

**El Teléfono Celular
como Plataforma de Servicios
Desafíos para la Seguridad**

**Eduardo Giménez
Grupo de Seguridad de las TI
INCO - Facultad de Ingeniería**



Objetivos

- Introducir algunos aspectos relativos a la seguridad de dispositivos móviles a través de un caso de estudio.
- Caso de estudio: tecnología NFC y acceso al STM.



Plan de la charla

- Servicios emergentes en telefonía celular
- La tecnología NFC
- Un caso de estudio: pago con móvil en STM
 - Problemática de seguridad
 - Mecanismos de seguridad de la aplicación
 - Arquitectura de seguridad del dispositivo
 - Algunos problemas a resolver



Servicios emergentes en telefonía celular

- Antes: solo telecomunicaciones
- Ahora, dispositivo multifunción para:
 - Geocalización de servicios próximos
 - Gestión de datos personales (agenda, pins)
 - Difusión de contenidos (música, videos)
 - Juegos
 - Medios de pago
 - Control de acceso (redes de transporte)
 - Navegación en internet
 - etc.



Cohabitación de servicios de naturaleza diferente

- Servicios sensibles:
 - Medios de pago
 - Gestión de datos personales
 - Control de acceso
- Servicios no sensibles:
 - Juegos
 - Navegación en internet
 - Difusión de contenidos
 - Geolocalización (límite...)



Motivaciones para la aparición de estos servicios

- Mayor capacidad de almacenamiento, cálculo y comunicación en los teléfonos
- Infraestructura ya desplegada y fácilmente extensible
- Dispositivo de relativo bajo costo para el usuario
- Oportunidad de negocios para operadores
- Incluye un componente de alta seguridad (SIM)
- Nuevas tecnologías de comunicación sin cables (NFC)



Plan de la charla

- Servicios emergentes en telefonía celular
- **La tecnología NFC**
- Un caso de estudio: pago con móvil en STM
 - Problemática de seguridad
 - Mecanismos de seguridad de la aplicación.
 - Arquitectura de seguridad del dispositivo
 - Algunos problemas a resolver en el modo OTA



Near Field Communication (NFC)

- Protocolo de comunicación peer-to-peer por radio frecuencia de corto alcance (13.56 MHz).
- Activada cuando dos dispositivos NFC se encuentran a menos de 4 cm.
- Por su corto alcance, las comunicaciones NFC se adaptan bien a las transacciones seguras (comparar con Bluetooth).
- Estándares: ISO 14443 Type A/Type B, Felica
- Inicialmente desarrollado e impulsado por Sony/Philippis.
- Masivamente desplegado en Japón (DoCoMo:30 millones), numerosos proyectos y prototipos en Europa y Asia.

NFC: algunas aplicaciones posibles

El celular como tarjeta de crédito



Pago en transportes públicos



<http://www.nfc-forum.org>



ACERCAR

Publicidad interactiva



Control de acceso

Muchas otras aplicaciones posibles...



Intercambio de datos
entre dispositivos
electrónicos

Ayuda para personas con
problemas de visión



Más de 100 proyectos en el mundo



NFC Forum: sponsors



NFC Forum: 140 miembros

PRINCIPAL MEMBERS

ASSOCIATE MEMBERS

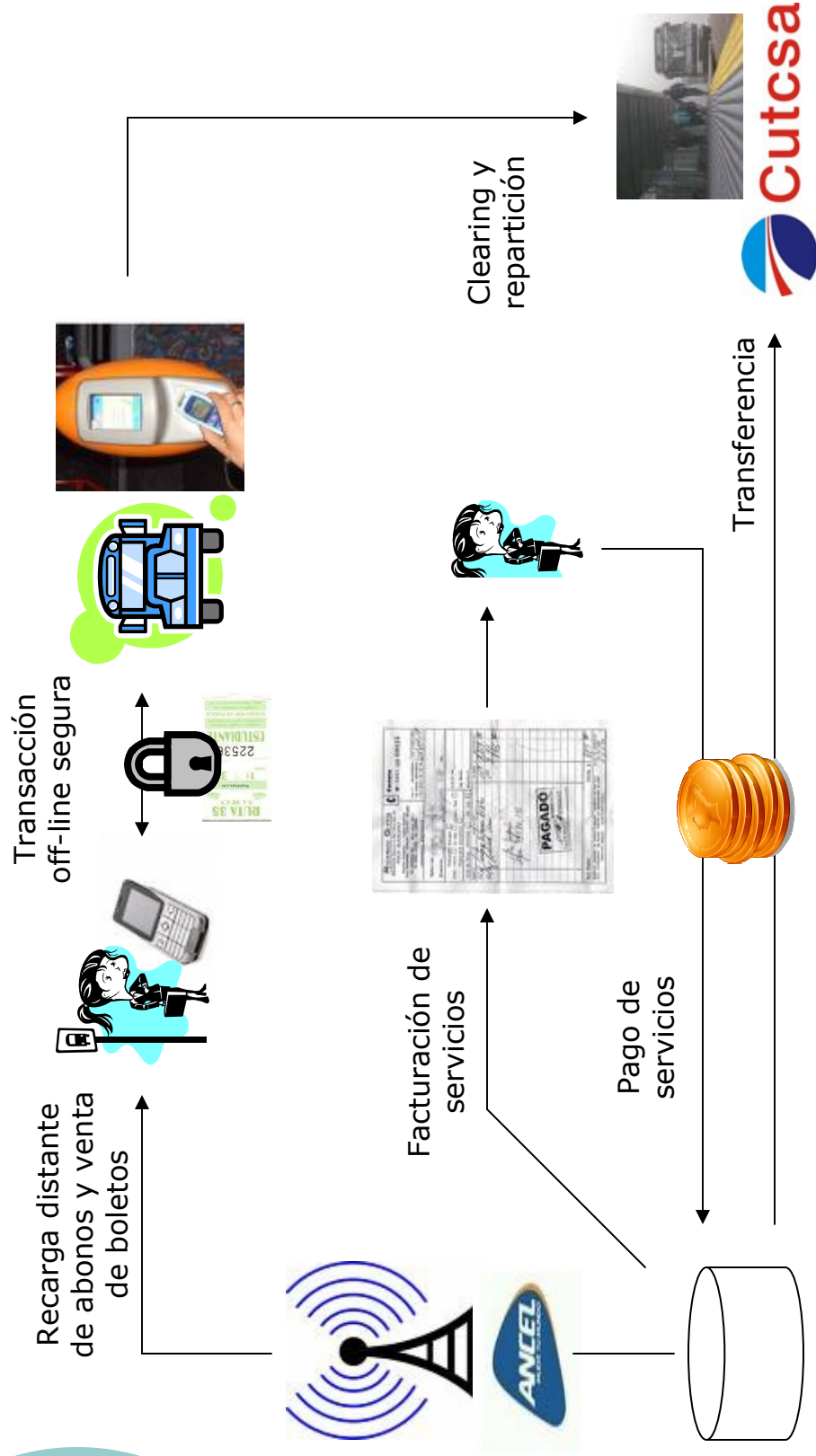
NON-PROFIT MEMBERS



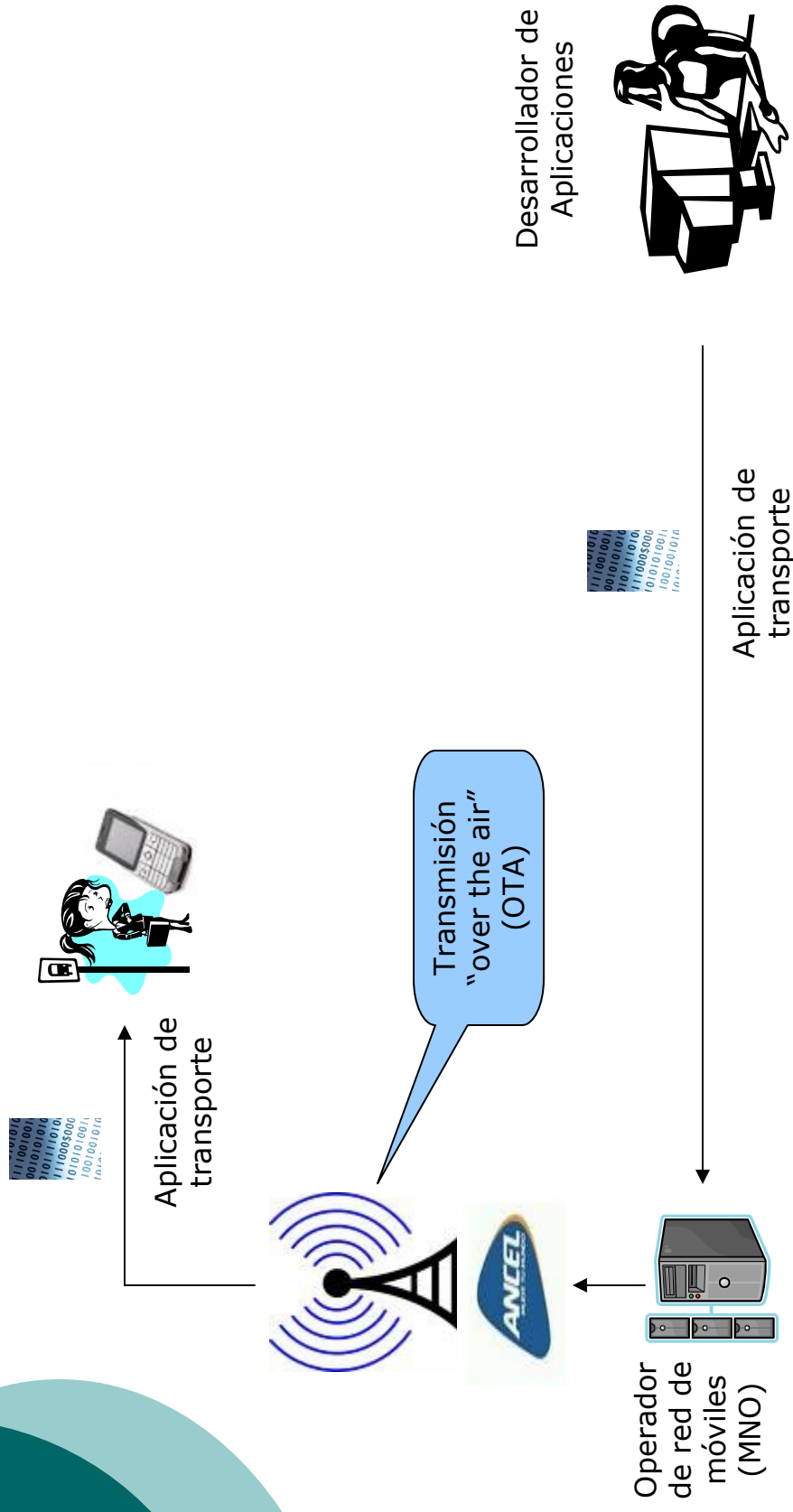
Plan de la charla

- Servicios emergentes en telefonía celular
- La tecnología NFC
- **Un caso de estudio: pago con móvil en STM**
 - Problemática de seguridad
 - Mecanismos de seguridad de la aplicación
 - Arquitectura de seguridad del dispositivo
 - Algunos problemas a resolver

