SISTEMAS DE COBRO ELECTRÓNICO Y OTRAS APLICACIONES

GESTIÓN DE LAS CLAVES DE SEGURIDAD

MINISTERIO DE OBRAS PÚBLICAS, TRANSPORTES Y TELECOMUNICACIONES (MOPTT)

CHILE

VERSIÓN 1.0

4 DE NOVIEMBRE 2002

Página en Blanco

SISTEMAS DE COBRO ELECTRÓNICO Y OTRAS APLICACIONES

GESTIÓN DE LAS CLAVES DE SEGURIDAD

- **Documento Número** : ST3
- **Versión** : 1.0
- **Estado** : Versión 1
- **Fecha de Emisión** : 4 de Noviembre de 2002

- **Autores : Consultores**

Ronald Bull (INTEC, Chile)
Guillermo Cuadra (IGYC, Chile)

- **Autores : MOPTT**

Georgina Febré (MOPTT, Chile)

- **Contacto 1** :

Georgina Febré
Ministerio de Obras Públicas, Transportes y Telecomunicaciones – Chile
Tel. : +56 2-258-3722
Fax : +56 2-258-3779
Email: georgina.febre@moptt.gov.cl

MINISTERIO DE OBRAS PÚBLICAS, TRANSPORTES Y TELECOMUNICACIONES
CHILE

Sistemas de Cobro Electrónico y otras Aplicaciones

Gestión de las Claves de Seguridad

Contenido

1 Introducción y Alcances 2

2 Referencias 2

3 Claves de Seguridad usadas en las Concesiones MOPTT 3

3.1 Claves Residentes en el Transponder 3

3.2 Claves Usadas en el Sistema de Cobro de Peaje de la Concesión 4

3.3 Partes Perjudicadas con el Compromiso de las Claves 5

4 Procedimientos de Seguridad de la Concesión 6

5 Generación y Respaldo de las Claves Maestras 8

5.1 Requerimientos para la Generación de Claves 8

5.2 Respaldo de las Claves 8

6 Protección de las Claves Maestras Usadas por las Concesiones 10

6.1 Requerimientos 10

6.2 Distribución y Carga de las Claves Maestras a los Módulos Seguros 10

6.2.1 Claves Maestras del Dominio del MOPTT 10

6.2.2 Claves Maestras del Dominio del Operador y del Emisor del Transponder 11

7 Protección de las Claves Usadas para la Producción de Transponders 12

8 Vida de las Claves Maestras 13

Sistemas de Cobro Electrónico y otras Aplicaciones

Gestión de las Claves de Seguridad

1 Introducción y Alcances

Las técnicas criptográficas, aplicadas a las transacciones antena – transponder vía comunicaciones DSRC definidas para las concesiones del Ministerio de Obras Públicas, Transportes y Telecomunicaciones de Chile (MOPTT), dependen de claves de seguridad. La gestión de estas claves es un aspecto complejo y crítico en la provisión de la seguridad necesaria. Es crucial poder asegurar que las claves generadas tengan las propiedades necesarias y que estén lo suficientemente protegidas contra compromiso o sustitución. Adicionalmente, las claves deben ser distribuidas con anticipación a los sistemas donde son requeridas para su operación.

El propósito de este documento es definir la forma en que estas claves deben ser gestionadas.

2 Referencias

[MOPTT_ST1] **MOPTT ST1: Julio 15, 2002**
"Sistemas de Cobro Electrónico y otras Aplicaciones,
Especificación para la Interoperabilidad en la Transacción Antena - Transponder"

[MOPTT_ST6] **MOPTT ST6: Noviembre 4, 2002**
"Sistemas Electrónicos de Cobro y Otras Aplicaciones,
Generación de Claves Maestras, Interfaz de Exportación de Claves"

[A1] **TR 4001 A1: June 12, 1999**
Version ER9_1.3
Interoperable EFC Transaction Using Central Account Based on DSRC
Alcatel, Combitech, Kapsch, CSSI

[FIPS 140] **FIPS PUB 140-2: May 25, 2001**
Security Requirements for Cryptographic Modules
U.S. Department of Commerce
National Institute of Standards and Technology

[ANSI X9.17] **ANSI X9.17: 1985**
American National Standard for Financial Institution Key Management (Wholesale)
American Bankers Association

3 Claves de Seguridad usadas en las Concesiones MOPTT

El esquema de seguridad definido en [MOPTT_ST1] emplea claves de seguridad simétricas. Esto significa que claves secretas se mantienen tanto en el equipo a bordo o OBE, y en el interior de los sistemas de las concesiones, específicamente en los equipos al costado de la carretera o RSE, en el Centro de Operaciones y/o en el Centro de Atención a Clientes. Según se explica en [MOPTT_ST1], para asegurar las transacciones se emplean claves DES derivadas de Claves Maestras 3-DES. Las claves residentes en los OBE son DES, derivadas de las Claves Maestras según se describe en [A1]. Este diseño protege las Claves Maestras, ya que bajo ninguna circunstancia ellas se están en el interior de equipamiento distribuido al público.

