



Monitoreo de dispositivos móviles

*Un análisis de escenarios y
propuesta de solución*

El análisis de escenarios y la propuesta de solución



El problema



DOA - El concepto



Overlay de Información



Propuesta de Arquitectura



Conclusiones

- Los dispositivos móviles
 - Tiene cada vez más funciones agregadas
 - Tiene añadida más tecnologías
- Las personas son cada vez más dependientes de su dispositivo móvil
- Los modelos sofisticados son símbolos de estatus
- Como consecuencia : La tasa de robos y hurtos va en aumento

- En el futuro :
 - IoT e M2M exigirán más tecnologías integradas
 - Las estafas son cada vez más sofisticados

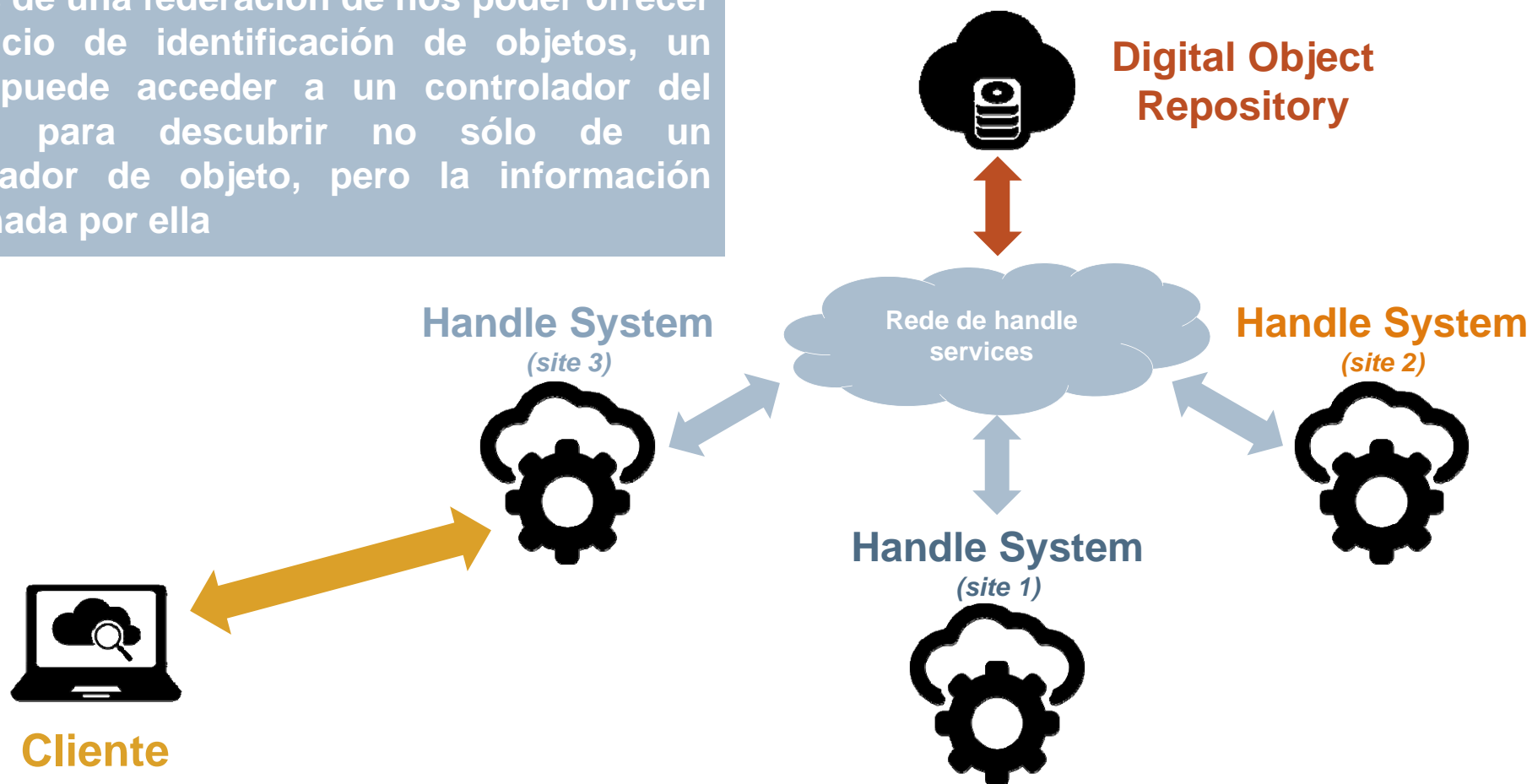
Cómo combatir el robo y el fraude?