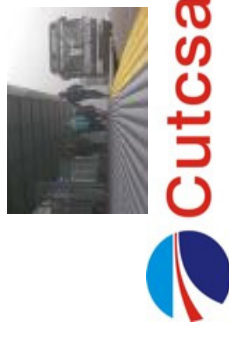
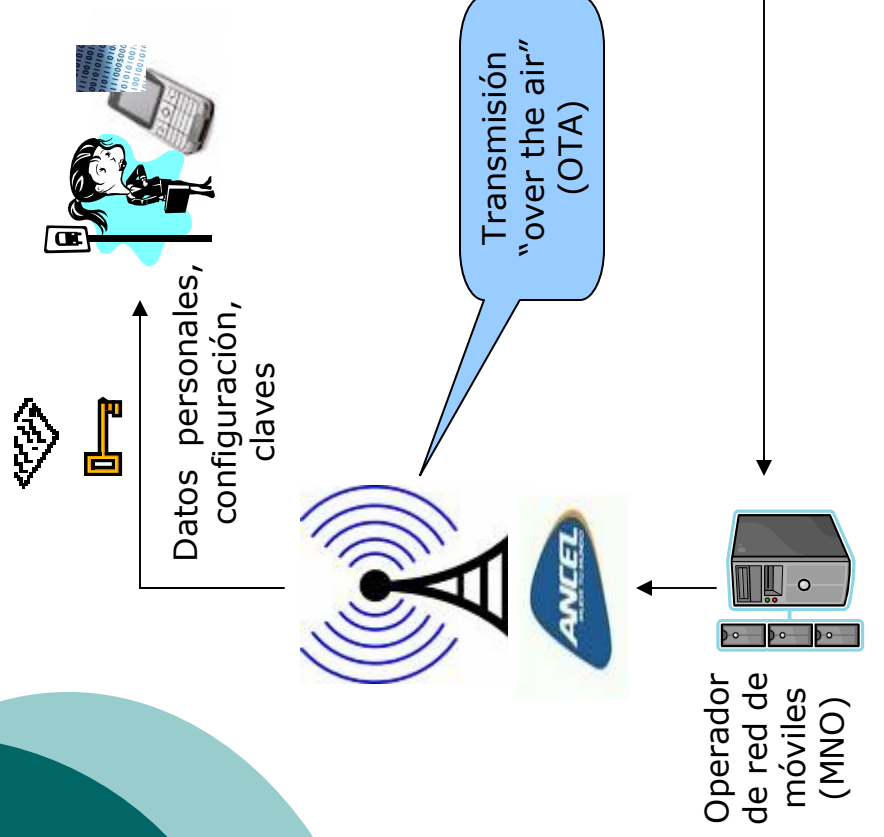
Caso de estudio: acceso al transporte público (ejemplo)



Caso de estudio: cargado inalámbrico de la aplicación



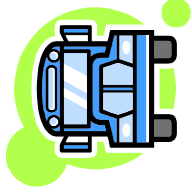
Caso de estudio: personalización de la aplicación



Ventajas de esta arquitectura

- Transportista

- Disminuye el posibilidad de falsificación
- Minimiza la instalación de terminales
- Reduce el número de tarjetas STM a producir.
- Permite llegar a un amplio público



- Usuario

- Más practicidad (todo en un solo dispositivo)
- Evita el uso de efectivo
- Proporciona mas seguridad (anulación en caso de robo)



- Operador telefónico

- Fideliza al cliente
- Proporciona nueva área de negocios
- Factor de diferenciación
- Abre la puerta a futuros servicios

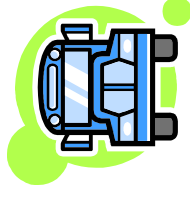




Plan de la charla

- Servicios emergentes en telefonía celular
- La tecnología NFC
- Un caso de estudio: pago con móvil en STM
 - **Problemática de seguridad**
 - Mecanismos de seguridad de la aplicación
 - Arquitectura de seguridad del dispositivo
 - Algunos problemas a resolver

Problemática de seguridad: visión del transportista



- Control de acceso a la red de transporte
 - El usuario tiene abono o boleto válido cuando viaja
- Autentificación del dispositivo
 - La aplicación es genuina
- Autentificación de los comandos
 - No se trata de una sesión anterior que fue grabada
- Abono o boleto es siempre consumido
 - Decremento debe ser transacción atómica
- Prueba de compra
 - El pedido de boletos viene de la aplicación de transporte

Problemática de seguridad: visión del usuario



- Evitar uso fraudulento de su abono
 - Autenticación del usuario (claves, PIN)
 - Compromiso con eficiencia...
- Invalidar abono en caso de robo
 - Comunicación remota con dispositivo
 - SMS que bloquee la aplicación a distancia

Problemática de seguridad: visión del operador telefónico



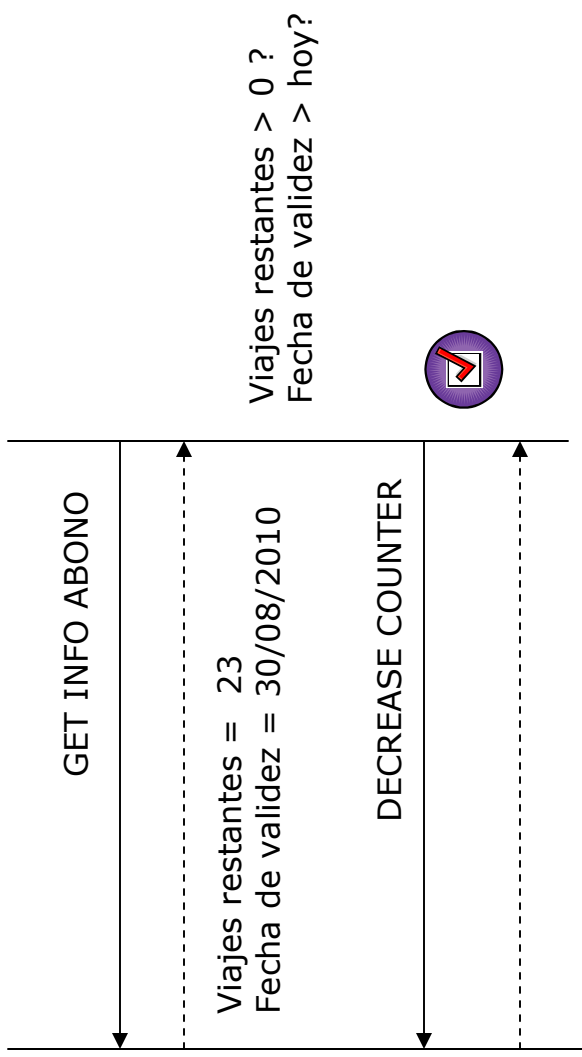
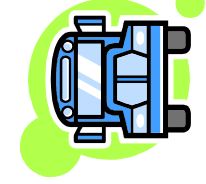
- El operador es un intermediario
 - Mismos requerimientos que el transportista...
 - ...restringidos a operaciones en línea.
- Responsable de las transacciones hechas a través de sur red de comunicaciones:
 - Instalación de la aplicación en el dispositivo
 - Personalización con datos usuario y activación del servicio
 - Recarga de boletos
- Prueba de compra
 - Poder exhibir evidencia de un pedido de compra



Plan de la charla

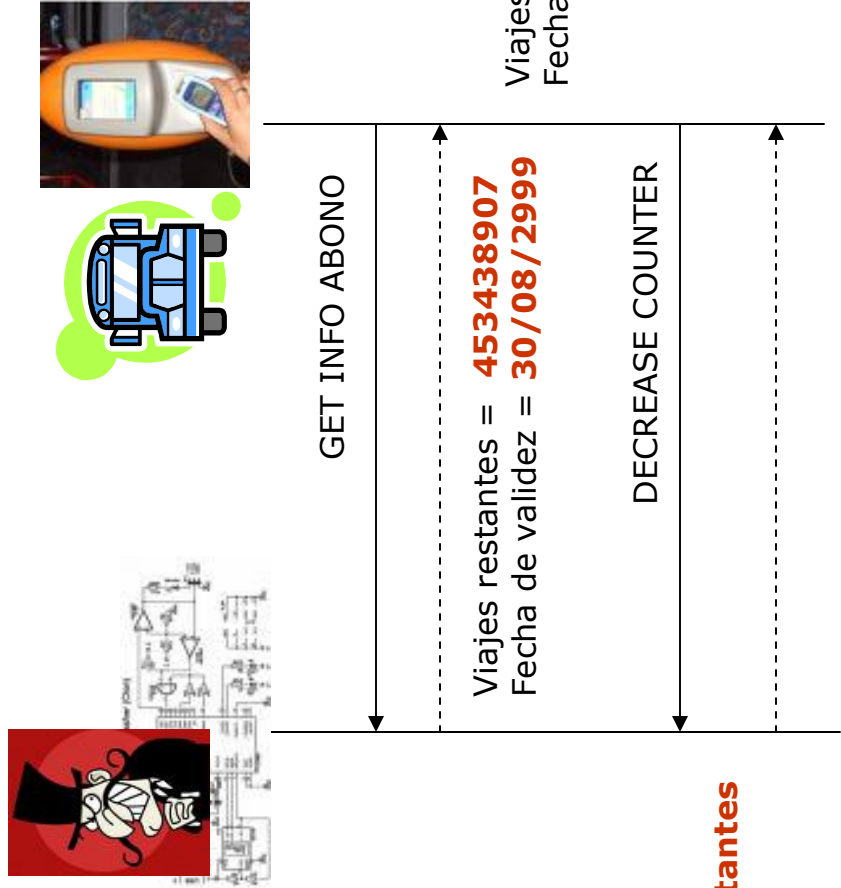
- Servicios emergentes en telefonía celular
- La tecnología NFC
- Un caso de estudio: pago con móvil en STM
 - Problemática de seguridad
 - **Mecanismos de seguridad de la aplicación**
 - Arquitectura de seguridad del dispositivo
 - Algunos problemas a resolver en el modo OTA