En las secciones siguientes, los identificadores que se emplean para las claves maestras son iguales a los de las claves derivadas, excepto por la presencia de la letra "M". Por ejemplo, clave derivada EFC-EAcK-V se obtiene de la clave maestra EFC-MEAcK-V.

3.1 Claves Residentes en el Transponder

La Tabla 3.1 presenta las claves residentes en cada transponder.

En el campo identificador de la clave, "V" es la versión de la clave de seguridad, asignado en conjunto por el MOPTT y el emisor del transponder. El valor "V" se registra el byte 6 del atributo EFC-ContextMark. Inicialmente "V" tendrá el valor 1, y será incrementado a medida que nuevas versiones se adopten en el futuro.

Tabla 3.1. Claves de Seguridad del Transponder

Elemento	Nombre de la Clave	Propietario	Identificador
Sistema	ElementAccessKey	Emisor	SYS-EAcK-V
Peaje Interoperable	ElementAuthenticationKeyA1	Emisor	EFC-EAuKA1-V
	ElementAuthenticationKeyA2	Issuer	EFC-EAuKA2-V
	ElementAuthenticationKeyF1	MOPTT	EFC-EAuKF1-V
	ElementAuthenticationKeyF2	MOPTT	EFC-EAuKF2-V
	ElementAuthenticationKeyI1	MOPTT	EFC-EAuKI1-V
	ElementAuthenticationKeyI2	MOPTT	EFC-EAuKI2-V
	ElementAuthenticationKeyI3	MOPTT	EFC-EAuKI3-V
	ElementAuthenticationKeyI4	MOPTT	EFC-EAuKI4-V
	ElementAccessKey	MOPTT	EFC-EAcK-V
Emisor	ElementAccessKey	Emisor	ISS-EAcK-V
Gestión de Estacionamientos	ElementAuthenticationKey	MOPTT	PM-EAuK-V
	ElementAccessKey	MOPTT	PM-EAcK-V
Sonda de Tráfico	ElementAccessKey	MOPTT	TP-EAcK-V

En el elemento de Peaje Interoperable, las claves de autenticación tienen dos o cuatro generaciones: dos generaciones para EFC-EAuKAx-V y EFC-EAuKFx-V, y cuatro para EFC-EAuKIx-V.

Todas las claves de seguridad de un transponder deberán tener el mismo número de versión "V". Para cada versión "V", el MOPTT entregará a todas las concesiones los mismos valores de las Claves Maestras para que obtengan las respectivas claves derivadas. Por ejemplo, suponiendo que se trata de la versión 1 de las claves, el mismo valor de EFC-MEAuKI1-1 será usado por todas las concesiones para derivar las claves EFC-EAuKI1-1 residentes en los transponders.

3.2 Claves Usadas en el Sistema de Cobro de Peaje de la Concesión

La Tabla 3.2 presenta las claves usadas en el sistema de cobro de la concesión. Los equipos del punto de cobro, así los del resto del sistema, deberán ser capaces de operar con todas las versiones de claves emitidas por el MOPTT. El uso de la clave MasterElementAuthenticationKeyAi (i = 1, 2) en el RSE es opcional, pudiendo el operador usar en su lugar la clave MasterElementAuthenticationKeyIp (p = 1, 2, 3, 4). Las claves MasterElementAuthenticationKeyFx (x = 1, 2), y asimismo las claves usadas para las aplicaciones de Gestión de Estacionamientos y Sonda de Tráfico, no son necesarias en los sistemas de cobro de peaje.

