Generación de tokens para proteger los datos de tarjetas bancarias

Trabajo terminal No. 2017-B008

Presentan

Daniel Ayala Zamorano

daz23ayala@gmail.com

Laura Natalia Borbolla Palacios

ln.borbolla.42@gmail.com

Ricardo Quezada Figueroa

qf7.ricardo@gmail.com

Directora

Dra. Sandra Díaz Santiago

Ciudad de México, 9 de noviembre de 2018

Escuela Superior de Cómputo

Instituto Politécnico Nacional

Contenido

Recapitulación, contenido

¿Qué es la tokenización?

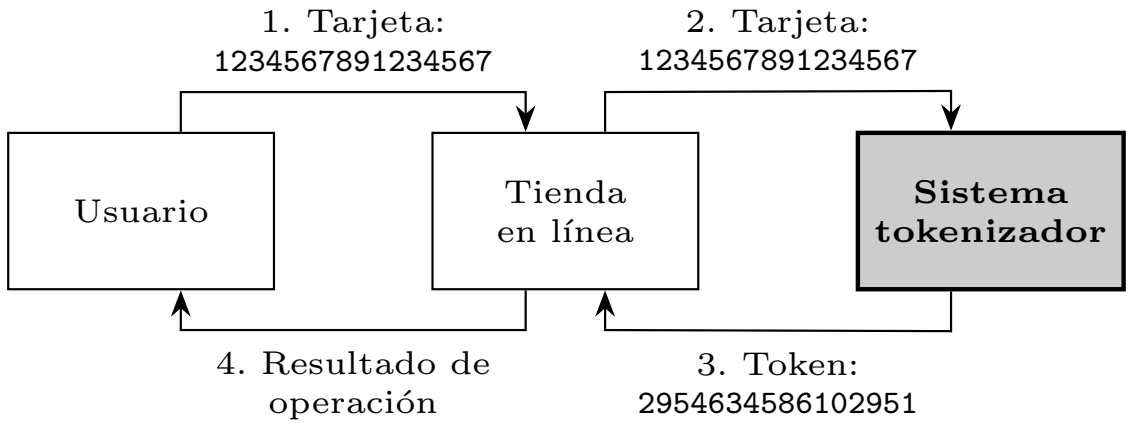
Tokenización en otros contextos

- Moneda de uso particular sin valor legal.
- Componente de seguridad en la comunicación por sesiones.
- Componente léxico de una gramática.

¿Qué es la tokenización?

Tokenización en criptografía

- Es la sustitución de datos sensibles por valores representativos sin una relación directa.
- Existen muchas empresas que proveen el servicio de tokenización, pero lo hacen sin detallar la forma en la que se realiza [1]-[3].

