Universidad
Carlos III de Madrid

INGENIERÍA EN INFORMÁTICA
PROYECTO FIN DE CARRERA

Extensión de NCTUns 5.0 para simular el entorno de infraestructura y desarrollo del sistema de representación de indicadores para EVIGEN

Alumno: Sergio García Rueda
Profesor Tutor: José María de Fuentes García-Romero de Tejada

Octubre, 2010

Índice

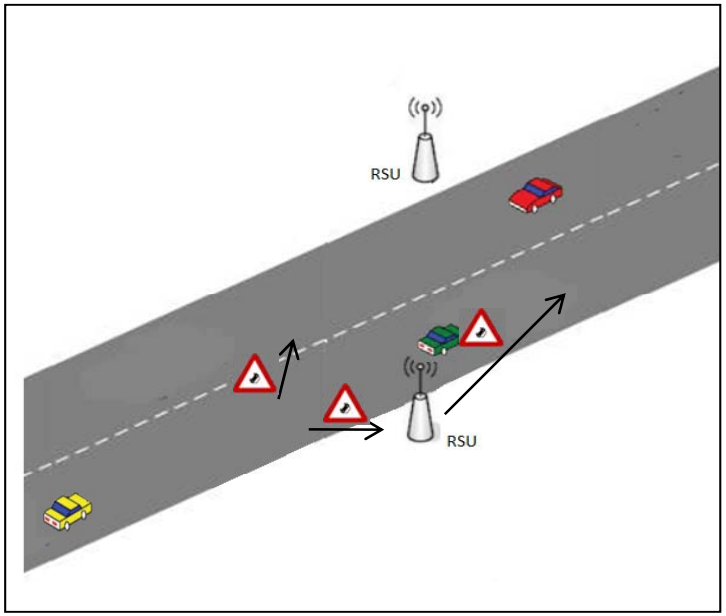
- Introducción.
- Motivación.
- Objetivos.
- Descripción del sistema.
- Conclusiones y líneas futuras.

Índice

- **Introducción.**
- Motivación.
- Objetivos.
- Descripción del sistema.
- Conclusiones y líneas futuras.

Introducción. Redes vehiculares

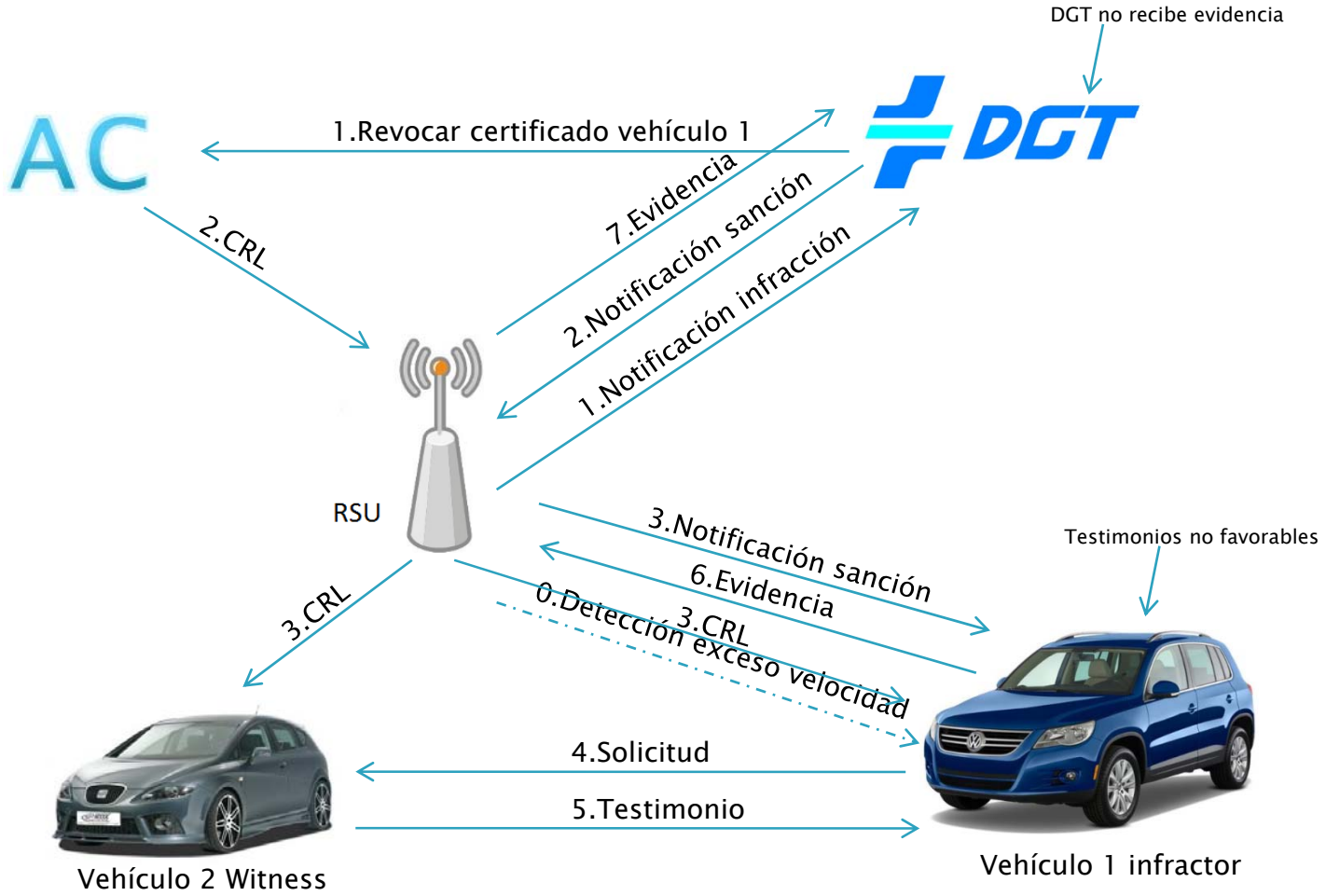
- Entidades participantes.
  - Vehículos (OBU).
  - Infraestructuras (RSU).
- Comunicación.
  - OBU-OBU.
  - OBU-RSU o RSU-OBU.
- Fuerte desarrollo.
  - Nuevos servicios o aplicaciones que ofrecen:
    - Mejoras en seguridad vial.
    - Mejoras en la actividad de conducción.
  - Protocolo EVIGEN.