Funcionamiento de la aplicación



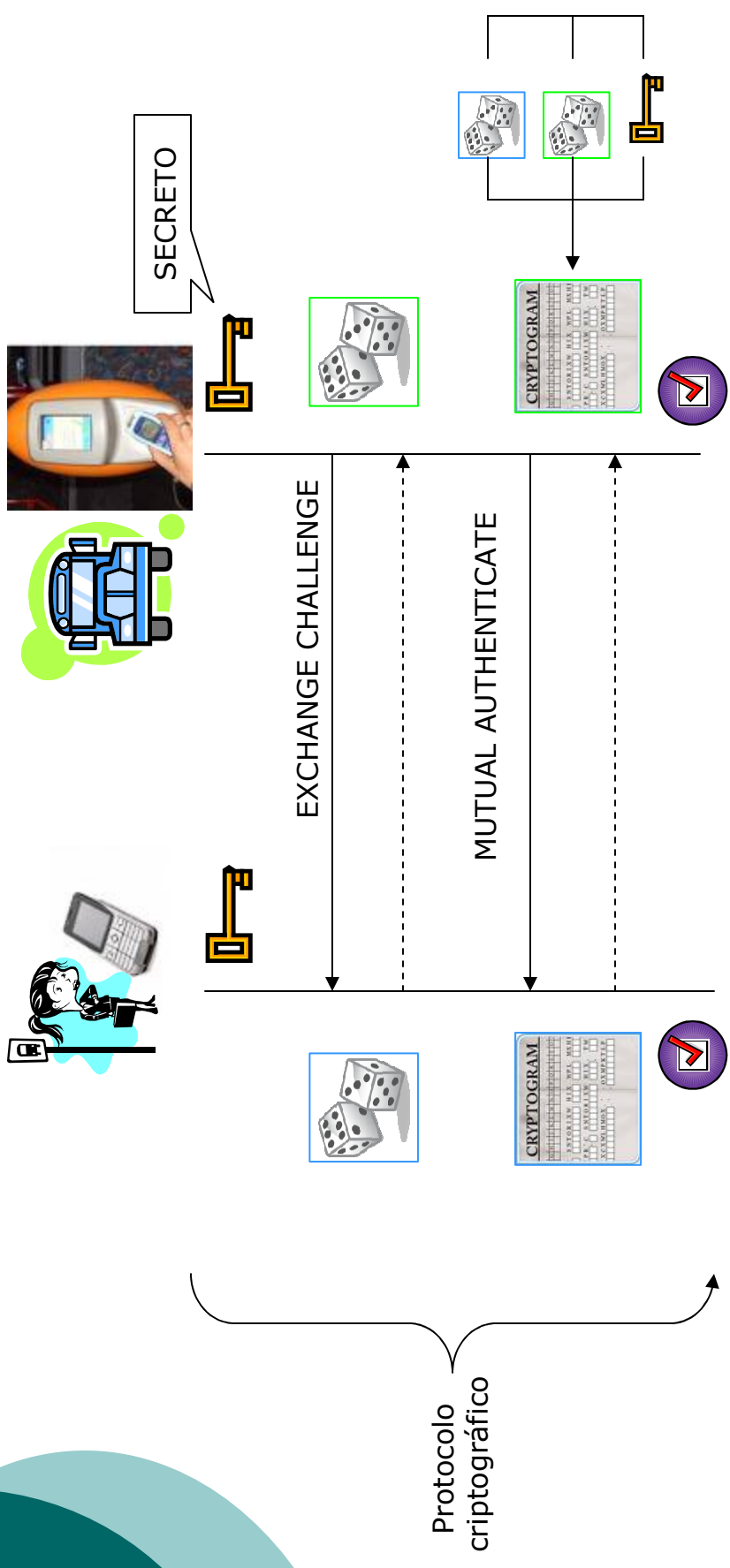
Viajes restantes : = viajes restantes -1

Escenario de ataque : control de acceso



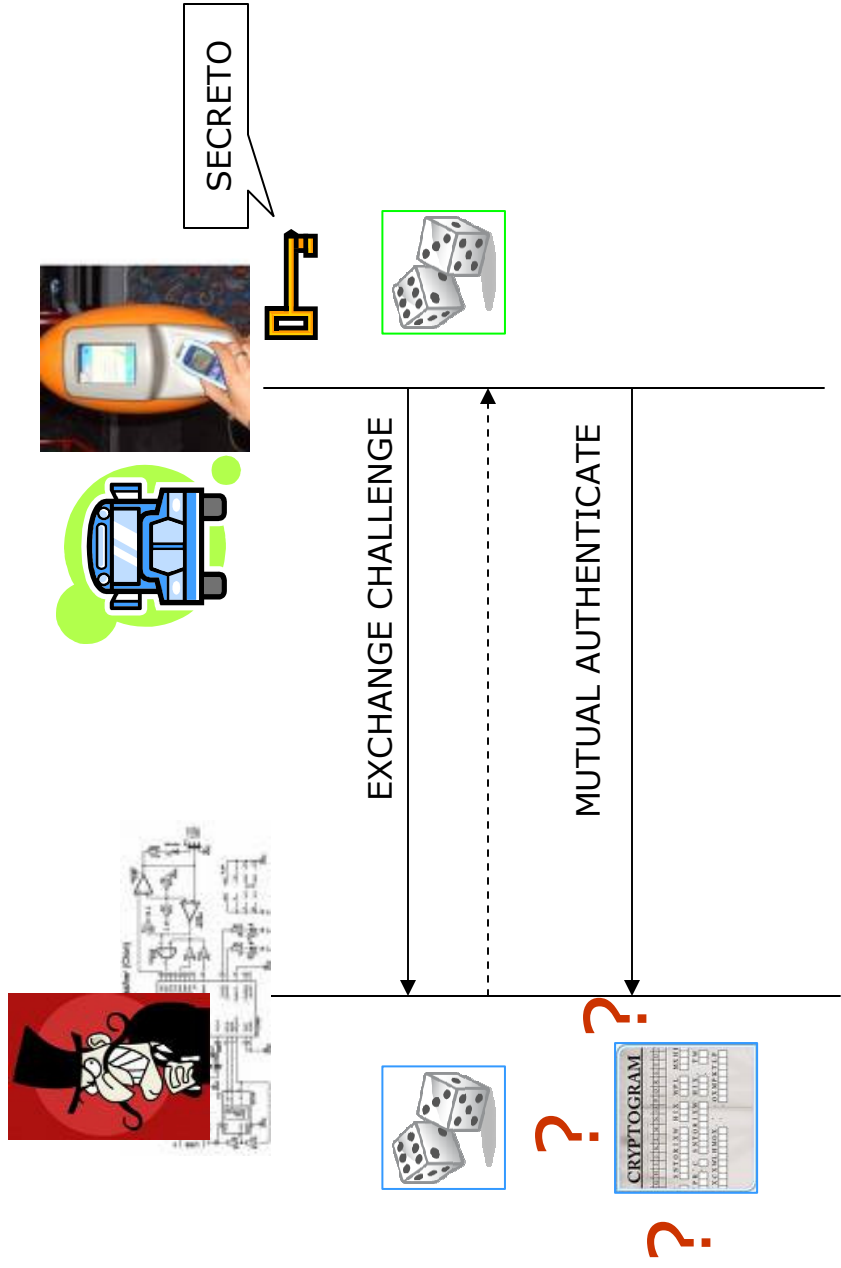
Viajes restantes := **viajes restantes**

Mecanismos de Seguridad de la aplicación : autenticación del usuario (1/2)

