ESTUDIO DEL PAGO MÓVIL Y SU SEGURIDAD

Autores:
DIANA TERESA PARRA
RAFAEL MARTÍNEZ-PELÁEZ
CRISTINA SATIZÁBAL

ACIS

CONTENIDO

1. Introducción
2. Funcionamiento del Pago Móvil
3. Requerimientos de los Sistemas
4. Requerimientos de Seguridad
5. Operaciones Criptográficas
6. Longitud de las Claves
7. WPKI (*Wireless Public Key Infrastructure*)
8. WPKI y Seguridad en Pago Móvil
9. Conclusiones

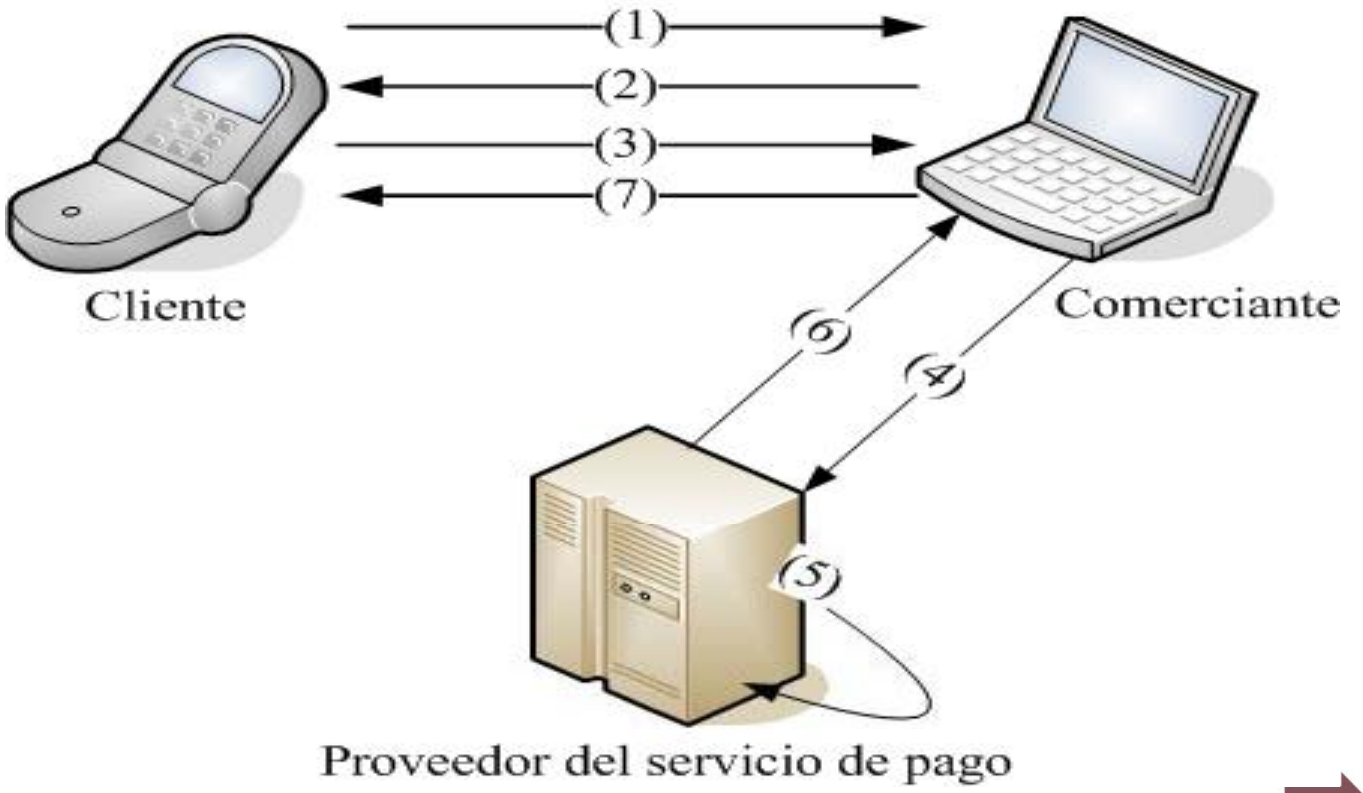
ACIS

1. Introducción

- Convergencia: Comunicaciones móviles e Internet
- PAGO MÓVIL: Intercambio de valores financieros usando dispositivos móviles para pagar por productos y servicios[1]
- Características:
  - Medio de transmisión inseguro
  - Capacidad limitada de dispositivos móviles
  - Necesidad de Seguridad

[1] S S. Nambiar, C-T. Lu y L-R. Liang, "Analysis of payment transaction security in mobile commerce", en *Proceedings of the IEEE International Conference on Information Reuse and Integration, (IRI'04)*, 2004, pp. 475-480.