Introducción. Protocolo EVIGEN (I)

- Propósito: crear evidencias en entornos vehiculares.
  - Demostrar correcto comportamiento ante una infracción en contra de la seguridad vial.
  - Evidencia creada en base a testimonios aportados por vehículos cercanos.
- Participantes:
  - Entorno inalámbrico:
    - Vehículo infractor (*Requester*).
    - Vehículo testigo (*Witness*).
    - Vehículo no equipado (*NoEquipped*).
  - Entorno de infraestructura:
    - RSU (Road Side Unit).
    - DGT (Dirección General de Tráfico).
    - AC (Autoridad de Certificación).

Introducción. Protocolo EVIGEN (II)



Introducción. Protocolo EVIGEN (III)

- Problemas de seguridad.
  - Comunicación inalámbrica.
  - Elevado número de entidades.
- Servicios de seguridad:
  - Confidencialidad.
  - Integridad.
  - Autenticación.
  - No repudio en emisión.
- Otras amenazas:
  - Ataques de repetición.
  - Ataques de denegación de servicio.

Universidad Carlos III de Madrid

Índice

- Introducción.
- **Motivación.**
- Objetivos.
- Descripción del sistema.
- Conclusiones y líneas futuras.

Motivación

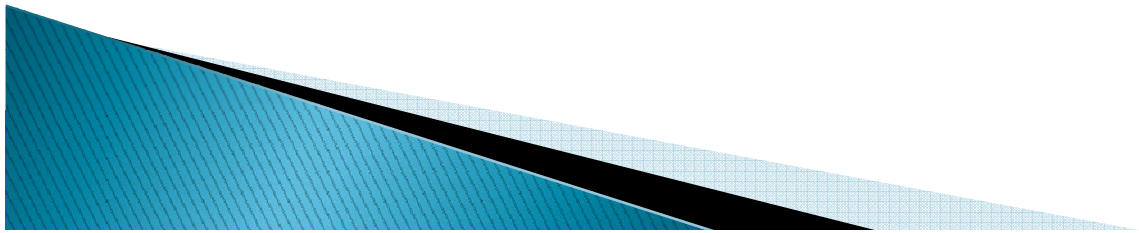
- Elevados costes de implantación en entornos vehiculares.
  - Necesidad de numerosa cantidad de infraestructura situada a lo largo de las carreteras.
  - Grandes pérdidas económicas en caso de fracaso.
- Necesidad de estudiar la viabilidad de las soluciones previamente a su implantación.
  - Determinar su funcionamiento y rendimiento.
- **En el presente Proyecto, estudiar la viabilidad del protocolo EVIGEN.**
- Simuladores de redes vehiculares.
  - Simulación de escenarios con características muy similares a entornos vehiculares reales.
  - Simulador utilizado en Proyecto: NCTUns 5.0.