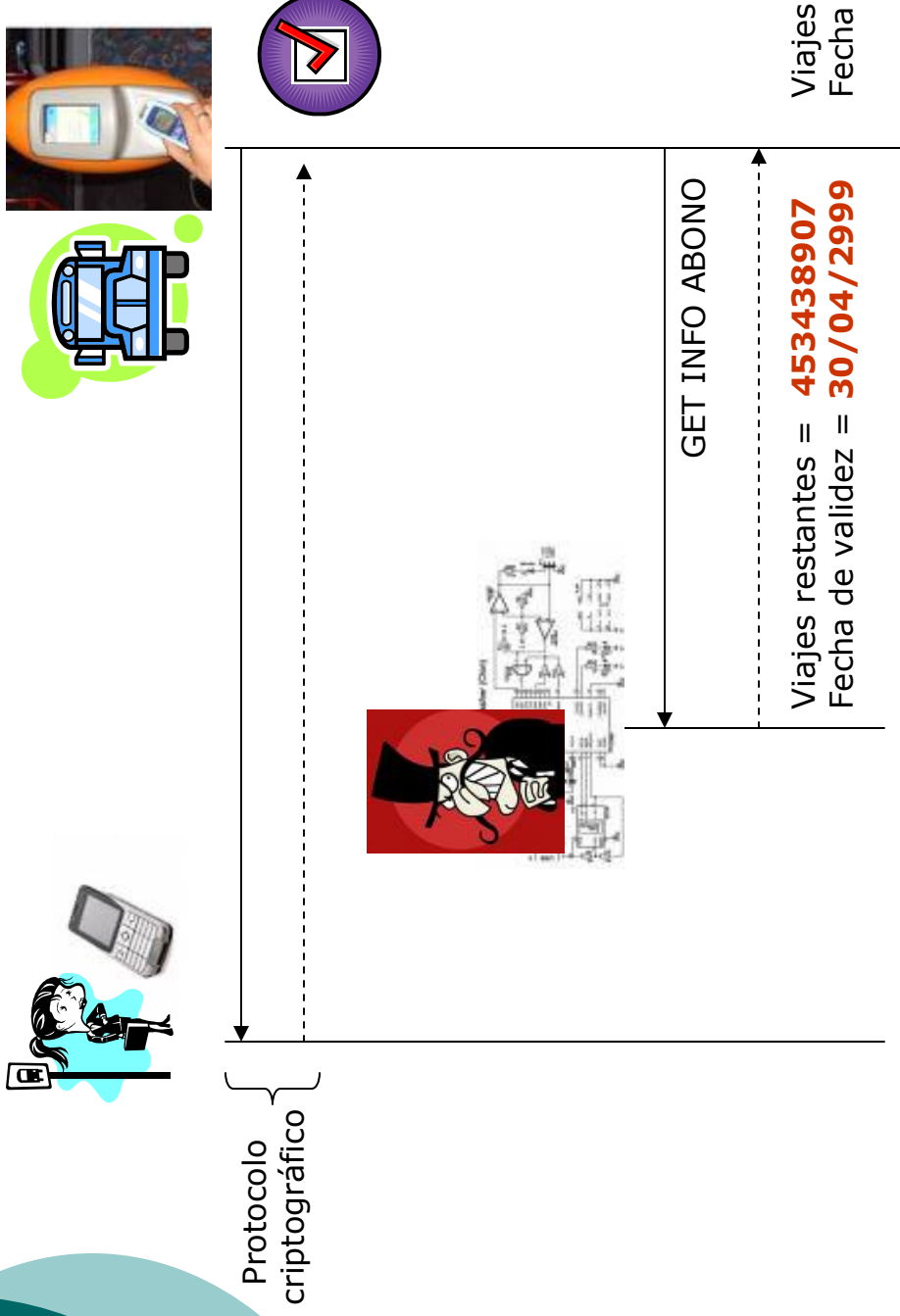


Protocolo
criptográfico

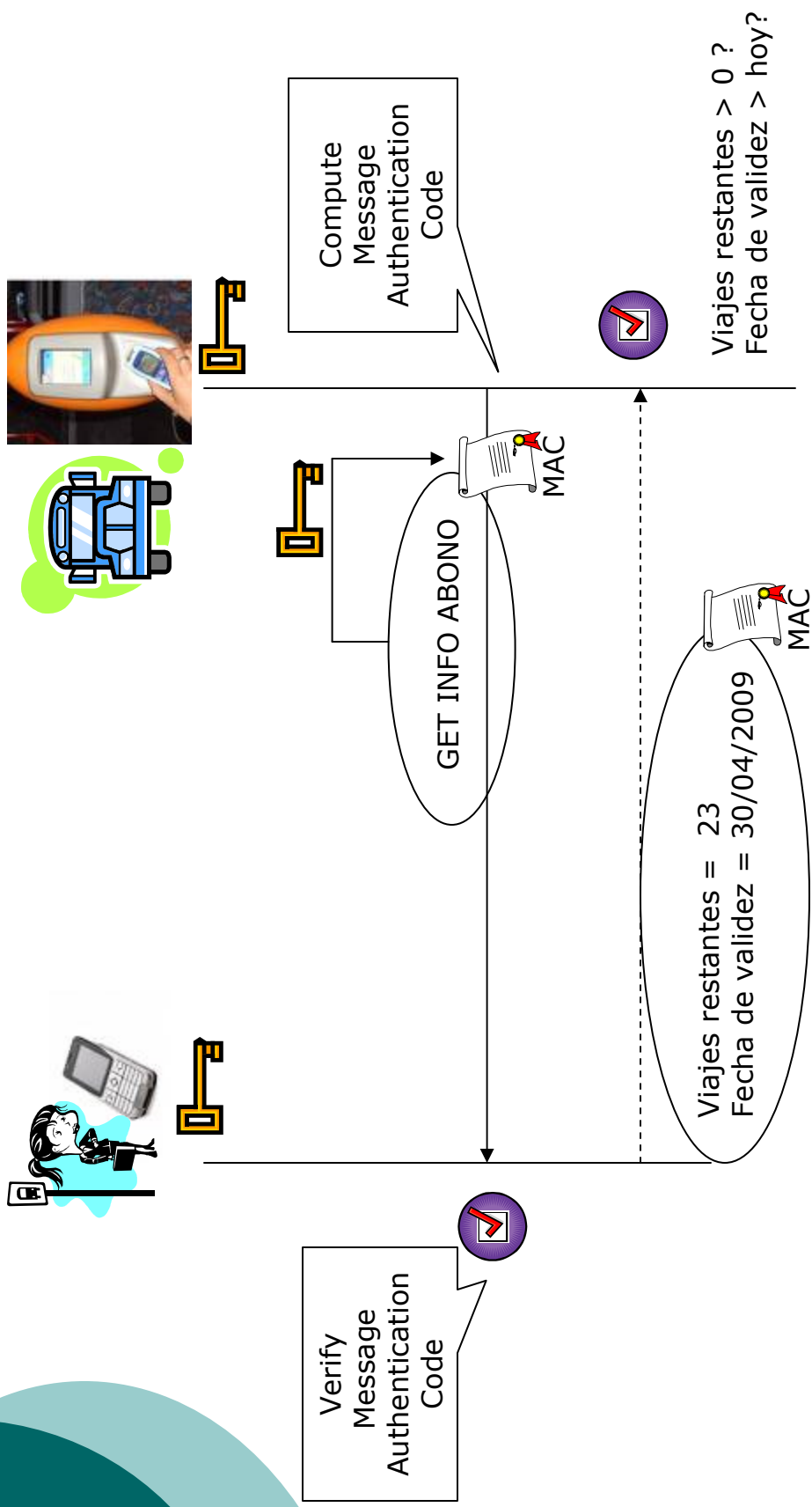
Mecanismos de Seguridad de la aplicación : autenticación del usuario (2/2)



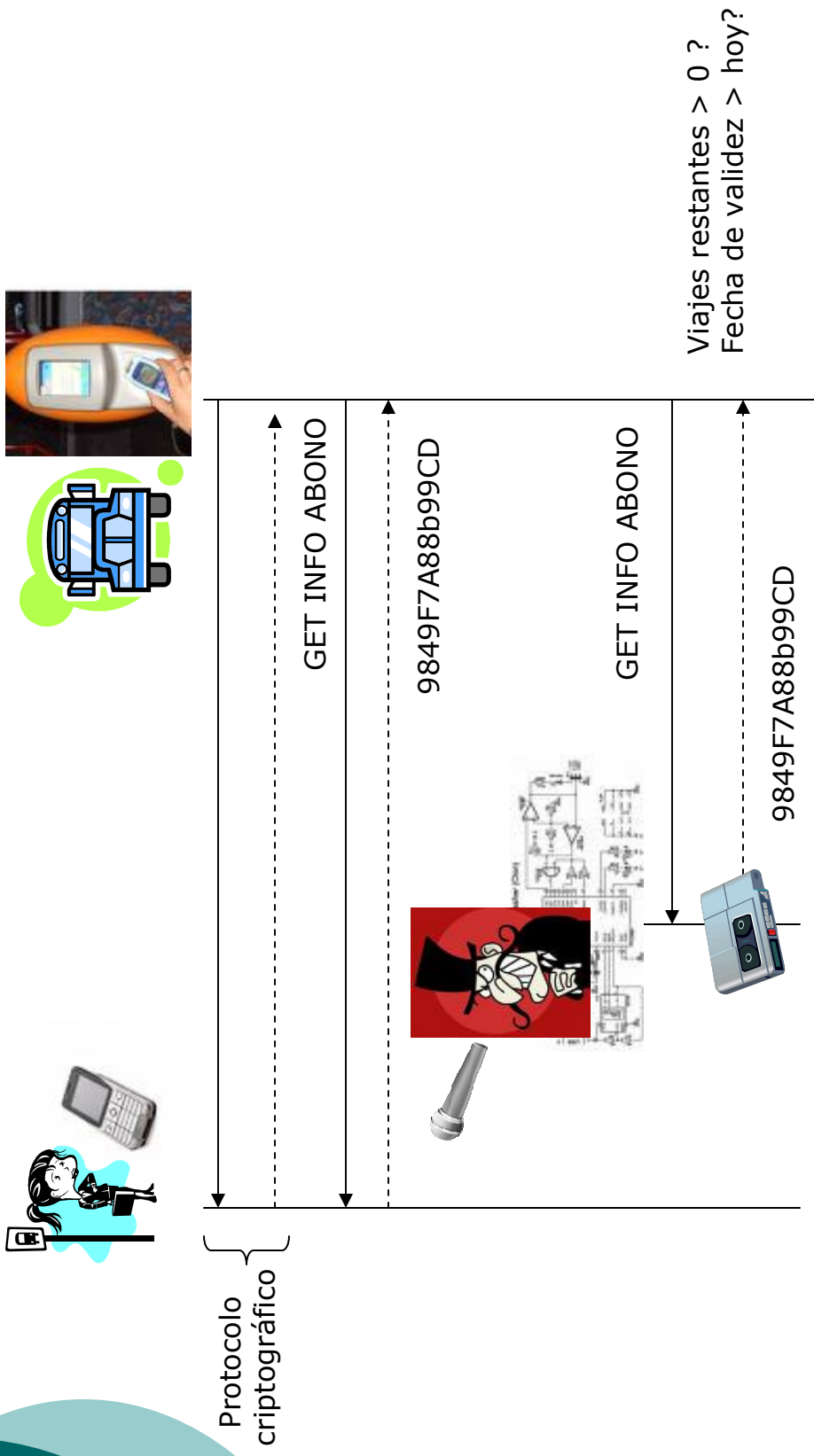
Escenario de ataque : falsificación de comandos (v1)



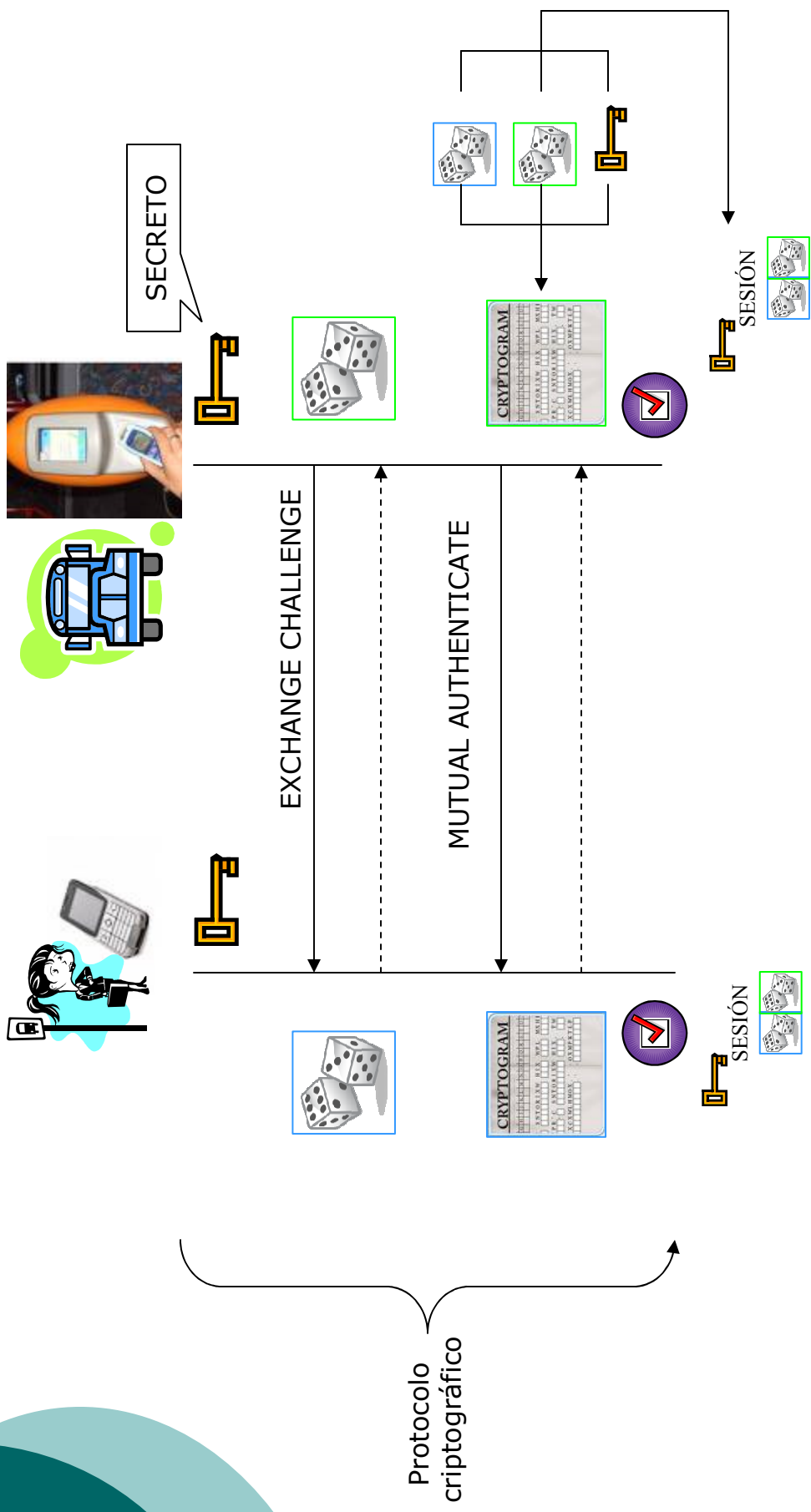
Mecanismos de Seguridad de la aplicación : autenticación de comandos



