PAI-5. MOBIFIRMA. DESARROLLO DE PILOTO PARA COMPRAS CON DISPOSTIVOS MÓVILES PARA UNA CORPORACIÓN HOTELERA INTERNACIONAL

Ángel Jesús Varela Vaca
Grupo de Investigación **IDEA Research Group**,
Universidad de Sevilla

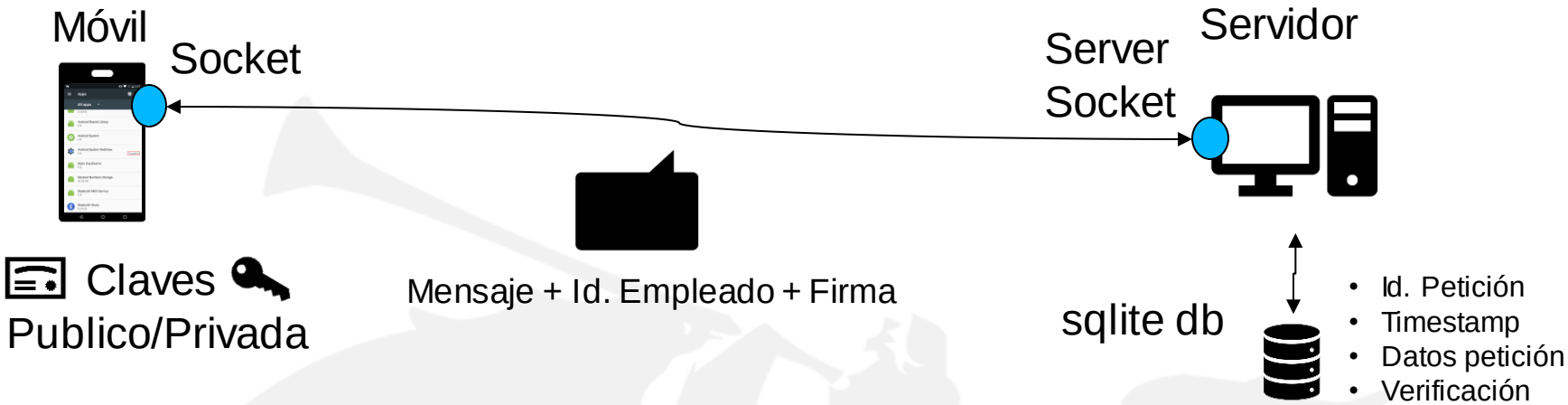
Objetivos

"Todos los mensajes desde los dispositivos móviles sobre ***peticiones de compras de material hostelero deberán ir firmados por el responsable de la petición y transmitirse de forma confidencial e íntegra***. Cada mes el Gobierno de la Seguridad de la Información de la corporación debe ser informado de los porcentajes de peticiones verificadas correctamente su firma y de las tendencias con respecto a los dos meses anteriores."

Se propone a los Security Teams de INSEGUS alcanzar los objetivos siguientes:

1. Arquitectura cliente/servidor Piloto para las compras electrónicas en la corporación. Desarrollar/Desplegar la arquitectura cliente/servidor que permita mensajería autenticada mediante firma digital con dispositivos móviles con el sistema operativo Android que permita firmar las peticiones de compra en el cliente y verifique dicha firma en el servidor. La transmisión por las redes públicas debe ser autenticada, confidencial e íntegra.
2. El servidor debe recoger además de las peticiones de compras, la información necesaria para los indicadores exigidos en la Política de Seguridad Corporativa para que pueda usarse por el Gobierno de la Seguridad de la información de la Corporación respecto a la incorrecta autenticación de los clientes.

Arquitectura Prototipo



Flujo de app:

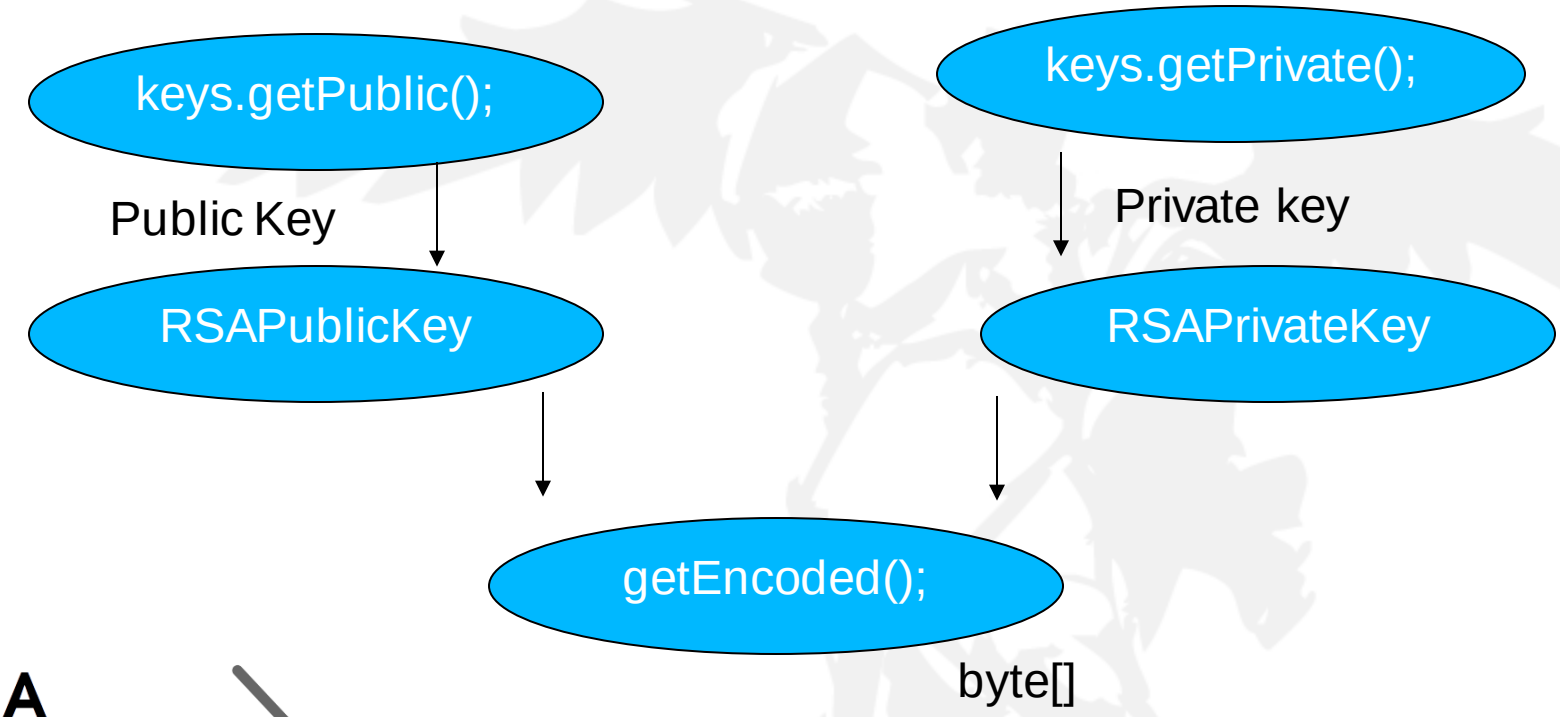
1. Establecer connexion
2. Firmado petición
3. Envio mensaje

Flujo del Server:

1. Abrir socket escucha
2. Verificar firma
3. Almacenar información
4. Capturar KPIs
   - Verificados correcto
   - Verificados incorrecto
5. Enviar informe mensual

Generación claves (RSA-2048)

```
KeyPairGenerator kgen = KeyPairGenerator.getInstance("RSA");
kgen.initialize(2048);

KeyPair keys = kgen.generateKeyPair();
```



Firmado de información (SHA-256+RSA)

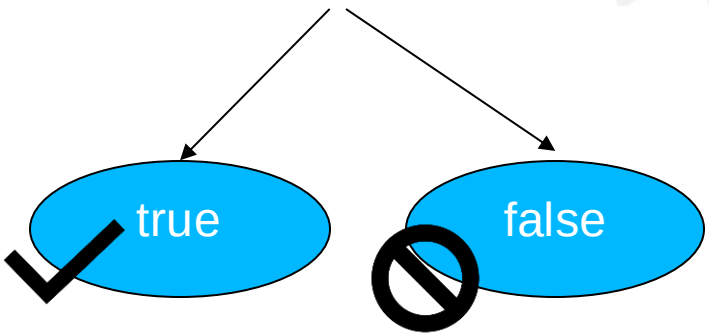
```
Signature sg = Signature.getInstance("SHA256withRSA" … );

sg.initSign(privateKey);

sg.update(message.getBytes());

// Firma
byte[] firma = sg.sign();
```