Tabla 3.2. Claves de Seguridad usadas en el Sistema de Cobro de Peaje de la Concesión

Elemento	Nombre de la Clave	Propietario	Identifiacador
Sistema	MasterElementAccessKey (clave presente sólo para transponders propios)	Emisor	SYS-MEAcK-1
			SYS-MEAcK-2
			…
Peaje Interoperable	MasterElementAuthenticationKeyAi (i = 1, 2)	Emisor	EFC-MEAuKAi-1
	MasterElementAuthenticationKeyAj (j = 1, 2)		EFC-MEAuKAj-2
	…		…
	MasterElementAuthenticationKeyIp (p = 1, 2, 3, 4)	MOPTT	EFC-MEAuKIp-1
	MasterElementAuthenticationKeyIq (q = 1, 2, 3, 4)		EFC-MEAuKIq-2
	…		…
	MasterElementAccessKey	MOPTT	EFC-MEAcK-1
			EFC-MEAcK-2
			…
	MasterReceiptAuthenticationKey	Operador	EFC-MReAuK-1
			EFC-MReAuK-2
			…
Emisor	MasterElementAccessKey	Tag Issuer	ISS-MEAcK-1
			ISS-MEAcK-2
			…

Todas las claves requeridas durante una transacción deberán estar residentes en el equipamiento del punto de cobro. Algunas claves serán usadas en otras partes del sistema. Cada concesión será responsable de la adopción de políticas y medidas para proteger las claves incluidas en la Tabla 3.2, con el fin de que no sean reveladas a terceros. Estas políticas y medidas deberán ser propuestas por cada concesión, cumplir con el presente documento y requerirán de la aprobación por parte del MOPTT.

3.3 Partes Perjudicadas con el Compromiso de las Claves

Una vez que una clave de seguridad es conocida afuera de su dominio, se ha perdido el control y para todos los fines prácticos debe suponerse que ella es pública. En este contexto, el compromiso puede ocurrir con personas internas o externas al sistema de concesiones MOPTT. La Tabla 3.3 identifica las partes perjudicadas cuando una clave queda comprometida.

Tabla 3.3 Partes Perjudicadas con el Compromiso de las Claves

Clave Maestra Comprometida	MOPTT	Usuarios	Concesión Emisora	Oras Concesiones
SYS-MEAcK-V	Si	Si	Si	Si
EFC-MEAuKAi-V	Si	Si	Si	No
EFC-MEAuKIp-V	Si	No	①	Si
EFC-MEAcK-V	Si	Si	Si	No
EFC-MReAuK-V	No	No	No	No
ISS-MEAcK-V	No	Si	Si	No

①: Depende del caso

4 Procedimientos de Seguridad de la Concesión

Cada concesión deberá preparar un documento escrito especificando las políticas y procedimientos organizacionales para la protección de las Claves Maestras, el que deberá ser puesto en conocimiento de todo su personal con responsabilidades en la gestión de dichas claves. Este documento requerirá la aprobación por parte del MOPTT.

El documento deberá tomar en consideración que las soluciones de encriptación basadas en software serán consideradas no seguras.

La generación y manipulación de las Claves Maestras deberá estar a cargo de personal calificado, usando procedimientos establecidos y herramientas adecuadas con el fin de garantizar una operación segura.

Cada concesión deberá designar una persona encargada que será responsable por la gestión de todas las claves identificadas en el capítulo 3. El nombre de esta persona deberá ser comunicado al MOPTT, a lo menos 30 días antes de que pueda efectuarse cualquier transferencia de claves desde el MOPTT a la concesión. De la misma manera, cualquier cambio en esta designación deberá ser comunicada al MOPTT a lo menos 30 días antes de entrar en vigencia.

El documento deberá cubrir como mínimo los siguientes temas:

- Organización de la concesión para la gestión de las Claves Maestras. Deberá definir quiénes son responsables por:
  - ✓ La seguridad del sistema de generación de Claves Maestras
  - ✓ Las auditorías al sistema de generación de claves
  - ✓ La capacitación del personal involucrado
  - ✓ La correcta ejecución de los procedimientos
  - ✓ La revisión y mejoramiento periódico de los procedimientos
  - ✓ El ciclo de vida de las Claves Maestras

- Gestión del Hardware:
  - ✓ Protección del hardware de amenazas físicas
  - ✓ Control del inventario
  - ✓ Ciclo de fin de vida del hardware
  - ✓ Seguridad física
  - ✓ Gestión de medios removibles de computación y su disposición
  - ✓ Acceso al hardware y controles a ser usados para el acceso por terceros

- Gestión del Software:

- ✓ Registro de las aplicaciones instaladas
- ✓ Control de acceso a las aplicaciones
- ✓ Protección frente a software malicioso