Escenario de ataque : falsificación de comandos (v2)

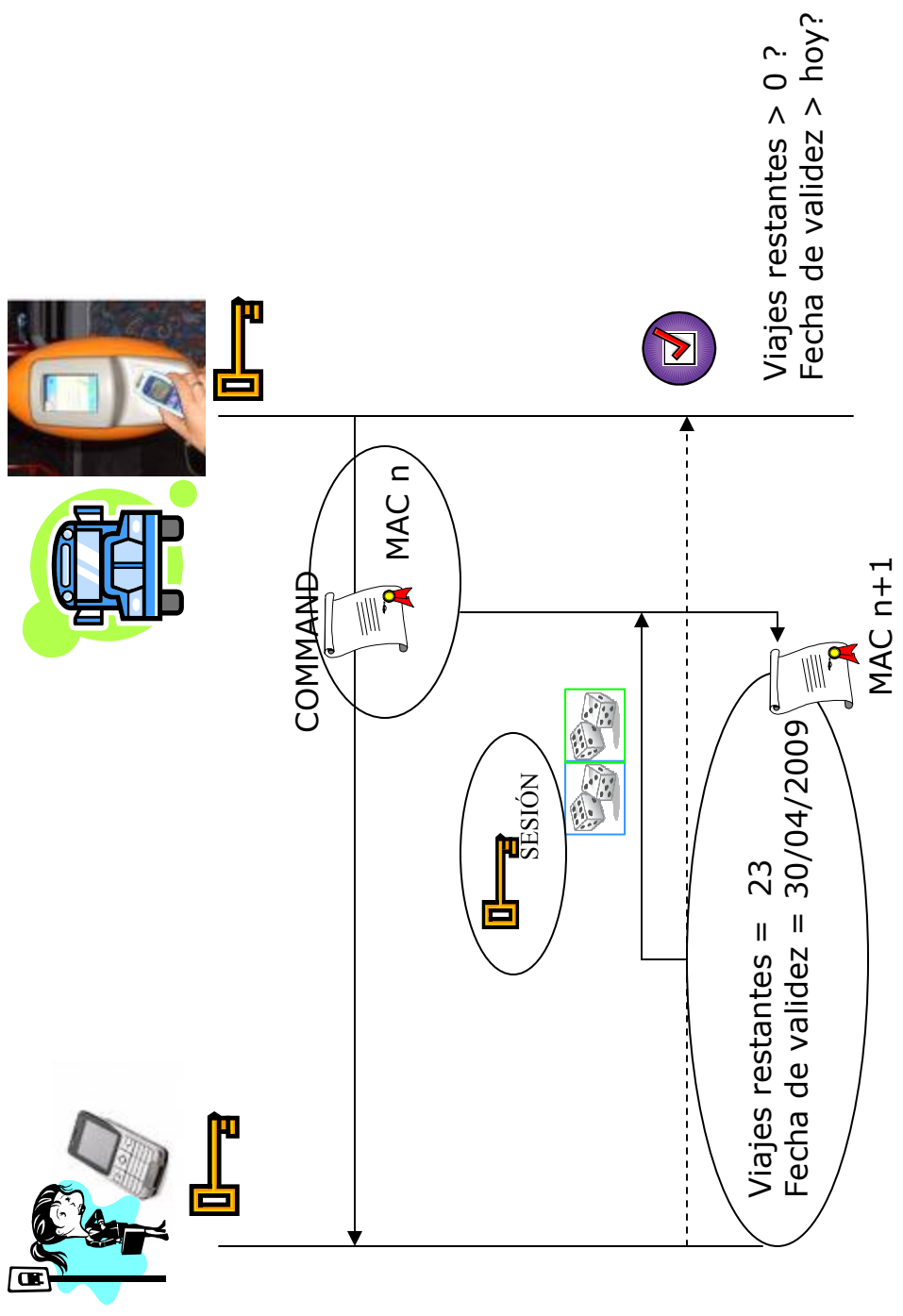


Mecanismos de Seguridad de la aplicación : claves de sesión

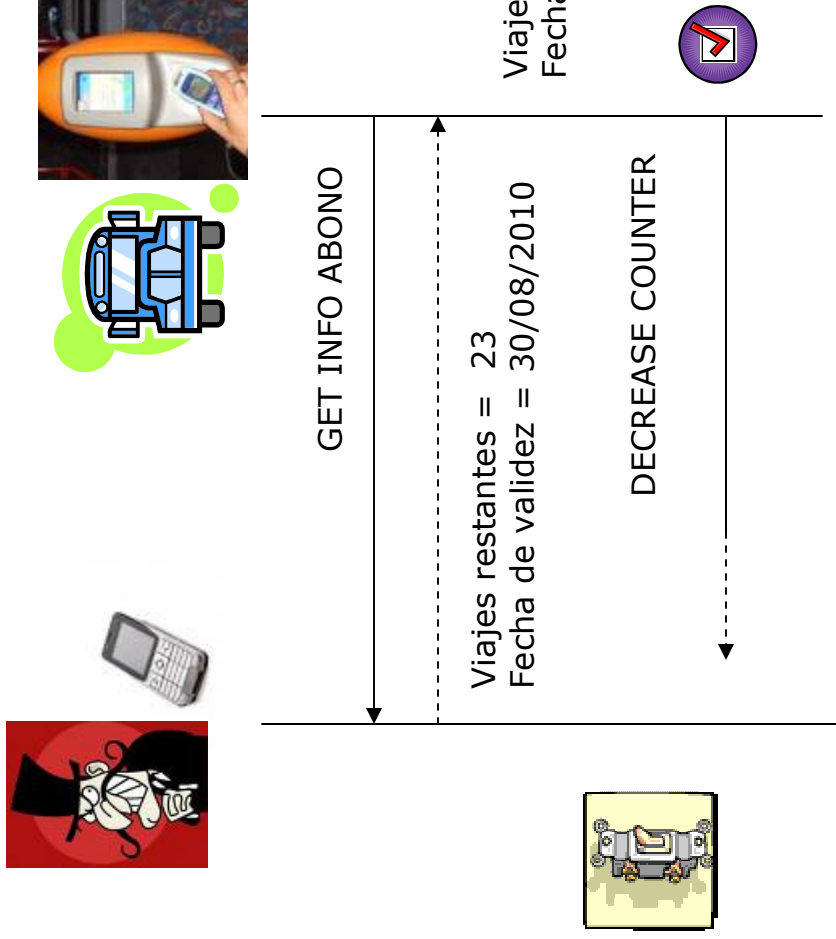


Protocolo
criptográfico

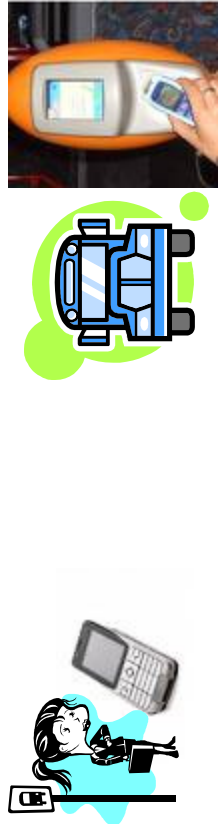
Mecanismos de Seguridad de la aplicación : autenticación de comandos



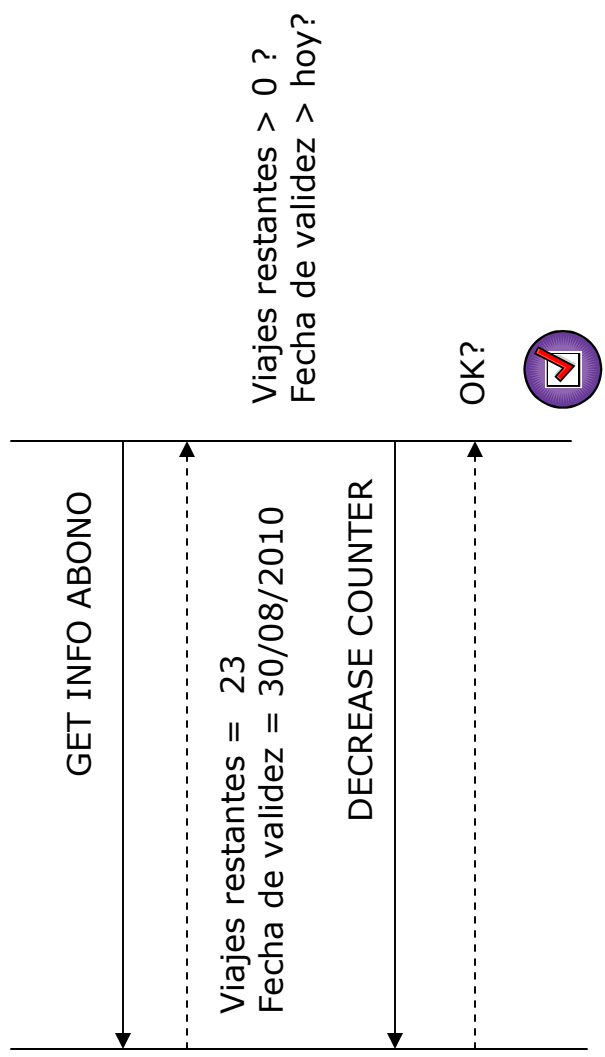
Escenario de ataque : interrupción de la ejecución



Mecanismos de Seguridad de la aplicación : contadores atómicos



Viajes restantes := viajes restantes - 1





Otros escenarios de ataque posibles

- Modificar código de la aplicación o de su ambiente de ejecución.
- Instalación de aplicaciones maliciosas en el dispositivo.
- Ataques criptográficos sobre las claves de la aplicación:
 - Análisis de consumo simple (SPA),
 - Análisis de consumo diferencial (DPA),
 - Inyección de errores
 - Explotación de errores en criptografía propietaria.
- Lectura óptica de la memoria del dispositivo para extraer las claves.
- Etcétera...