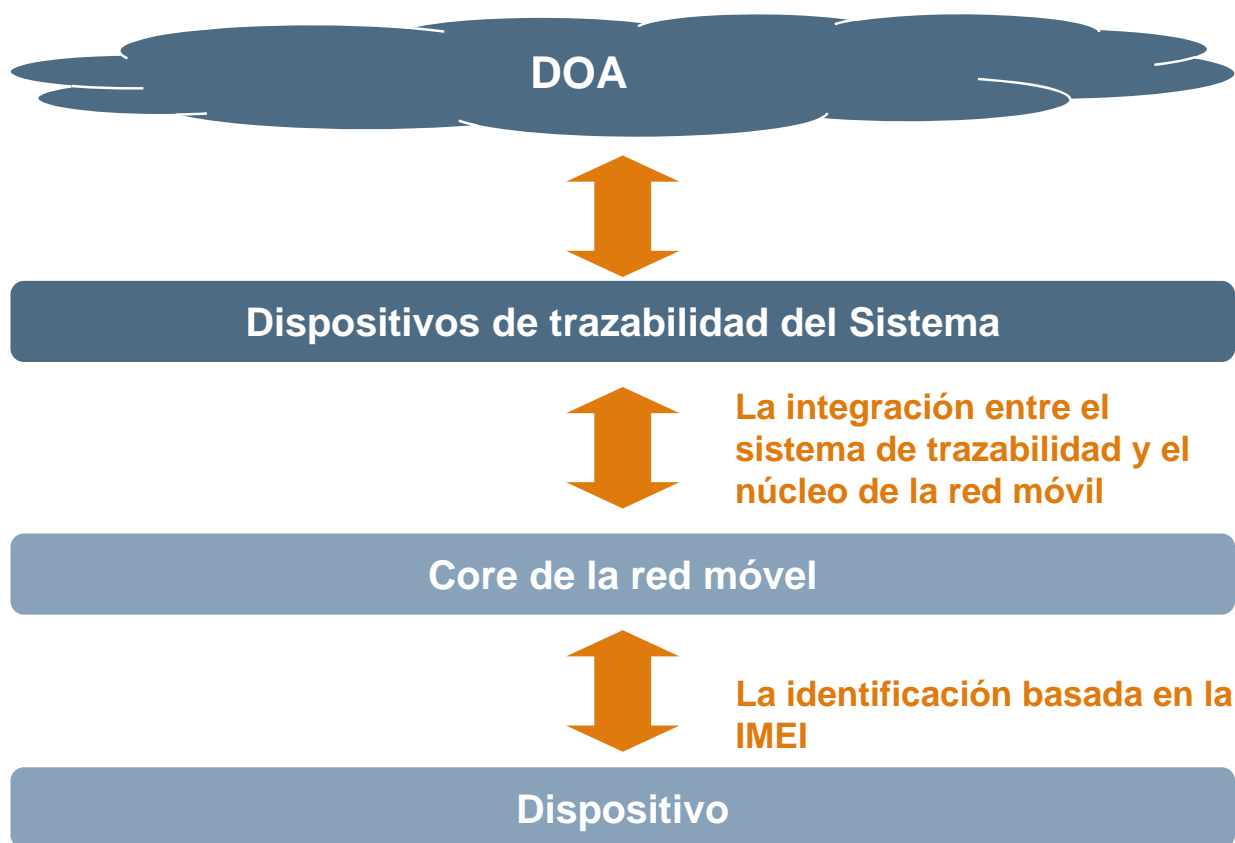
Resp : Un sistema de vigilancia basado en la arquitectura de identificación de objetos (DOA) propuesto por la UIT

Digital Object Architecture – El concepto



A través de una federación de nos poder ofrecer el servicio de identificación de objetos, un cliente puede acceder a un controlador del sistema para descubrir no sólo de un identificador de objeto, pero la información almacenada por ella