- Gestión de los usuarios:
  - ✓ Gestión de registro, autenticación, derechos de acceso, privilegios y contraseñas
  - ✓ Capacitación de los usuarios
  - ✓ Responsabilidades de los usuarios
  - ✓ Acuerdos legales a ser usados con el personal que tiene acceso a áreas restringidas y sensitivas

- Generación y gestión de las Claves Maestras:
  - ✓ Procedimientos para la generación de claves
  - ✓ Almacenamiento de copias de seguridad de las claves
  - ✓ Almacenamiento de claves usadas para la encriptación de claves
  - ✓ Procedimientos para la transferencia de las claves
  - ✓ Distribución de las claves para la producción de transponders
  - ✓ Distribución de las claves hacia los sistemas de peaje de las concesiones
  - ✓ Activación y desactivación de las claves
  - ✓ Destrucción de las claves

- Revisiones de la seguridad de los sistemas
- Reporte de errores del software y de incidentes

5 Generación y Respaldo de las Claves Maestras

5.1 Requerimientos para la Generación de Claves

Los requerimientos siguientes deberán aplicarse a cada concesión y asimismo al MOPTT. Si una concesión elige usar a un tercero para el proceso de generación de sus claves, el tercero deberá cumplir con estos requerimientos.

Las Claves Maestras deberán ser generadas en un sistema seguro con la exclusiva participación y bajo la supervisión de personal calificado en materia de seguridad. El sistema deberá ser diseñado de manera que al menos dos personas sean necesarias para ponerlo en marcha y para operarlo. Los usuarios autorizados deberán poseer un dispositivo de identificación legible por el sistema, junto a contraseñas secretas definidas por ellos para asegurar la identificación. El proceso de identificación de usuarios deberá ser resistente a ataques de "replay".

Las claves deberán ser generadas en el interior de un módulo seguro o dispositivo equivalente diseñado para cumplir con [FIPS 140] nivel 2. El módulo deberá ser configurado de manera que las claves sólo puedan ser extraídas de él cifradas mediante claves de encriptación. El proceso de generación de claves deberá cumplir con [ANSI X9.17]. Alternativamente y sujeto a la aprobación del MOPTT, podrá usarse un procedimiento diferente que entregue claves aleatorias e impredecibles. La generación de claves deberá asegurar que no se produzcan claves débiles o semi-débiles, y que ambas mitades de las claves triple DES sean diferentes.

El sistema de generación de claves deberá crear automáticamente una bitácora en la que se identifiquen los usuarios y todas las acciones ejecutadas en él.

Esquemas alternativos de generación de claves pueden ser aceptables, sujetos a una aprobación previa por parte del MOPTT.

5.2 Respaldo de las Claves

El respaldo de las Claves Maestras puede ser efectuado en cualquier dispositivo, siempre que las claves se encuentren cifradas mediante claves de encriptación. Cuando las claves de encriptación puedan ser recuperadas en texto claro sin el concurso de contraseñas, no deberán respaldarse en el mismo dispositivo las Claves Maestras y las de encriptación. El número de copias de respaldo deberá ser adecuado para asegurar la recuperación de las claves en una situación de peor caso. Las copias de respaldo no necesarias deberán ser destruidas.

Las claves de encriptación deberán ser guardadas mediante un procedimiento seguro que requiera a lo menos dos diferentes personas autorizadas para su recuperación. Esquemas alternativos pueden ser aceptables, sujetos a una aprobación previa por parte del MOPTT.

6 Protección de las Claves Maestras Usadas por las Concesiones

6.1 Requerimientos

Cada vez que una de las Claves Maestras identificada en la Tabla 3.2 sea usada en el interior de un sistema de una concesión, será obligatoria una implementación con un módulo de hardware seguro, diseñado para cumplir con [FIPS 140] nivel 2. Las Claves Maestras deberán ser guardadas en una zona protegida de la memoria de dicho módulo, de manera que estas claves no puedan ser extraídas de él. Bajo ninguna circunstancia estará permitido mantener copias en texto claro de las Claves Maestras en la memoria de trabajo de algún controlador del punto de cobro, en un disco duro, o en cualquier otro medio de almacenamiento dentro del sistema de la concesión que permita extraer las Claves Maestras en texto claro.

La velocidad de proceso de los módulos seguros instalados en los puntos de cobro deberá permitir al sistema completar la transacción de peaje especificada en [MOPTT_ST1] antes de que el vehículo abandone la zona de comunicaciones. Será posible el uso de módulos seguros más lentos en sistemas de peaje de una pista, con baja velocidad de paso de vehículos.