Amenazas y caminos de ataque

- Modificar código de la aplicación o de su ambiente de ejecución.
- Modificar la electrónica del dispositivo.
- Modificar o divulgar datos
 - Leerlos de la memoria
 - Escucharlos a través de canales ocultos
- Modificar o reutilizar comunicación (comandos)
- Explotar ambientes multi-aplicación abiertos
 - Interacción con otras aplicaciones



Plan de la charla

- Servicios emergentes en telefonía celular
- La tecnología NFC
- Un caso de estudio: pago con móvil en STM
 - Problemática de seguridad
 - Mecanismos de seguridad de la aplicación
 - **Arquitectura de seguridad del dispositivo**
 - Algunos problemas a resolver

Arquitectura de seguridad: ubicación de la aplicación



Dispositivo del usuario

=



Teléfono (terminal)

+



Tarjeta SIM



Aplicación

?

?



Características de cada dispositivo

- **Electrónica**
 - Posibilidad de introducir más seguridad a nivel del hardware
- **Modularidad**
 - Arquitectura del software embarcado en el dispositivo
- **Ciclo de desarrollo**
 - Duración de vida del dispositivo

Características de la tarjeta SIM



- Electrónica: simple
 - Permite introducir seguridad específica muy elevada a nivel del hardware con bajo costo (varios niveles físicos, detectores de luz y apertura, ofuscación y cifrado de la memoria, disimulación del consumo eléctrico, etc.).
- Modularidad: poca
 - Desarrollo monolítico fundido en silicio.
 - Pocas partes intercambiables.
 - Mejora con la introducción de estándares abiertos: Java Card, GlobalPlatform.
- Ciclo de desarrollo: largo y lento
 - Costo elevado de corrección de errores
 - Certificaciones de seguridad tradicionalmente requeridas.

Características del terminal (1/3)



- Electrónica: compleja
- Casi una computadora personal.
- Varios componentes: CPU, diferentes memorias, numerosos periféricos: teclado, pantalla, red telefónica, Bluetooth, puerto infrarrojo, GPS, extensiones de memoria, chipset NFC, etc...
- Alta miniaturización y frecuencias más grandes.
- Modelo de ejecución más complejo: concurrencia, código distribuido en varios componentes, etc.
- Innovaciones y conectividad en aumento todos los días.



Características del terminal (2/3)

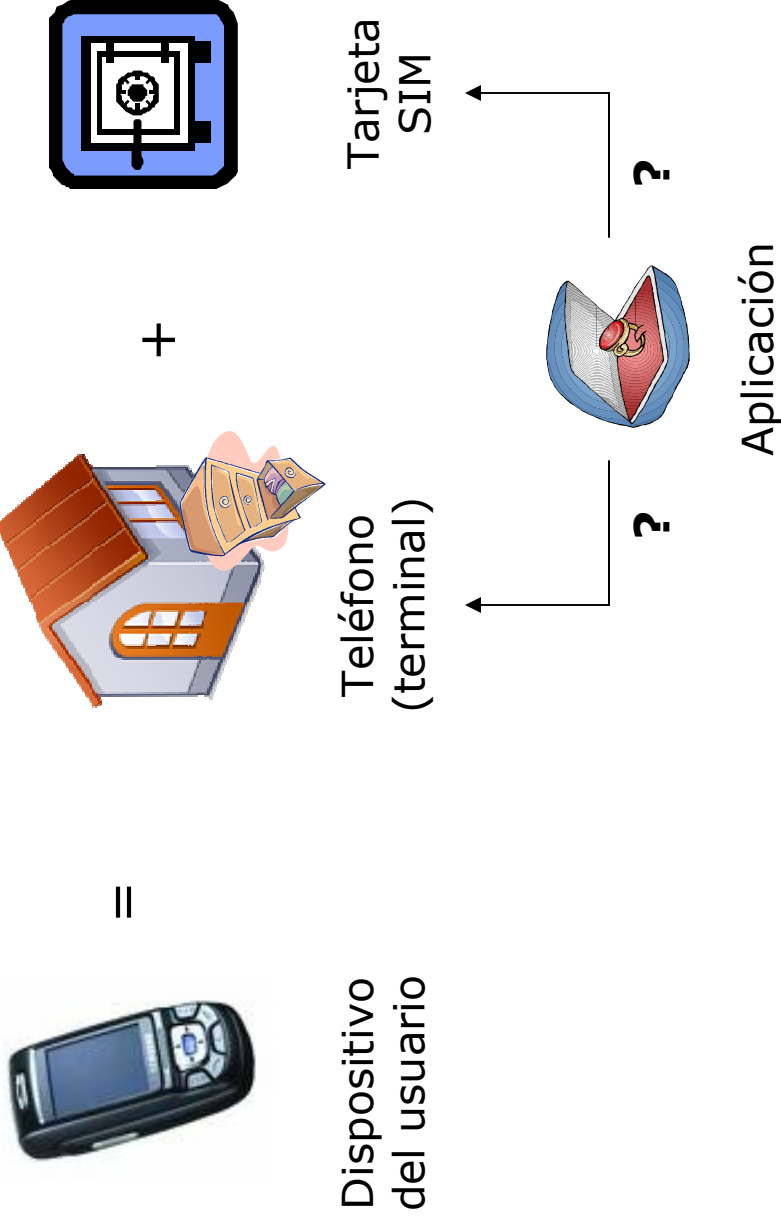
- Modularidad: alta
- Deriva de la alta complejidad del dispositivo y de su evolución constante.
- Muchos proveedores, cada uno especializado en una parte del dispositivo.
- Muchas versiones de cada hardware y software.
- Niveles de seguridad heterogéneos.



Características del terminal (3/3)

- Ciclo de desarrollo: muy corto
- Modelo económico:
 - Vendible a precio elevado durante algunos meses
 - Luego a precio de saldo (poco interesante).
- Consecuencias:
 - Testeo muy rápido
 - Incluye mecanismo de puesta al día del firmware
 - Modelos de certificación tradicional no aplicables
 - Primeras versiones testeadas por usuarios.

Arquitectura de seguridad: ubicación de la aplicación



Arquitectura de seguridad: implicancias del modelo comercial



=



+



Dispositivo
del usuario

Teléfono
(terminal)

Tarjeta
SIM

**Pertenece al
fabricante del
teléfono o al
usuario**

**Pertenece al
operador de la
red telefónica**



Plan de la charla

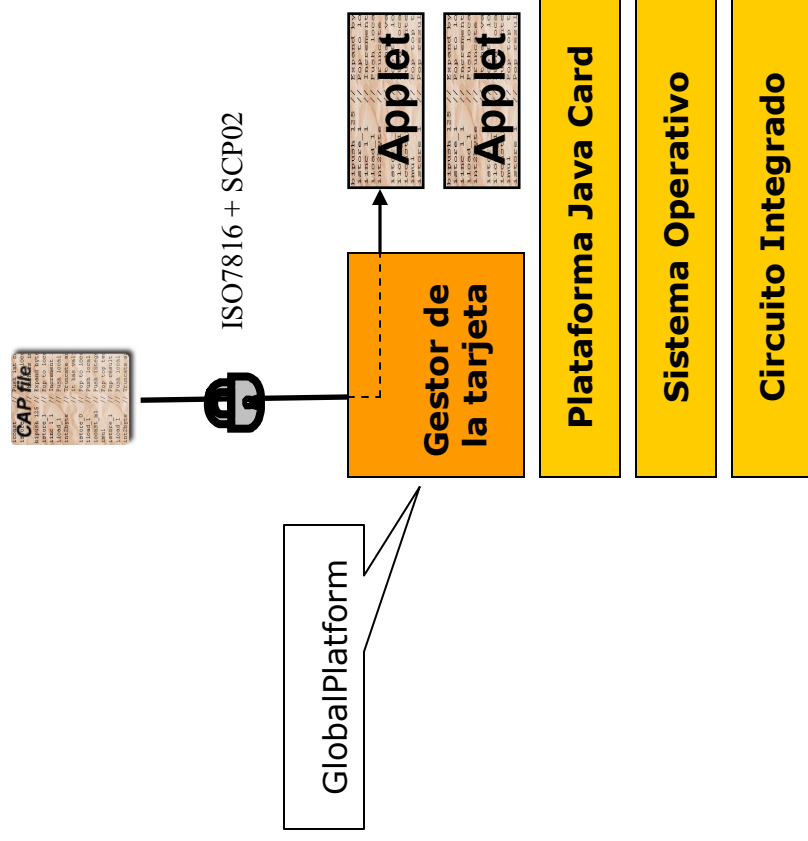
- Servicios emergentes en telefonía celular
- La tecnología NFC
- Un caso de estudio: pago con móvil en STM
 - Problemática de seguridad
 - Mecanismos de seguridad de la aplicación.
 - Arquitectura de seguridad del dispositivo
- **Algunos problemas a resolver (OTA)**



El estándar GlobalPlatform

- Estándar desarrollado por un consorcio de industriales vinculados a las tarjetas inteligentes.
- Especificaciones públicas:
 - <http://www.globalplatform.org>
- Orientado a tarjetas abiertas y multi-aplicación.
- Describe como gestionar este tipo de tarjetas.

