

**PROTOCOLO DE GENERACION Y TRANSPORTE
DE PINES DE TARJETAS DE SISTEMA PREPAGO
PARA COMPAÑIAS TELEFÓNICAS CELULARES**

1. Objetivo

Hemos desarrollado los sistemas y protocolos criptográficos para la generación, registro, y distribución segura de pines prepagos para compañías telefónicas celulares, aunque puede ser fácilmente adaptado a sistemas equivalentes en otras operaciones comerciales. Todos los desarrollos son multiplataforma y pueden ser provistos en C, C++ , C#, etc. ya sea como bibliotecas dinámicas .dll, shared libraries, activeX u objetos .NET. Este proyecto se encuentra en explotación exitosa en varias compañías telefónicas celulares de nuestro País y de Sudamérica.

2. Características del proyecto

2.1. Objetivo

Asegurar criptográficamente (Confidencialidad-Integridad-Certificación de Origen y No Repudio) el circuito de pines prepagos (generación, registro y distribución), tanto para la impresión de Tarjetas como para la venta por cajeros, incluyendo herramientas existentes y nuevos desarrollos.

2.2. Circuito asegurado

2.2.1. Desde el servidor ALFA generador de PINES se realiza la Generación de Tarjetas que inserta registros (tabla Phone_Card_Inventory) bajo cualquier plataforma (UNIX, WIN32, Mainframe, etc) en cualquier BDR (Oracle, Informix, SQLserver, etc). Nosotros proveemos el generador pseudoaleatorio de calidad criptográfica NBCSPRBG, totalmente modular y que asegura la ausencia de colisiones entre los PINES de los distintos lotes generados. En ningún momento los pines quedan "texto en claro", estando permanentemente fuertemente encriptados desde su mismo instante de creación hasta cualquier etapa de almacenamiento transitorio, tránsito y siendo validados internamente por medio de *hashing* criptográficamente seguro.

2.2.2. Desde el módulo de Gestión de Prepago, se pide la generación de archivos de pines encriptados, lo que dispara un proceso que corre en ALFA.

2.2.2.1. Características

2.2.2.1.1. Comunicación entre servidores para la ejecución de procesos, a través de Socket. El proceso se dispara desde un Windows Win32 y se ejecuta en un Server Solaris.

2.2.2.1.2. Para la ejecución del proceso se pide una clave que debe llegar segura al servidor ALFA (vía *Secure Shell*).

2.2.2.1.3. El proceso informa parámetros del operador a quien se enviará el archivo, a fin de determinar el formato del archivo de salida y realizar un cambio de estado de los pines en la plataforma, según sea el destino de los mismos.

2.2.3. El proceso en ALFA: se direcciona la salida de los pines por medio de pipes para que un nuevo proceso (otro desarrollo de Firmas Digitales) los tome generando un archivo de salida encriptado e impactando en tablas del Módulo de Gestión de prepago de Celulares (servidor Gamma) con los datos de los pines generados, el campo con el PIN se almacena fuertemente encriptado (RSA).

2.2.3.1. Características

2.2.3.1.1. Toma los pines y genera una salida encriptada (Base 64 y RSA 1024-bits) con el formato que necesita el operador que los reciba (imprentas, red de cajeros automáticos).

2.2.3.1.2. Actualiza Tablas de Gestión de Prepago en Gestión de Celulares con el detalle de los pines para cada operador y un registro encabezado con datos generales del lote.

Datos a almacenar en Gestión de Celulares:

Información del Lote de pines generados en ALFA:

- *Código del operador a quien se enviaron los pines*
- *Número del lote batch generado*
- *Número de serie inicial del lote*
- *Cantidad de pines generados*
- *Monto de los pines generados*

Información de los pines generados en ALFA:

- *Código de artículo para diferenciar los distintos montos de los pines*
- *Código del operador a quien se enviaron los pines*

- *Número del lote batch generado*
- *Número de serie de la tarjeta*
- *Número de Pin (Encriptado)*
- *Monto del Pin*
- *Fecha de Vencimiento del Pin (hasta cuándo puede utilizarse)*
- *Estado de los pines. (Inactivos los que van a imprentas – Distribuidos los que van en consignación para venta en cajeros automáticos)*

NOTA: La estructura de esta tabla es totalmente customizable, además de la información detallada arriba y que es la que se obtiene de la plataforma ALFA, se guardará la historia de los distintos estados por los que pasaron los pines e información de a quienes fueron vendidos.

2.2.3.1.3. Cambiar el estado de los pines en Phone_Card_inventory a 'Distribuido' para aquellos pines que se envían en consignación (Ej. Red Banelco). Se deberán insertar los registros de los pines a cambiar de estado en una tabla ya en producción en GAMMA (SAP_TARJETAS) que impacta sobre la tabla de ALFA (Phone_Card_inventory).

2.2.4. Envío de Archivos de Pines desde un servidor de la Compañía Telefónica Celular a las imprentas y a GIRE (que los reenvía a Red Banelco).

2.2.5. Desencriptación de pines en la Imprenta (sitio donde se generan las tarjetas): se recibe el archivo y se desencripta con una aplicación en Win32 (otro desarrollo de Firmas Digitales).

Se incluye en el desarrollo cliente:

2.2.5.1. Mantenimiento de claves de encriptación: funciones de generación de claves y mantenimiento de las mismas. Definición de roles de usuarios responsables.

2.2.5.2. Instalación de librerías de encriptación en el SERVIDOR WIN32, a fin de que estén disponibles para desarrollos en Gestión de Prepagos de ALFA que necesiten hacer comparaciones con el pin desencriptado.

3. Detalles técnicos del nuevo protocolo de mensajes seguros (NPMS)

Este protocolo (desarrollado por Firmas Digitales) describe en detalle el formato de intercambio de mensajes cifrados incorporando firma digital, encriptación, compresión y sincronismo de claves públicas. También se describen los formatos de intercambio de claves públicas. Se detallan:

- Formato de Mensajes Cifrados
- Formato de Claves Públicas
- Formato de Claves Privadas

Para poder acceder a los detalles de NPMS se debe firmar un Acuerdo de Confidencialidad (NDA) con nuestra empresa. Quedamos a vuestra disposición para ampliar información al respecto.