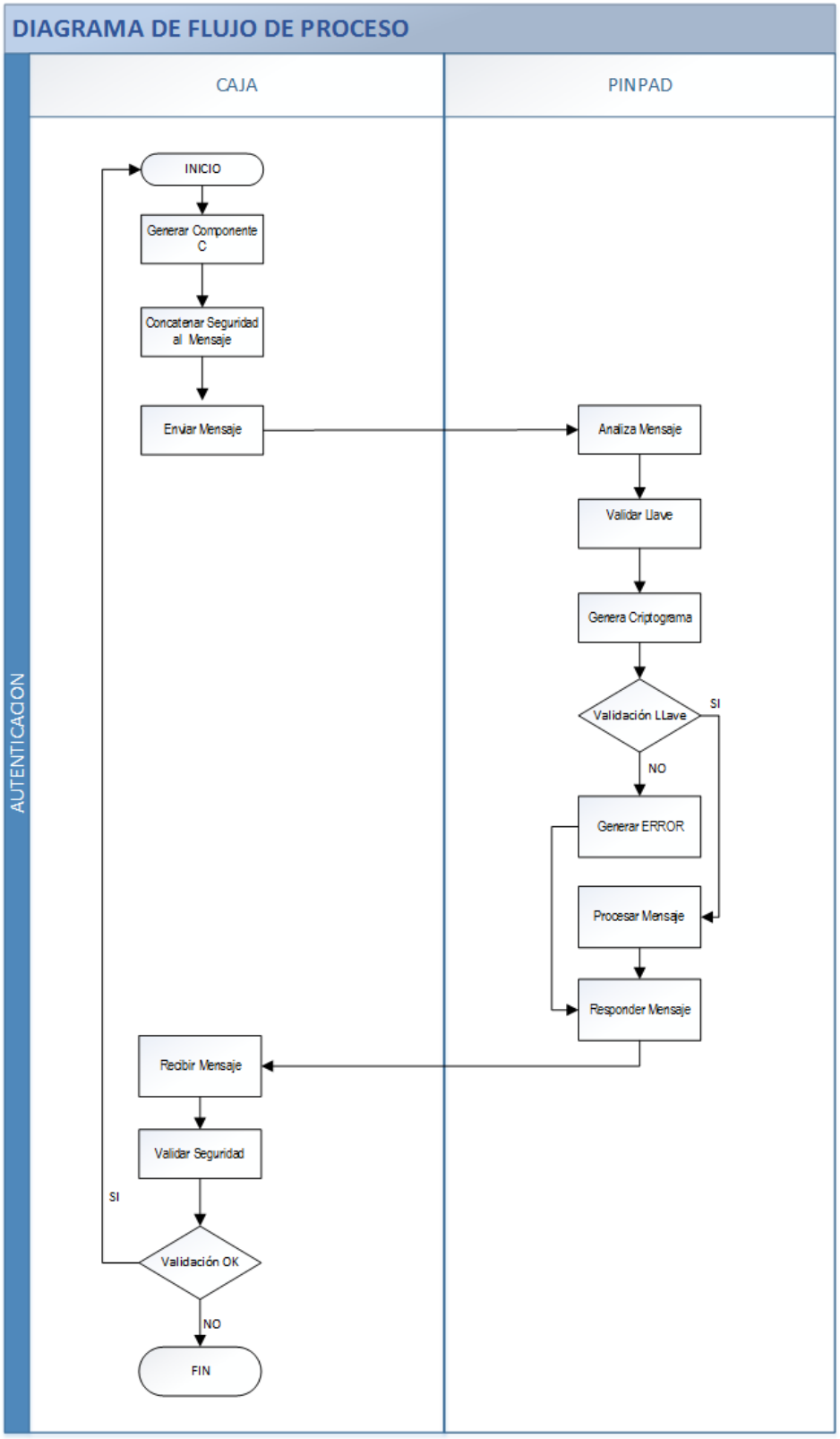
ENTRADAS		
CAMPO	**TIPO DATO**	**OBSERVACION**
Llave Izquierda	String	Key de 16 bytes Hexadecimales Generada por la Cadena
Llave Derecha	String	Key de 16 bytes Hexadecimales
Criptograma P	String	Criptograma devuelto por el Pinpad