Tarjetas multi-aplicación abiertas

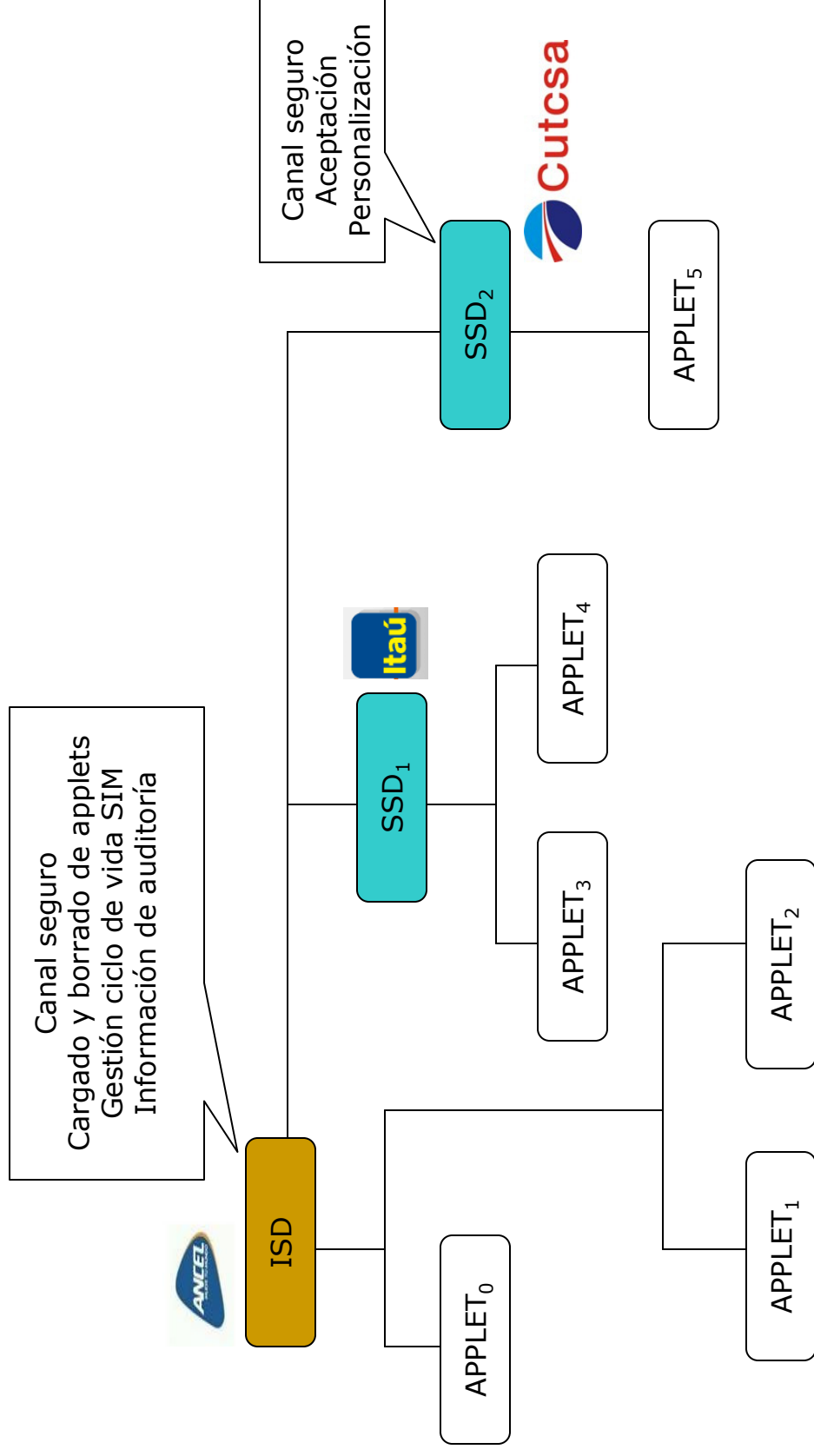




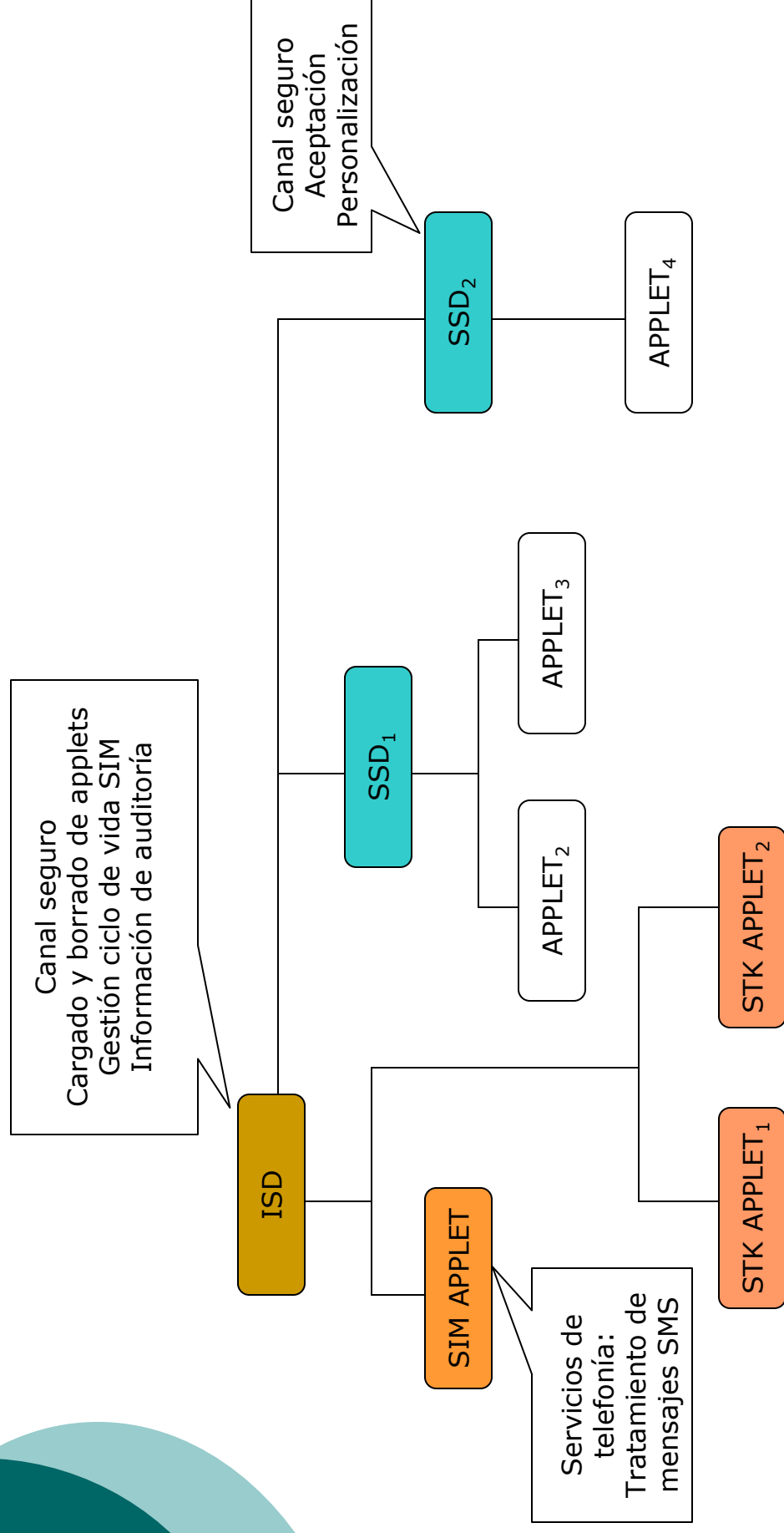
Roles definidos en GlobalPlatform

- Card Issuer:
 - Propietario de la tarjeta
 - Contrapartida: *Issuer Security Domain*
- Application Provider
 - Proveedor de aplicaciones
 - Ejemplo: de transporte, bancarias, etc.
 - Contrapartida: *Supplementary Security Domain*
- Usuario:
 - Interactúa con la tarjeta a través de comandos APDU