Índice

- Introducción.
- Motivación.
- **Objetivos.**
- Descripción del sistema.
- Conclusiones y líneas futuras.

Objetivos

- Extender NCTUns 5.0 para la simulación del entorno de infraestructura del protocolo EVIGEN.
- Desarrollar un sistema de representación de indicadores de rendimiento.
- Desarrollar un módulo criptográfico.



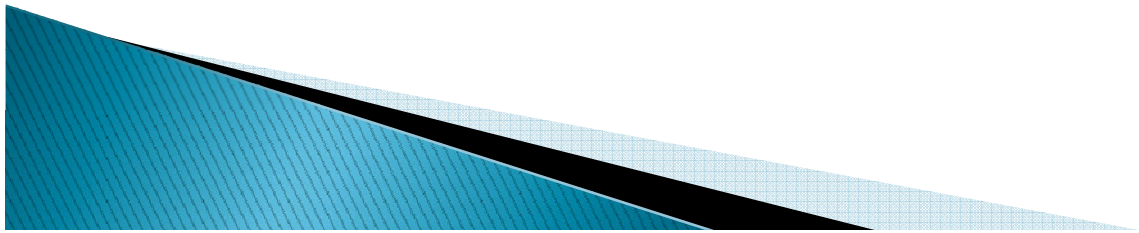
Universidad Carlos III de Madrid

Índice

- Introducción.
- Motivación.
- Objetivos.
- **Descripción del sistema.**
- Conclusiones y líneas futuras.

Descripción del sistema. Análisis

- Dos subsistemas independientes.
  - Extensión del simulador NCTUns 5.0 para simular el entorno de infraestructura de EVIGEN.
  - Sistema de representación de indicadores de rendimiento.
- Módulo criptográfico desarrollado como componente de la simulación del entorno de infraestructura de EVIGEN.



Universidad Carlos III de Madrid

Descripción del sistema. Análisis.

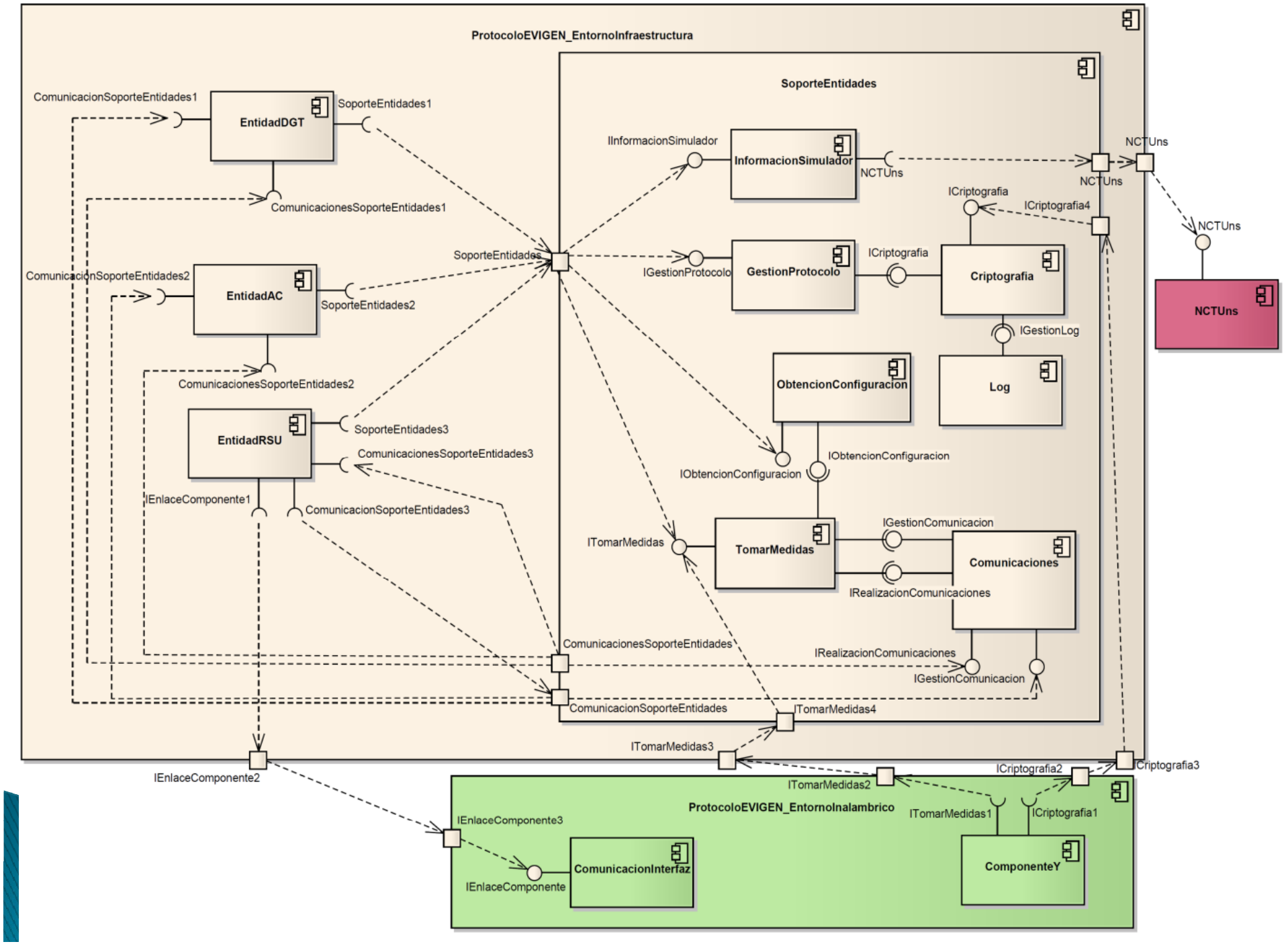
Simulación entorno de infraestructura de EVIGEN

