Seguridad en la Información

Trabajo Práctico – Requerimientos

Adel Arja Santiago Nolasco Luis Guanuco*

27 de agosto de 2015

Resumen

Se trabajará sobre la propuesta denominada *TOKER_IUA*. En esta primera entrega se comparten los requerimientos que demandará el proyecto. La figura que acompaña al final del documento complementa el texto.

1. Requerimientos

1. Se utilizará un sistema embebidos de bajo costo y una computadora de escritorio (PC) como dispositivos principales que se comunicarán entre sí.

2. El dispositivo embebido recibirá de la PC, mediante una comunicación serial, un archivo (mensaje) y al mismo se le aplicarán técnicas/algoritmos para conservar:

   - Confidencialidad
   - Autenticidad
   - Integridad

   el nuevo mensaje generado en el sistema embebido será devuelto a la PC. Dónde se comprobarán que se hayan mantenido los items anteriores.

   a) La confidencialidad del mensaje se realiza con alguna técnica de encriptación a definir.

   b) Se autenticará el mensaje utilizando el concepto de "firmas digitales". Se definirán claves públicas y privadas de los dispositivos que participan de la comunicación.

   c) La integridad del mensaje se mantiene utilizando técnicas de digesto.

*contacto: guanucoluis@gmail.com

2. Análisis y Diseño

Cómo primera alternativa se evalúa la siguiente arquitectura a implementar.

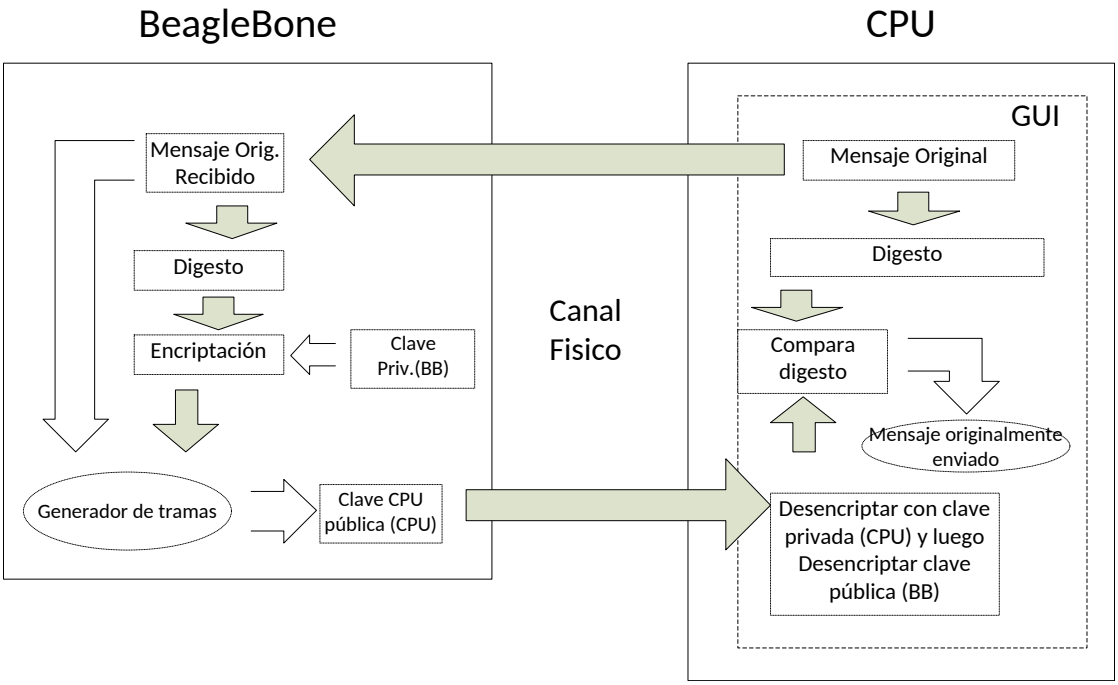

Figura 1: Diagrama general del sistema a implementar.