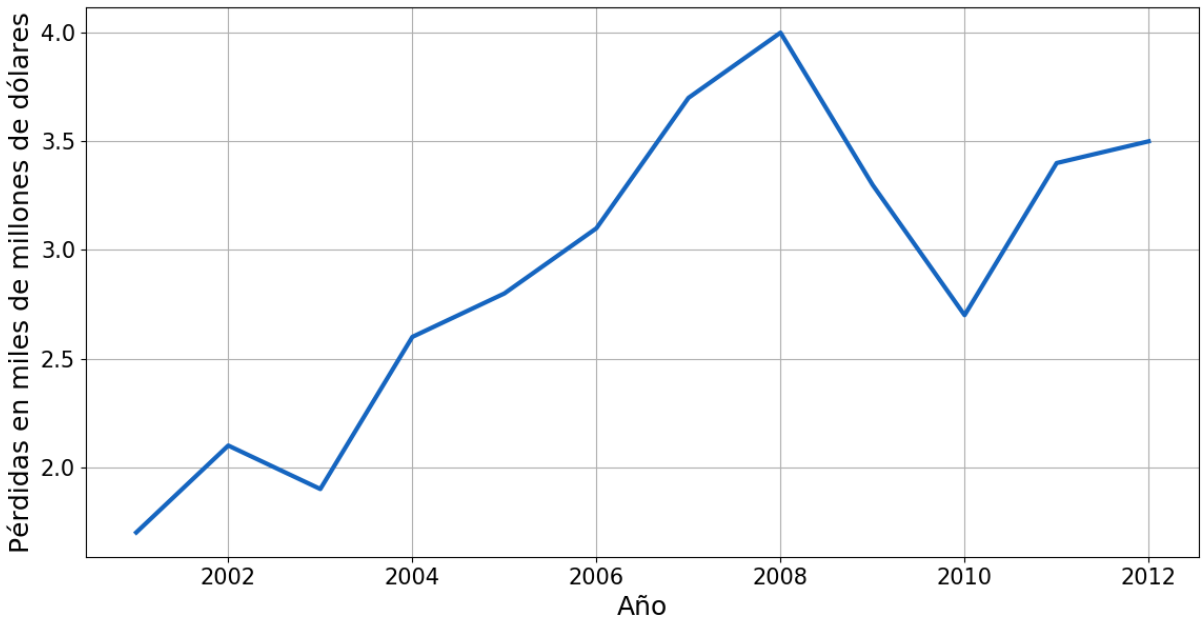


Arquitectura de sistema tokenizador: operación de tokenización.

Planteamiento del problema

La protección de datos bancarios

El crecimiento del comercio en línea, aunado a sistemas débilmente protegidos, propició un incremento en los robos de datos bancarios.



Pérdidas debidas al fraude en línea (2001-2012) [4].

Planteamiento del problema

Publicaciones del PCI

- En 2004, se publicó el PCI DSS[1][5].
- Hasta este momento, el enfoque era proteger la información en donde sea que se encuentre.
- En 2011, el PCI SSC[2] publicó las primeras guías para los procesos de tokenización [6].

[1] *Payment Card Industry, Data Security Standard*
[2] *Payment Card Industry, Security Standards Council*

Prototipos

División del proyecto

- **Generación de tokens** [TT-I]
  Implementación de 5 algoritmos generadores de tokens, con su respectivas pruebas.

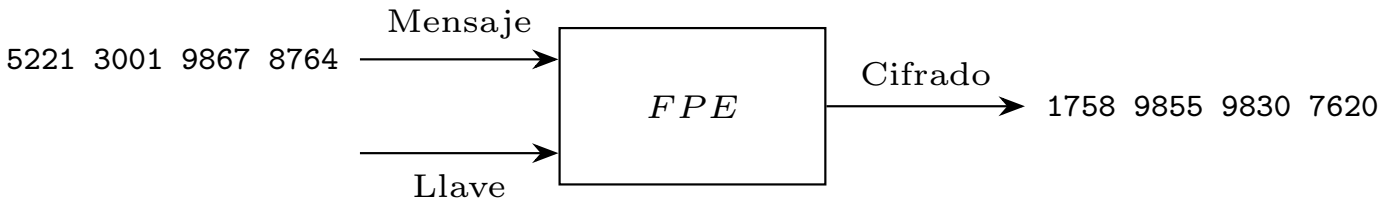
- **Servicio web** [TT-II]
  API que comunica al programa tokenizador con sus clientes.

- **Caso de prueba: tienda en línea** [TT-II]
  Librería en línea que integra el servicio web en el registro de una forma de pago y la realización de una compra.

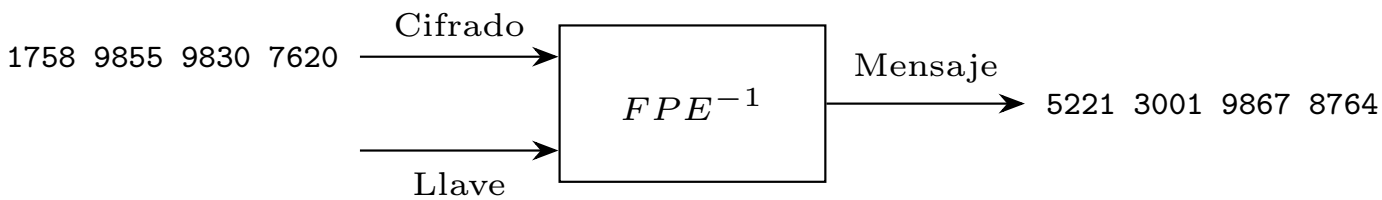
Generación de tokens

Algoritmos implementados (reversibles)

Entre los algoritmos reversibles, se encuentran FFX y BPS.