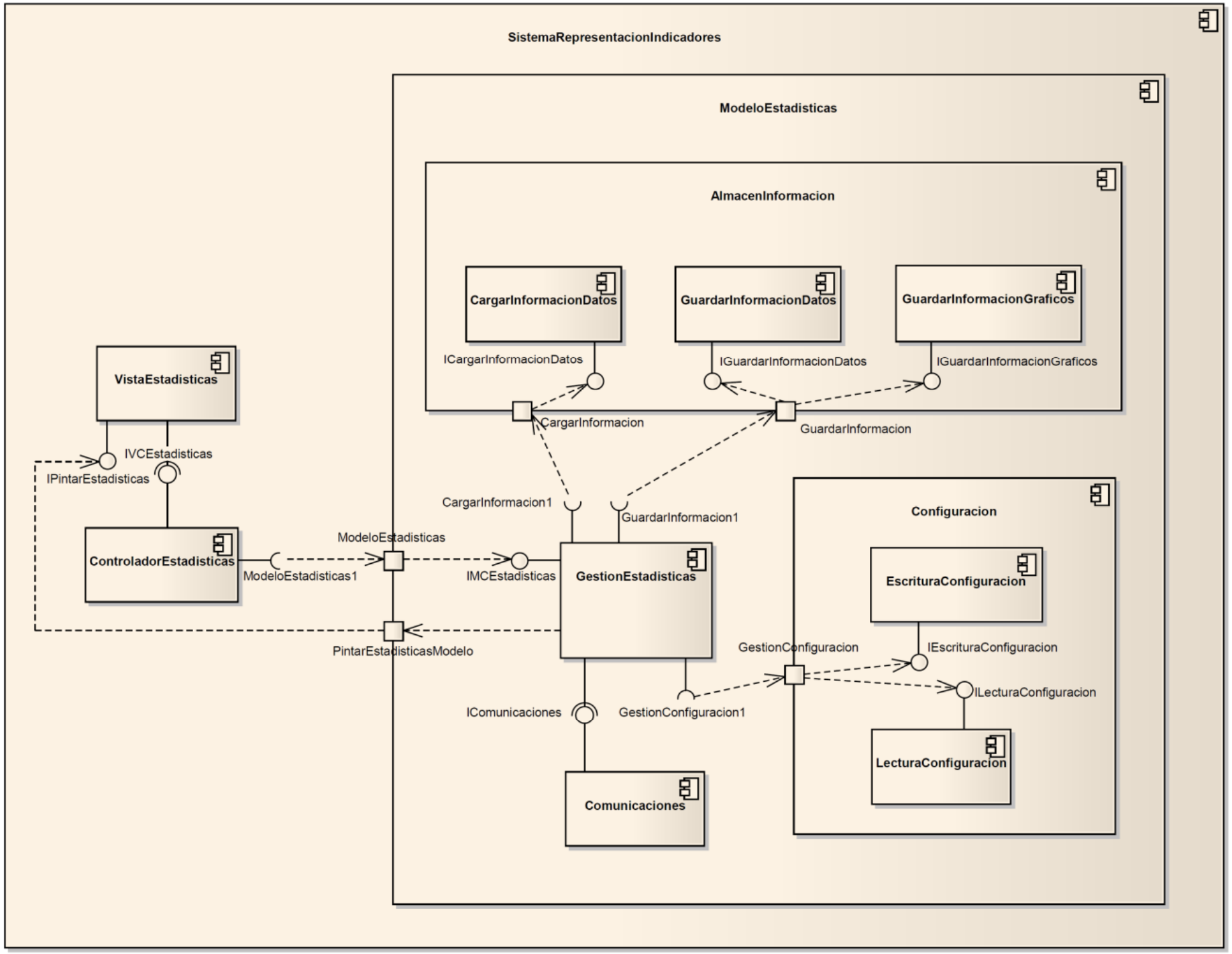
- Simular comportamiento de entidades de infraestructura.
- Otras consideraciones:
  - Reenvío:
    - Notificaciones de sanción.
    - CRL.
  - Sancionar al mismo vehículo una vez en un periodo de tiempo determinado.
  - Notificar infracción del mismo vehículo una vez en un intervalo de tiempo concreto.
  - Log de operaciones criptográficas.
  - Parámetros de configuración de entidades -> ficheros.