RETORNO		
REPUESTA	**TIPO**	**OBSERVACION**
Resultado	Int	Exitoso o Fallido

ALGORITMO
Resultado = Validar(Llave_Izquierda, Llave_Derecha, Criptograma_P, Criptograma_C) *¿3DES^{-1}(Criptograma P) = Llave Derecha* ?: **[SI]➔ Exitoso [NO]➔ Fallido**

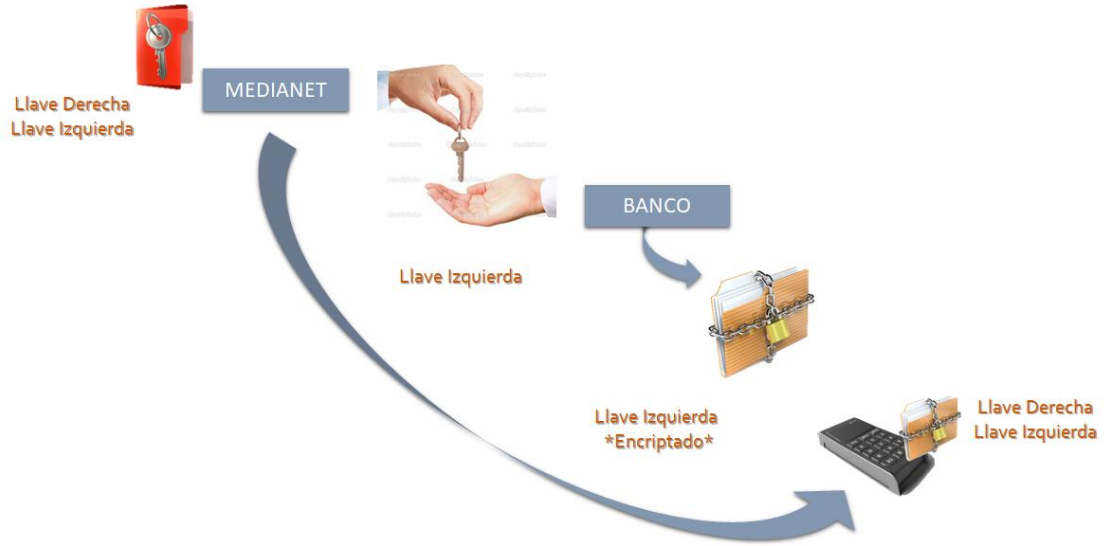
Diagrama de Flujo de Procesos

A continuación se detalla un diagrama para el proceso de seguridad entre la Caja y el Pinpad Vx805:



Administración de Llaves

El intercambio y almacenamientos de las llaves deben seguir el siguiente procedimiento.



Complementos a los Mensajes

El formato de los mensajes se mantiene según el documento "*Especificaciones Técnicas "Integración VENTANILLAS – PINPAD Verifone Versión Plan D*"
en su última versión disponible para PLAN D, pero para ejecutar la autenticación entre la Ventanillas y el PINPAD, se deben transmitir o se recibirán mensajes complementados de la siguiente manera:

REQUERIMIENTOS

[TALLA][ID][MENSAJE][COMPLEMENTO]