Proceso de tokenización, método reversible.

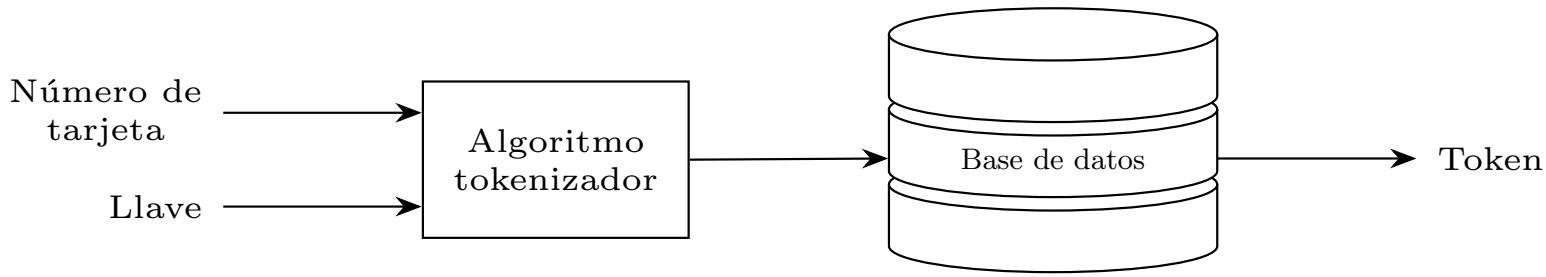


Proceso de detokenización, método reversible.

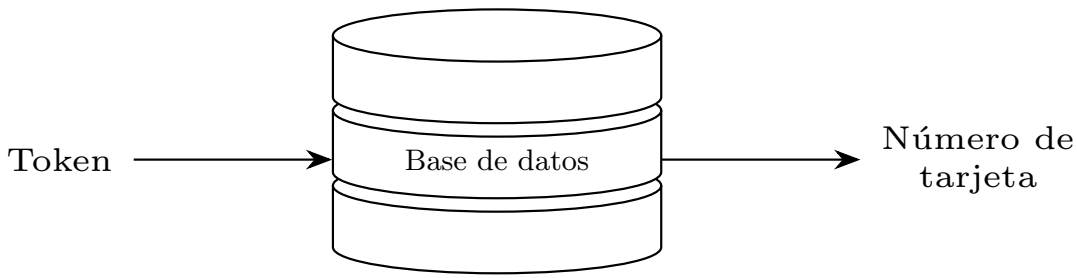
Generación de tokens

Algoritmos implementados (irreversibles)

Entre los algoritmos irreversibles, se encuentran TKR, AHR y DRBG.



Proceso de tokenización, método irreversible.



Proceso de detokenización, método irreversible.