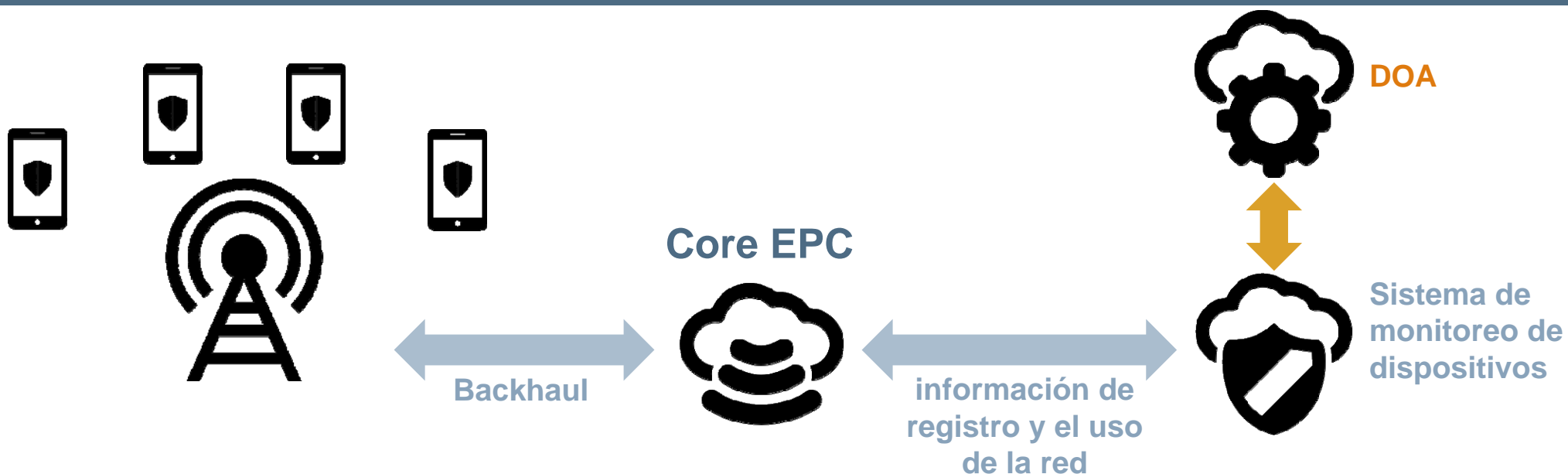




Utilizando la arquitectura de objetos digitales para identificar cada dispositivo en una perspectiva lógica, que une esta identificación con su ID de red (IMEI)

Almacenamiento de información de la historia en el propio repositorio de objetos digitales, lo que permite la detección de fraude

Propuesta de Arquitectura



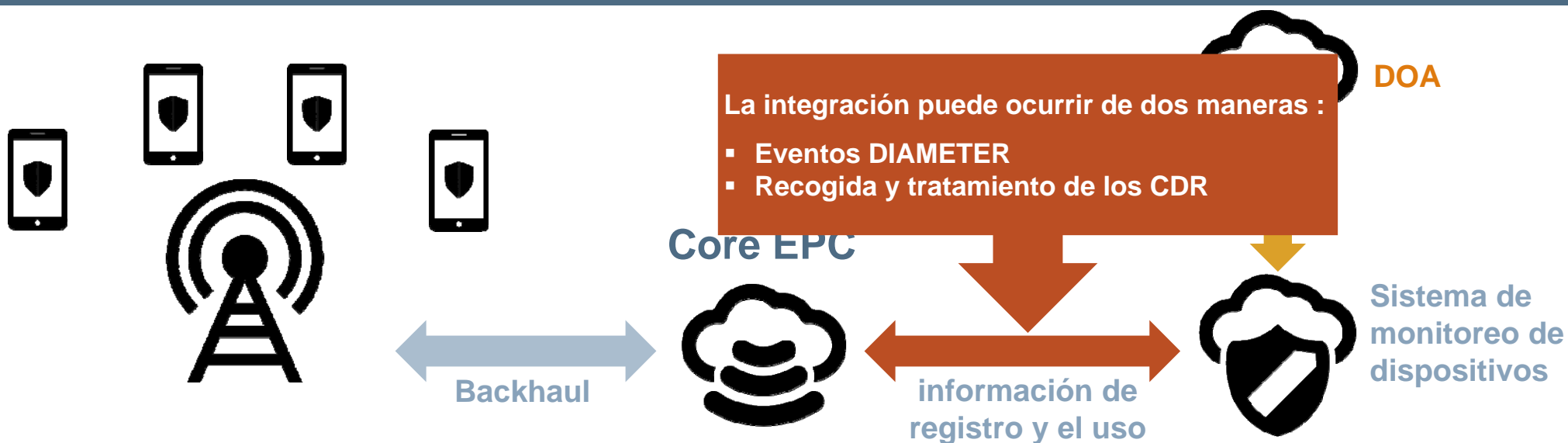
El sistema recoge la información sobre el registro y el uso de redes de dispositivos controlados cada uno

Con cada nuevo acceso a la red de cualquier operador, la historia del dispositivo se actualiza

La historia de cada dispositivo se almacena en el centro, bajo el Repositorio de Objetos Digitales.

Detectando un acceso anómalo, el sistema notifica a las autoridades responsables

Propuesta de Arquitectura



Suscripción de Eventos Diameter

+ Recopilación de información en tiempo real
Fuente creíble, sin intervención humana
Basado en estándares de la industria (3GPP)

- Solución más intrusivo con bajo riesgo a la red
Requiere la cooperación de los operadores

Recogida y tratamiento de los CDR

+ No presenta afectación de riesgo en la red
Menos intrusivo en el operador
Permite el procesamiento por lotes

- Padrones menos formales
Susceptible a la Intervención humana

- El modelo propuesto permite el mantenimiento de la identificación estándares de la industria
- Es una acción menos invasiva: protege la privacidad del usuario
- Permite una acción integrada entre los operadores y reguladores
- Añade confianza en el sistema
- Puede ser económicamente autosustentavel
- Es una preparación de los dispositivos para el futuro
- Inhibe el fraude y el robo

Gracias!

Leonardo Elias Mariote
Paulo José Pereira Curado