Modelo de gestión GlobalPlatform



Modelo de gestión SIM

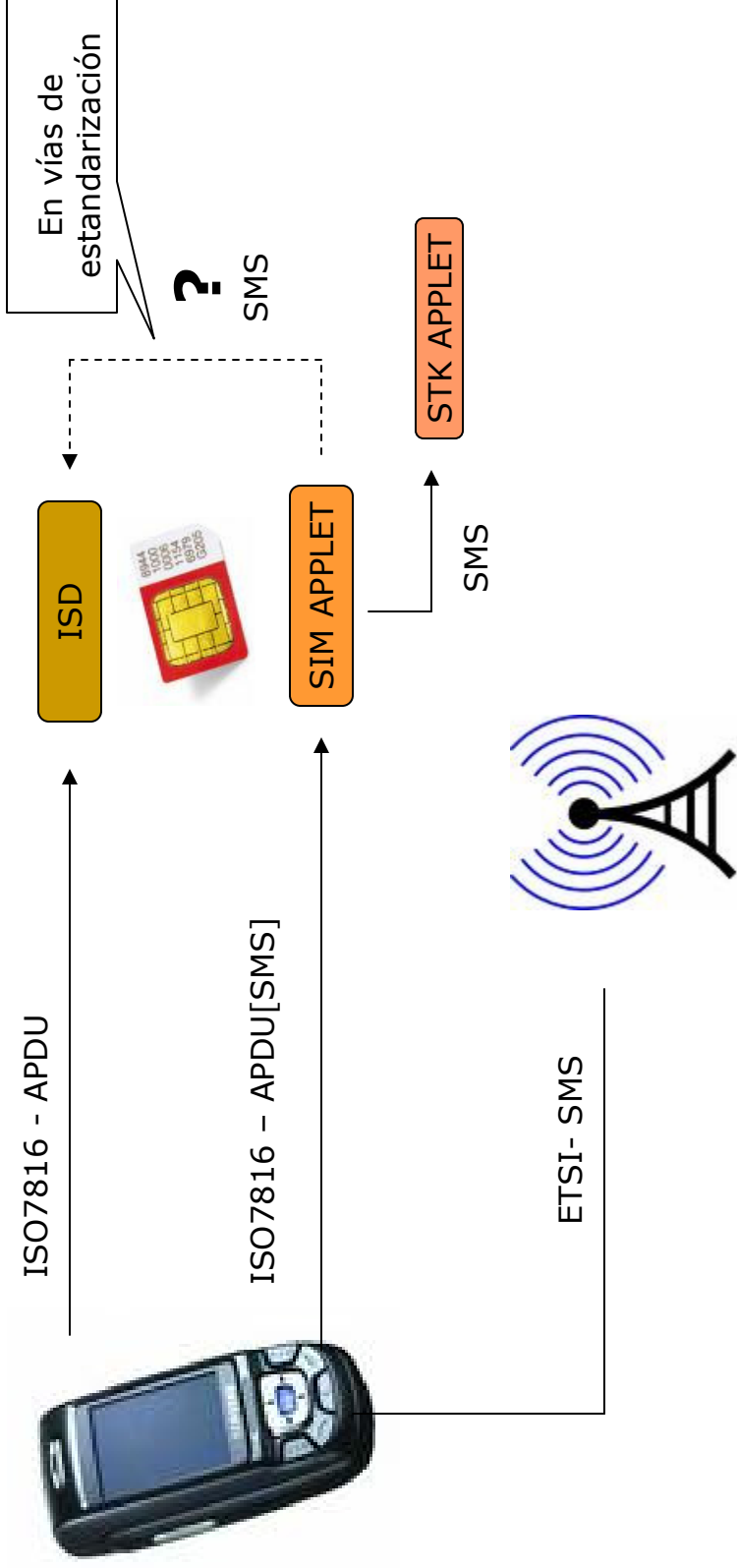




Algunos puntos a resolver en OTA

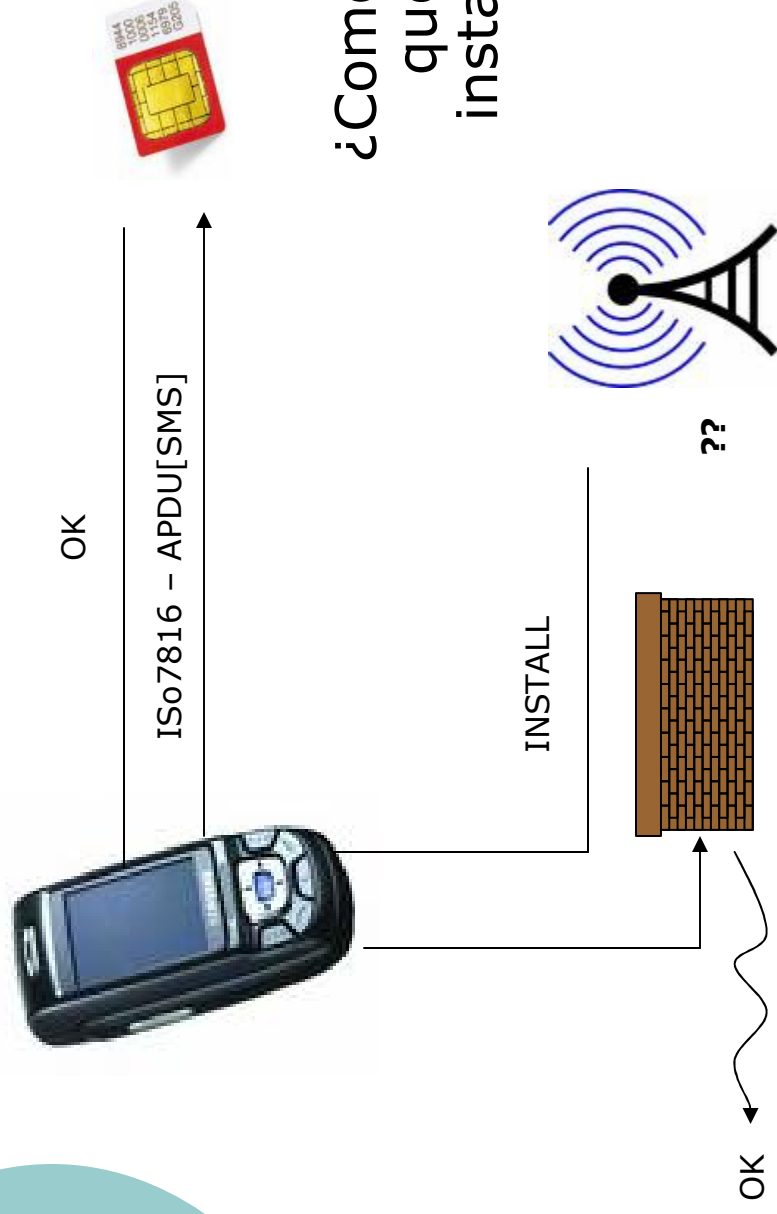
- Modelo de comunicación con la SIM
- Distribución de claves
- Confirmación de instalación

Comunicaciones con la SIM



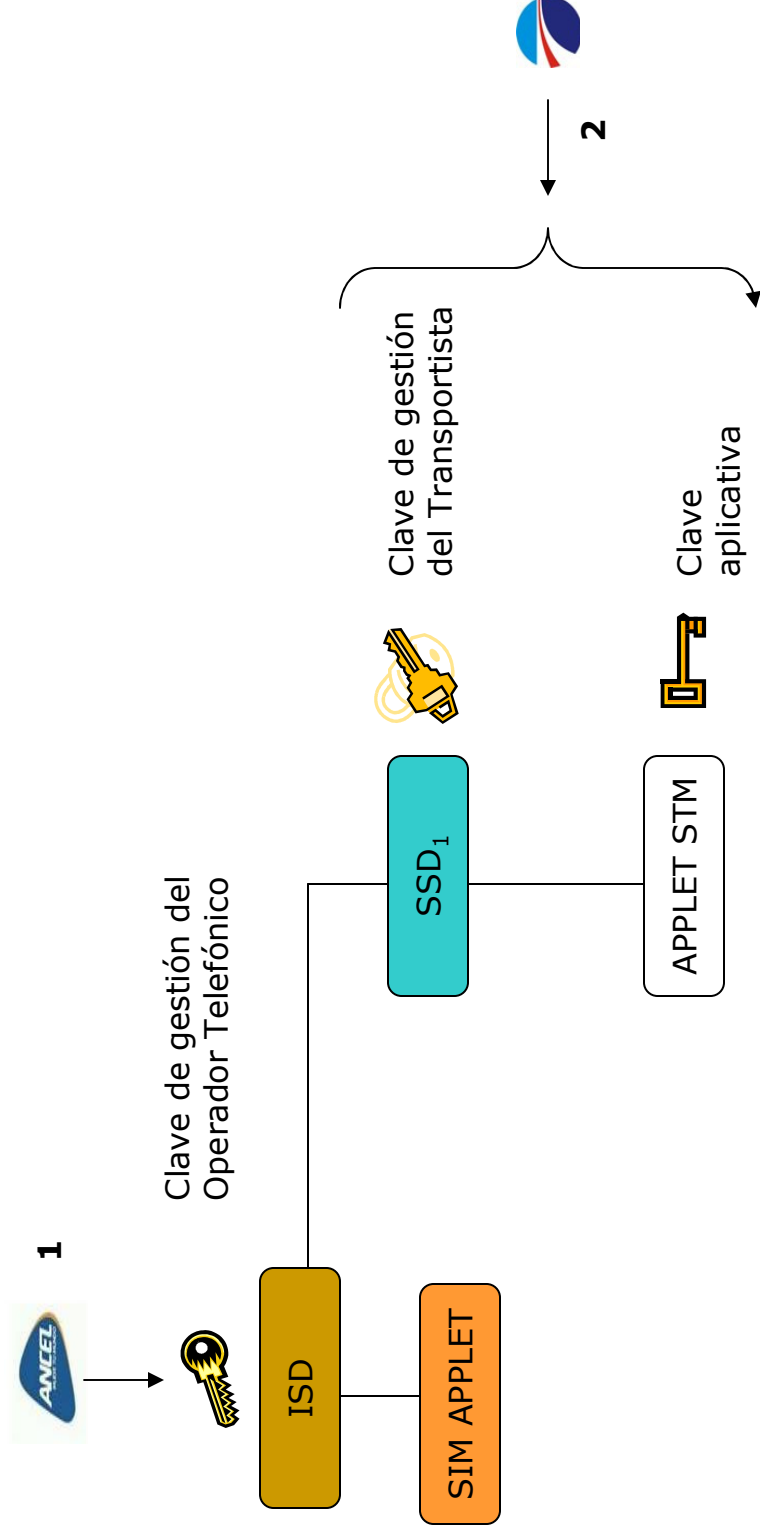
¿Como transmitir el código de una applet por SMS?

Confirmación de instalación en OTA

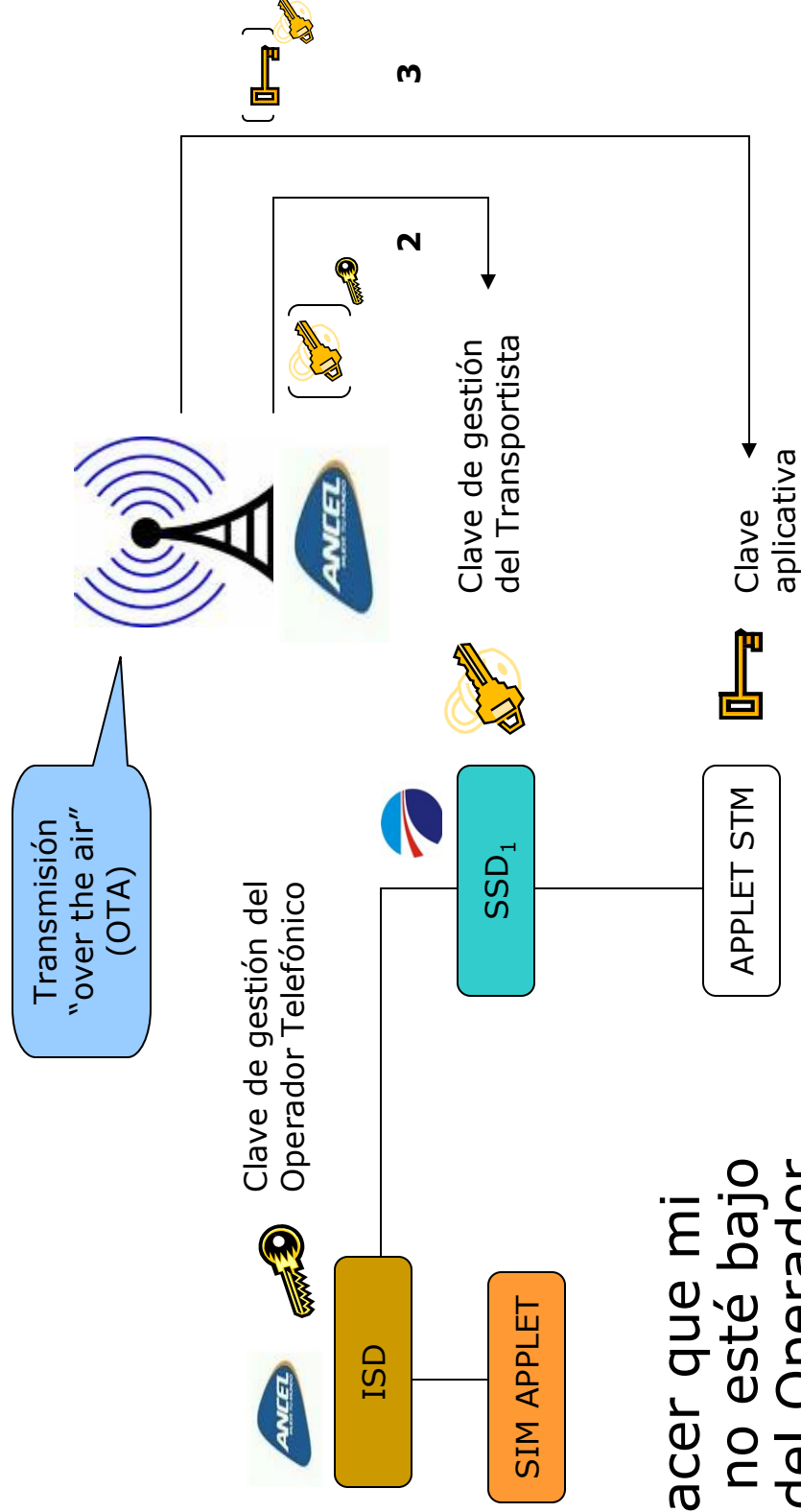


¿Como estar seguro de que la aplicación se instaló correctamente?

Personalización tradicional (tarjeta plástica)



Personalización OTA (Over The Air)



¿Cómo hacer que mi negocio no esté bajo control del Operador Telefónico?



Conclusiones

- La tecnología NFC ofrece potencialidades interesantes para desarrollar aplicaciones embebidas en SIM con alto nivel de seguridad.
- Es técnicamente posible desplegar una aplicación NFC de transporte segura.
- Algunos problemas técnicos quedan por resolver, pero estarán resueltos muy pronto.
- Las principales dificultades a resolver son organizacionales y de negocios más que técnicas.



¡Gracias!

¿Preguntas?