- ADICIONAL: 32 Bytes
- [16 Bytes] COMPONENTE
- [16 Bytes]LLAVE IZQUIERDA *ENCRIPTADA CON COMPONENTE* CRIPTOGRAMA **C**

RESPUESTAS

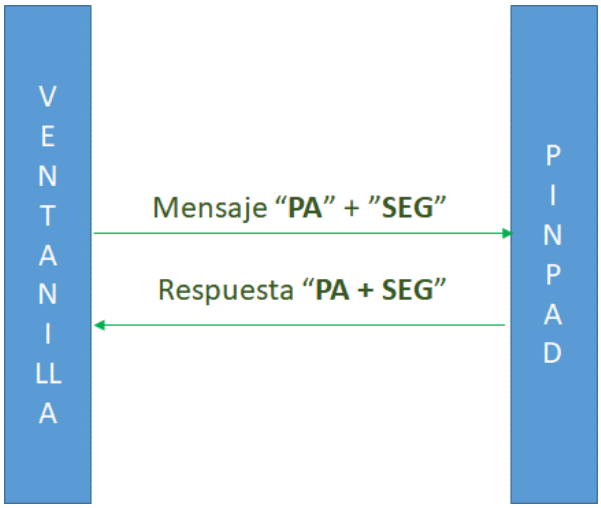
[TALLA][ID][MENSAJE][COMPLEMENTO]

- ADICONAL: 32 Bytes
- [16 Bytes] COMPONENTE
- [16 Bytes] CRIPTOGRAMA **P** *COMPONENTE ENCRIPTADO CON LLAVES*

Anexos

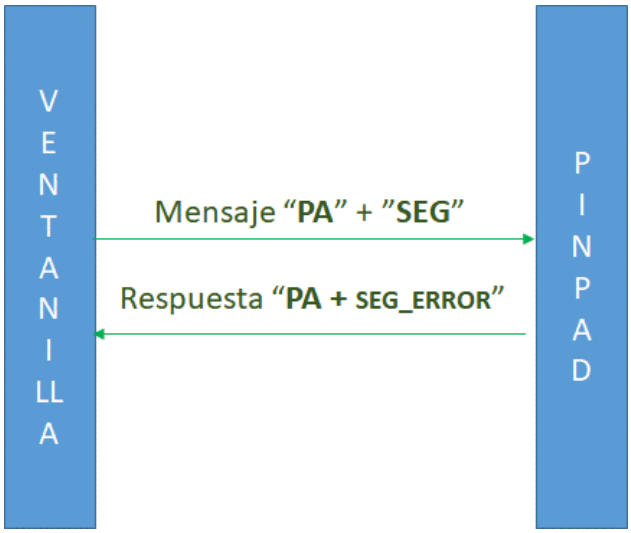
Flujo Transaccional

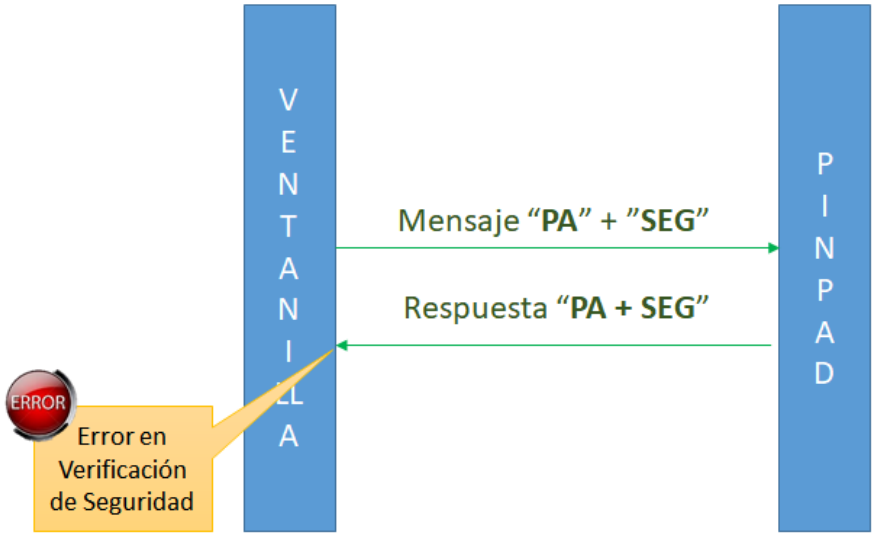
Proceso de Autenticación exitoso



SEG en Mensajes
ALEATORIO+CRIPTOGRAMA C
SEG en Respuestas
ALEATORIO+CRIPTOGRAMA P

Procesos de Autenticación no exitosos





SEG en Mensajes
ALEATORIO+CRIPTOGRAMA C
SEG en Respuestas
ALEATORIO+CRIPTOGRAMA P