Descripción del sistema. Análisis.

Sistema de representación de indicadores

- Representar gráficamente información de indicadores:
  - Número de bytes transmitidos.
  - Tiempo envío/respuesta/computación.
  - Tasas éxito-fracaso finalización protocolo/aceptación-rechazo participación protocolo.
- Estadísticas reflejadas:
  - Gráficas con los valores de los indicadores.
  - Media de los valores de los indicadores (número bytes transmitidos y tiempos).
  - Tasas de los indicadores (éxito y fracaso, y aceptación y rechazo).
  - Número de muestras obtenidas de cada indicador.
- Almacenamiento de estadísticas en PDF.
- Almacenamiento y carga de valores de los indicadores de Excel 2003.


ProtocoloEVIGEN_EntornoInfraestructura
SoporteEntidades
EntidadDGT
EntidadAC
EntidadRSU
InformacionSimulador
GestionProtocolo
Criptografia
ObtencionConfiguracion
Log
TomarMedidas
Comunicaciones
NCTUns
ComunicacionSoporteEntidades1
SoporteEntidades1
ComunicacionesSoporteEntidades1
ComunicacionSoporteEntidades2
SoporteEntidades2
ComunicacionesSoporteEntidades2
SoporteEntidades3
ComunicacionesSoporteEntidades3
IEnlaceComponente1
ComunicacionSoporteEntidades3
IInformacionSimulador
NCTUns
ICriptografia
ICriptografia4
SoporteEntidades
IGestionProtocolo
IGestionLog
IObtencionConfiguracion
ITomarMedidas
IGestionComunicacion
IRealizacionComunicaciones
ComunicacionesSoporteEntidades
ComunicacionSoporteEntidades
ITomarMedidas4
ITomarMedidas3
IEnlaceComponente2
ICriptografia2
ICriptografia3
ITomarMedidas2
ProtocoloEVIGEN_EntornoInalambrico
ITomarMedidas1
ICriptografia1
IEnlaceComponente3
ComunicacionInterfaz
IEnlaceComponente
ComponenteY