Security.getProviders()

Verificar firma

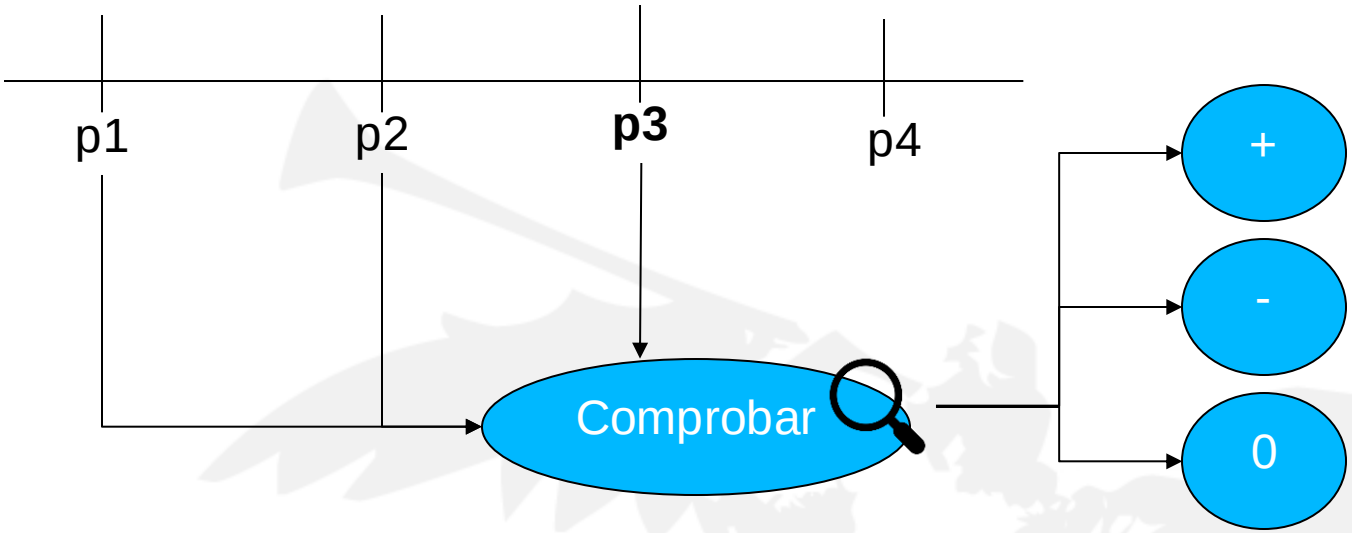
```
Signature sg = Signature.getInstance("SHA256withRSA" … );

sg.initVerify(publicKey);

sg.update(message.getBytes());

// Verification de firma
sg.verify(firma.getBytes())
```

Security.getProviders()



KPI – Ratio de verificación y tendencia

pX = Verificado OK / Total Verificados



Si (p3 > p1 and p3 > p2) or (p3 < p1 and p3 == p2) or (p3 == p1 and p3 > p2)

TENDENCIA POSITIVA

Si (p3 < p1 or p3 < p2)

TENDENCIA NEGATIVA

SI (p3 == p1 and p3 == p2)

TENDENCIA NULA

Entrega

- Cada grupo debe entregar a través de la Plataforma de Enseñanza Virtual y en la **actividad** preparada para ello un archivo zip, nombrado ***PAI5-ST*.zip**, que deberá contener al menos los ficheros siguientes:
  - ✓ **Documento en formato pdf que contenga un informe/resumen del proyecto** con los detalles más importantes de las decisiones, soluciones adoptadas y/o implementaciones desarrolladas, así como el resultado y análisis de las pruebas realizadas (máximo 10 páginas).
  - ✓ **Código fuente de las posibles implementaciones y/o scripts desarrollados y/o configuraciones y/o logs del analizador de código.**

Métricas de valoración

Resumen (30%)

- Tamaño del informe
- Calidad del resumen aportado
- Calidad de pruebas presentadas y resultados

Solución aportada (70%)

- Cumplimiento de requisitos establecidos
- Calidad del código entregado
- Complejidad de la solución
- Respuesta al conjunto de preguntas planteadas
- Pruebas realizadas (tendencias)