2. Funcionamiento del Pago Móvil



3. Requerimientos de los Sistemas

- Requerimientos de los Clientes
  - Facilidad de Uso
  - Flexibilidad
  - Interoperatividad
  - Bajo coste de transmisión y operación
  - Escalabilidad
- Requerimientos de los Comerciantes
  - Bajo coste de transmisión y operación
  - Estandarización

4. Requerimientos de Seguridad

- Autenticación de los participantes
- Autorización del pago
- Confidencialidad de la información compartida
- Integridad de los mensajes intercambiados
- No repudio del pago

5. Operaciones Criptográficas

Algoritmo	PDA (seg)	Portátil (seg)
RSA Cifrado	0.0263	0.0004
RSA Descifrado	1.8990	0.0036
RSA Firma	1.8973	0.0014
RSA Verificación	0.0263	0.0004
DES Cifrado	0.0010	0.00001
DES Descifrado	0.0010	0.00001
SHA-2	0.0006	0.00001

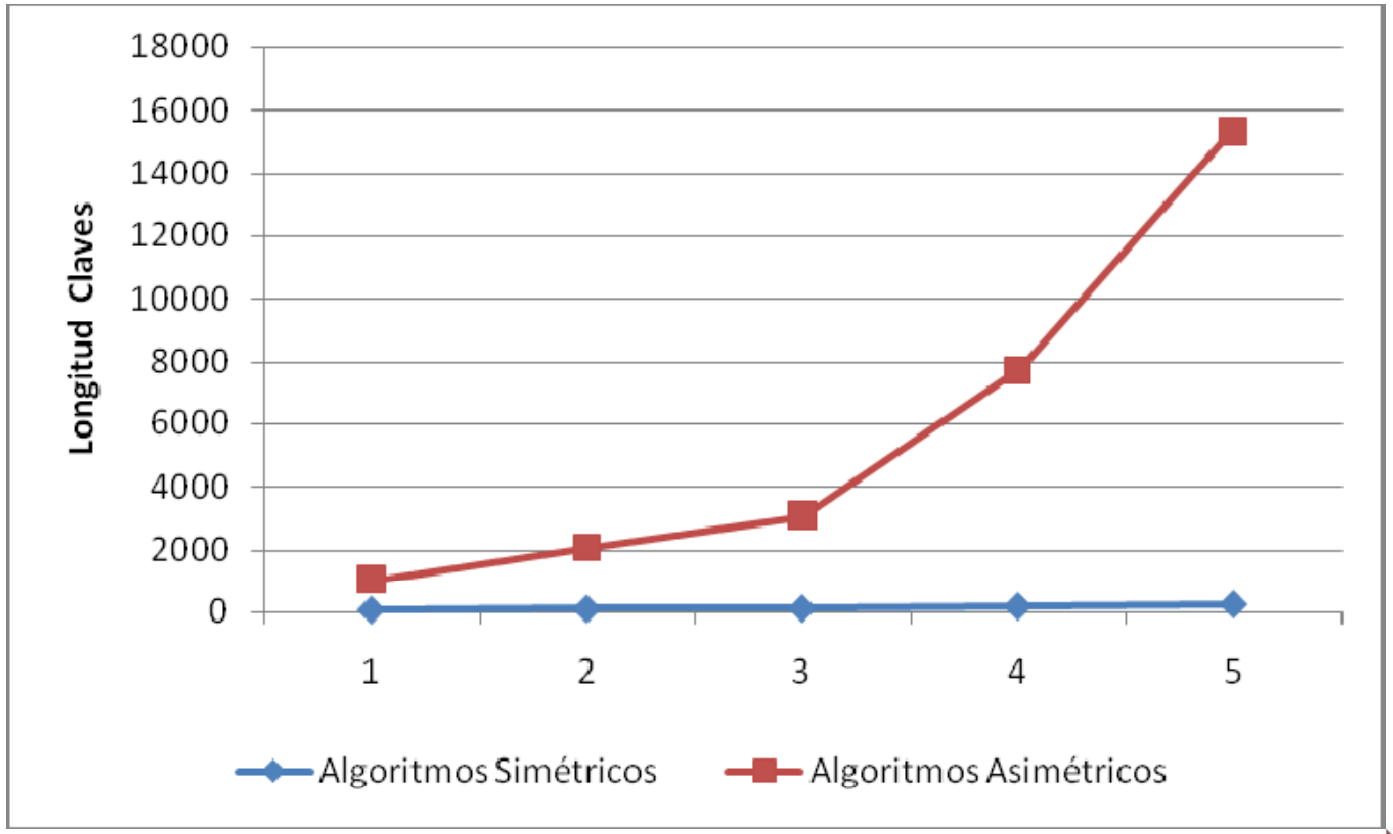
[26] R. Martínez-Peláez, F. Rico-Novella y C. Satizábal, “Study of mobile payment protocols and its performance evaluation on mobile devices”, *International Journal of Information Technology and Management*, pendiente de publicación.