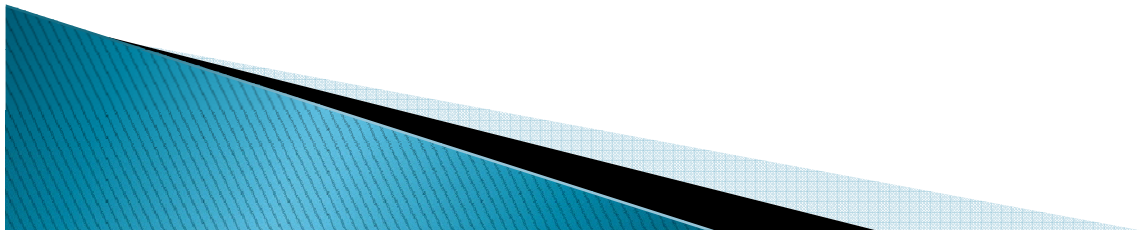

SistemaRepresentacionIndicadores
ModeloEstadisticas
AlmacenInformacion
CargarInformacionDatos
GuardarInformacionDatos
GuardarInformacionGraficos
ICargarInformacionDatos
IGuardarInformacionDatos
IGuardarInformacionGraficos
CargarInformacion
GuardarInformacion
VistaEstadisticas
IVCEstadisticas
IPintarEstadisticas
CargarInformacion1
GuardarInformacion1
Configuracion
ControladorEstadisticas
ModeloEstadisticas
ModeloEstadisticas1
IMCEstadisticas
GestionEstadisticas
EscrituraConfiguracion
PintarEstadisticasModelo
GestionConfiguracion
IEscrituraConfiguracion
ILecturaConfiguracion
IComunicaciones
GestionConfiguracion1
LecturaConfiguracion
Comunicaciones

Descripción del sistema.
Implementación.

- Ver video.

Descripción del sistema.
Implementación. Módulo criptográfico

- Utiliza librería criptográfica de OpenSSL.
- Ofrece soporte para:
  - Cifrado y descifrado asimétrico con RSA.
  - Cifrado y descifrado simétrico con AES-CCM.
  - Realización y verificación de resumen SHA1.
  - Firma y su verificación con RSA.
  - Validación de certificados X509.



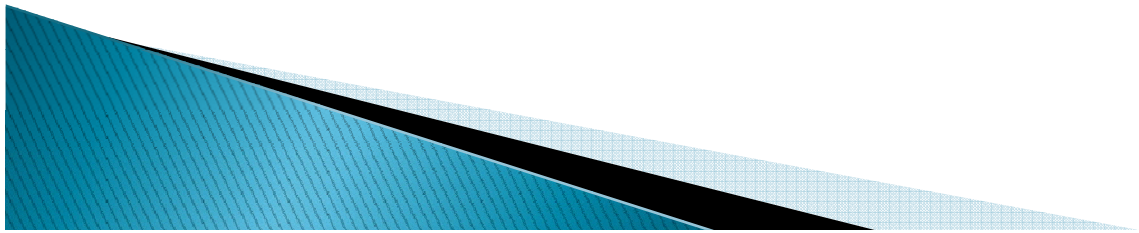
Universidad Carlos III de Madrid

Índice

- Introducción.
- Motivación.
- Objetivos.
- Descripción del sistema.
- **Conclusiones y líneas futuras.**

Conclusiones y líneas futuras (I)

- Objetivos cumplidos:
  - Simular el entorno de infraestructura de EVIGEN en NCTUns 5.0.
  - Herramientas para estudiar el funcionamiento y rendimiento de EVIGEN.
  - Desarrollo de un módulo criptográfico.
- Aspectos aprendidos:
  - Desarrollo de un proyecto mediante técnicas de Ingeniería del Software.
  - Afrontar los problemas presentes durante el Proyecto.
  - Mayor capacidad de investigación.



Universidad Carlos III de Madrid

Conclusiones y líneas futuras (II)

- Dificultades:
  - Trabajo en solitario.
  - Integración en una aplicación ya existente.
  - Complejidad implementación considerable:
    - Implementación de distintos sistemas.
    - Cantidad de funcionalidad a desarrollar adecuada.
    - Gran número de comunicaciones.
    - Uso de tecnología no conocida.
  - Integración con otro Proyecto desarrollado en paralelo.

Conclusiones y líneas futuras (III)

- Líneas futuras:
  - Incluir nuevos tipos de infracciones.
  - Implementar mecanismos para la detección de infracciones de manera más fiable.
    - Simular sensores en las carreteras.
  - Ampliación de NCTUns para realizar las simulaciones en un entorno distribuido.
    - Resultados más fiables.
  - Integración de la solución implementada en NCTUns 6.0.

Universidad
Carlos III de Madrid

¿PREGUNTAS?