6.2 Distribución y Carga de las Claves Maestras a los Módulos Seguros

6.2.1 Claves Maestras del Dominio del MOPTT

Para instalar las Claves Maestras en los módulos seguros, las claves del dominio de MOPTT serán entregadas cifradas mediante una clave de encriptación. Las claves deberán ser desencriptadas en el interior del módulo seguro. Para este fin la concesión deberá generar una clave de transporte secreta, y comunicarla mediante un procedimiento seguro al MOPTT.

El MOPTT encriptará las claves de su dominio y las entregará a la concesión en un medio de transporte suministrado por la concesión. El esquema de transferencia deberá ser diseñado de manera que se requiera un mínimo de dos operadores de la concesión para cargar las Claves Maestras a los módulos seguros.

Las Claves Maestras podrán ser transferidas desde un módulo seguro hacia otros módulos seguros de la concesión, pero sólo cifradas con una clave de transporte. En este caso, las claves de transporte deberán requerir la participación de a lo menos dos operadores de la concesión para su instalación.

Con el fin de emplear un una interfaz común de transferencia de Claves Maestras entre el MOPTT y las concesiones, deberá adoptarse el esquema de transferencia especificado en [MOPTT_ST6].

Si una concesión desea emplear un esquema diferente, deberá someter todos sus detalles al MOPTT para un análisis caso por caso. El MOPTT se reserva el derecho de aprobar o rechazar lo propuesto sin expresión de causa.

6.2.2 Claves Maestras del Dominio del Operador y del Emisor del Transponder

Cada concesión deberá asegurar que sus claves privadas sean protegidas de compromiso o sustitución. Por lo tanto, se aplican a las claves de su dominio los mismos requerimientos establecidos 6.2.1.

7 Protección de las Claves Usadas para la Producción de Transponders

Según se describe en el capítulo 3, las claves residentes en el transponder son derivadas de las respectivas Claves Maestras. Todas las claves del transponder, incluidas las diferentes generaciones de las claves de autenticación, se graban en el transponder durante el proceso de producción. Esto significa que las respectivas Claves Maestras son necesarias durante la producción de estos dispositivos.

El esquema empleado para transferir las claves al transponder deberá ser diseñado de manera tal que las Claves Maestras no sean reveladas fuera de su propio dominio. Específicamente, las Claves Maestras nunca deberán ser comunicadas al fabricante de transponders. El fabricante deberá usar medios seguros provistos por la concesión dentro de un ambiente seguro para cargar las claves a los transponders, y deberá devolver los medios empleados a la concesión, una vez que la producción se haya completado.

Con el fin de emplear una interfaz común de transferencia de Claves Maestras entre el MOPTT y las concesiones, deberá adoptarse el esquema de transferencia especificado en [MOPTT_ST6].

Si una concesión desea emplear un esquema diferente, deberá someter todos sus detalles al MOPTT para un análisis caso por caso. El MOPTT se reserva el derecho de aprobar o rechazar lo propuesto sin expresión de causa.

8 Vida de las Claves Maestras

Ninguna clave de encriptación es segura si es usada por un período indefinido. Siempre existe la posibilidad de revelación, accidentes, pérdida, o incluso que sea quebrada por alguien. Esto significa que las claves deben tener una vida limitada. Para las concesiones del MOPTT, se aplicará lo siguiente:

- El MOPTT y cada concesión deberán emitir una nueva versión de claves cada dos años y medio. Los transponders deberán ser producios con la última versión liberada.
- Cada vez que se cambie la batería de un transponder, deberá cargarse en él la última versión de claves liberada.
- La vida de las siguientes claves de seguridad residentes en el transponder será igual a la vida de la batería de éste:
  - ✓ SYS-EAcK-V
  - ✓ EFC-EAcK-V
  - ✓ ISS-EAcK-V
  - ✓ PM-EAuK-V
  - ✓ PM-EAcK-V
  - ✓ TP-EAcK-V
- Según se especifica en [MOPTT_ST1], los transponders llevan más de una generación de claves de autenticación para la aplicación de peaje. La vida de estas claves será la siguiente:
  - ✓ EFC-EAuKAx-V: 2.5 años
  - ✓ EFC-EAuKFx-V: 2.5 años
  - ✓ EFC-EAuKIx-V: 1.25 años

  El MOPTT definirá las fechas en las cuales las nuevas generaciones entren en servicio. Los transponders que no hayan agotado su batería en cinco años pueden permanecer en funciones con la última generación de claves en su interior.