Bogotá D.C. 23 de Septiembre de 2008.

REQUERIMIENTO TÉCNICO No.1

PARA:	Ingeniero **MANUEL POLO PEREZ.** (Cerrejón)
DE:	Ingeniero **CARLOS ENRIQUE ORTIZ R.** (PDA Soluciones Ltda.)
ASUNTO:	Investigación seguridad en comunicaciones plataforma Blackberry

1.-DESCRIPCION DEL REQUERIMIENTO:

Se requiere investigar sobre la seguridad en las comunicaciones para la plataforma Blackberry con el propósito de presentar las soluciones disponibles en el mercado local para mejorar los procesos de encriptación de la información (voz y datos) entre un número importante de equipos que requieren niveles de seguridad especial. Se deben revisar las soluciones actuales entre Hardware, Firmware y Software que cumplan con el propósito mencionado y sean susceptibles de incorporar a la compañía.

2. INVESTIGACIÓN:

Se contactó al director de inteligencia del Departamento Administrativo de Seguridad (DAS), antiguo director de inteligencia de la Armada Nacional, y algunos otros contactos que usan tecnologías de seguridad dentro de multinacionales del sector privado, encontrando algunas soluciones disponibles y resaltando dos (02) como viables de incorporar en el Cerrejón.

3.- SOLUCIONES POSIBLES:

Existen dos tipos de soluciones disponibles y viables de incorporar a sus necesidades:

3.1. Token de seguridad:

Un token de seguridad, o de autenticación criptográfico, es un dispositivo electrónico que se le entrega a un usuario autorizado para facilitar el proceso de autenticación. Los *tokens* electrónicos tienen un tamaño portátil que permiten ser cómodamente llevados en el bolsillo y se usan para almacenar claves criptográficas como firmas digitales o datos biométricos como las huellas digitales.

Los Tokens SecurID son entonces productos disponibles para varias plataformas informáticas (Blackberry y Palm incluidas) que facilitan la autenticación por medios físicos en varias presentaciones, que proveen un proceso fácil y de un solo paso para identificar positivamente a los usuarios de una red, previniendo acceso de usuarios no autorizados.

La autenticación de los Tokens de SecurID está basada en dos factores para que el usuario se autentique a sí mismo: algo que el usuario conoce (una contraseña reutilizable o PIN) y algo que el usuario tiene (la tarjeta inteligente o token). De este modo, ambos factores se combinan, para crear una contraseña de única vez. Además, si el usuario no posee su tarjeta inteligente y el password, no podrá ingresar a la red.

Dado que la autenticación tradicional de usuarios por medio de contraseñas reutilizables no provee la suficiente seguridad en los ambientes de redes actuales, la mejor solución para reducir ataques externos o internos a los sistemas de información es eliminar o reducir la transmisión de este tipo de contraseñas y adoptar los passwords dinámicos que pueden ser utilizados una sola vez.

Los Tokens SecurID generan códigos de acceso únicos e impredecibles cada 60 segundos. Para tener acceso a recursos protegidos, un usuario simplemente ingresa su PIN secreto, seguido por el código que aparece en la pantalla del SecurID token. La autenticación es asegurada cuando los módulos para control de acceso reconocen el código único del token en combinación con el PIN único del usuario. La tecnología utilizada sincroniza cada token con un hardware o software encargado de controlar el acceso (ACM, access control module). El ACM puede residir en un computador grande, un sistema operativo, en una red de recursos del cliente o en un dispositivo de comunicación, en general en cualquier recurso de información que necesite seguridad.

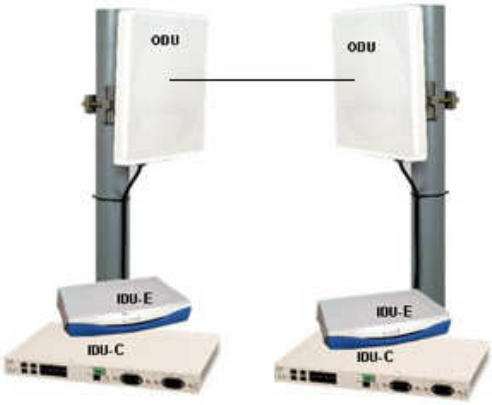
Para consulta técnica y de disponibilidad en precios para la plataforma Blackberry puede consultar los siguientes enlaces:

https://www.mypw.com/

http://www.etek.com.co/

3.2. Canales dedicados:

Los servicios dedicados en telefonía son facilidades de transmisión dedicados a la conexión de dos o más puntos entre sí, sin posibilidad de lograr acceso a otros que no estén involucrados en la topología definida por los usuarios y el servicio.



Los canales dedicados para telefonía celular son entonces conductos de doble vía que permiten la comunicación dentro de una red de usuarios predefinida, donde los protocolos de seguridad son implementados para garantizar la adecuada y oportuna comunicación entre las personas a nivel de voz y datos.

Dichas comunicaciones son punto a punto y garantizan la seguridad debida siempre y cuando no se permita a otros usuarios no autorizados a la red su ingreso, y se facilite la posibilidad de vulnerar la seguridad por medio de software malicioso que controle de manera remota el dispositivo emisor y/o receptor.

En las FF.MM y el DAS se ha implementado la seguridad por estos medios, manteniendo niveles apropiados de seguridad sobre redes muy afinadas entre usuarios que las usan con protocolos muy bien definidos . En Colombia operadores celulares como COMCEL ofrecen este tipo de canales dedicados para enlazar personas en entornos corporativos por medio de paquetes de voz y datos con perfiles y protocolos de seguridad suficientes para garantizar la comunicación entre las partes rápida y oportunamente.

4.- CONCLUSIONES

- Existen varios métodos disponibles comercialmente (productos y servicios) para asegurar las comunicaciones móviles en empresas que requieran el sigilo en la información.
- Dichos métodos son variaciones entre el hardware, firmware y software que facilitan procesos de encriptación de voz y datos simultáneamente.
- Actualmente en Colombia, y desde hace algunos años, son usados varios de estos métodos en el sector oficial y privado.
- No obstante los niveles de seguridad entregados por dichas plataformas ninguno es 100% por 100% seguro, existiendo siempre la posibilidad de que las comunicaciones sean interceptadas durante el proceso emisión – recepción , o desde alguno de los dispositivos intervinientes.
- Existen dispositivos electrónicos de punta (y emergentes) que son dispuestos por gobiernos extranjeros (USA e Israel principalmente) al sector oficial que permiten el manejo de la información por medios mucho más seguros, pero que no son de dominio ni adquisición pública.

5.- RECOMENDACIONES:

- Incorporar en su compañía a nivel de comunicaciones móviles, y específicamente para la plataforma Blackberry, una solución mixta (producto + servicios) entre Tokens SecurID y canales dedicados de voz y datos
- Estudiar los protocolos de seguridad existentes para consolidar los propios, y disponer de los procedimientos claros para el debido uso de los sistemas de seguridad móviles entre los diferentes tipos de usuarios.
- Incorporar conocimiento a todo nivel de las vulnerabilidades existentes en el manejo de la información por medios móviles, identificando claramente las variables y constantes a tener en cuenta para minimizar los riesgos posibles.

Atentamente,

Ingeniero
CARLOS ENRIQUE ORTIZ RANGEL
Gerente General
PDA SOLUCIONES LTDA.