6. Longitud de las Claves

Algoritmos Simétricos			Algoritmos Asimétricos	
DES	**3DES**	**AES**	**RSA**	**DH**
80			1024	1024
	112		2048	2048
		128	3072	3072
		192	7680	7680
		256	15360	15360

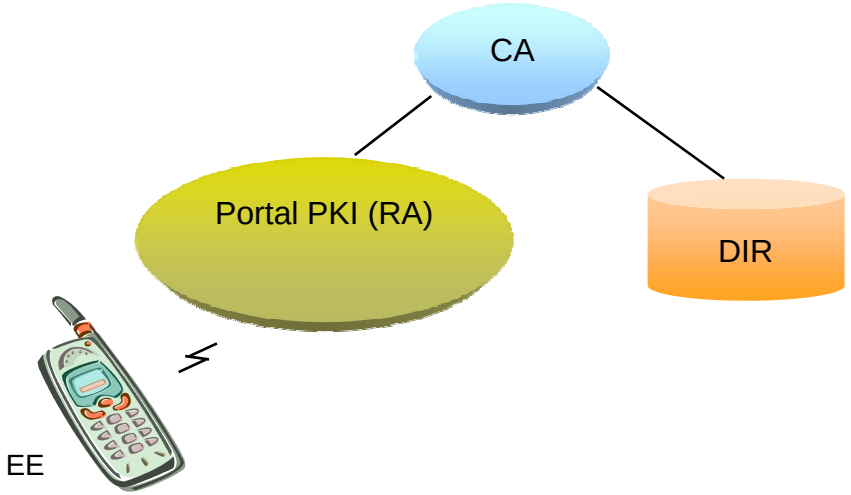
[43] S.A:Vanstone, “Next Generation Security for Wireless: Elliptic Curve Cryptography”. Computers & Security, 2003. 22(5)(5): p. 412-415.

6. Longitud de las Claves



7. WPKI (*Wireless Public Key Infrastructure*)

- Optimización de PKI para el entorno inalámbrico. Optimiza:
  - Protocolos
  - Formato de los certificados
  - Algoritmos criptográficos y claves



8. WPKI y Seguridad en Pago Móvil

- Autenticación mutua a través de WTLS
- Autorización del pago a través de firma digital
- Confidencialidad de la información a través de WTLS
- Integridad de los mensajes a través de funciones de Hash
- No repudio del pago con firma digital

9. Conclusiones

- Pago móvil requiere seguridad por importancia de información compartida y medio inseguro
- Implementación de seguridad difícil por capacidades limitadas de dispositivos móviles
  - Algoritmos asimétricos requieren mayor tiempo de ejecución de operaciones criptográficas (En PDA, DES sólo toma 38% del tiempo requerido con RSA para cifrar y 5% del tiempo para descifrar)
  - Algoritmos asimétricos requieren mayor espacio en memoria para las claves (90% más espacio que algoritmos simétricos)
- WPKI permite implementar servicios de seguridad, pero:
  - Gran tamaño de certificados
  - Verificación de caminos de certificación

ACIS

GRACIAS!!!!

UNIVERSIDAD DE PAMPLONA
COLOMBIA

ACIS