Servicio web, contenido

Casos de uso

Diagrama general

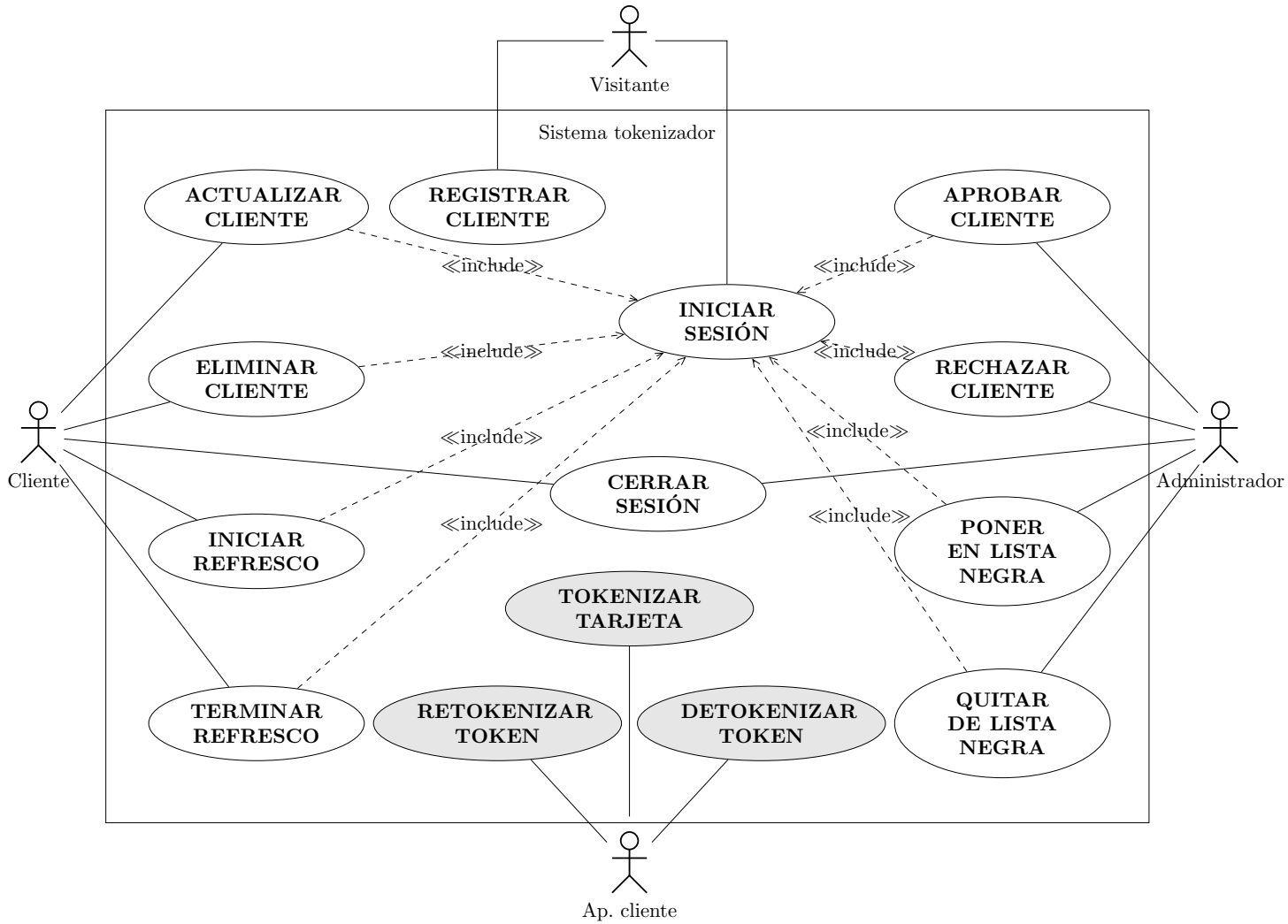


Diagrama general de casos de uso del servicio web de tokenización.

Tokenización y detokenización

Operaciones básicas del servicio web

- Ocupan el prototipo de generación de tokens.
- La aplicación sigue el modelo arquitectónico REST[3].
- Esquema de autenticación básico: las credenciales viajan en el encabezado de la petición.
- El protocolo encargado de asegurar la confidencialidad de los datos es HTTPS[4].
- La autoridad certificadora ocupada es *Let's Encrypt*. Para evitar tener que conseguir un nombre de dominio se ocupa el servicio de `xip.io`.

[3] *REpresentational State Transfer*

[4] *HyperText Transfer Protocol* con SSL/TLS

Refresco de llaves y retokenización

Refresco de llaves

- En el estándar del NIST sobre la administración de las llaves criptográficas (NIST SP-800-57 [7]) se habla sobre los criptoperiodos y se hace énfasis en cambiar las llaves cada que estos se cumplan.
- El PCI DSS especifica que debe existir un mecanismo que permita a los usuarios reemplazar sus llaves y actualizar sus tokens.

Refresco de llaves y retokenización

Refresco de llaves

El servicio web logra esto mediante un mecanismo llamado **refresco de llaves**.

- Se cambia el estado del cliente a *en cambio de llaves*.
- Se crean nuevas llaves.
- Las tokenizaciones se realizan con las llaves nuevas.
- Las detokenizaciones se pueden realizar con ambas llaves.

Cuando el cliente termina el **refresco de llaves**, se le regresa a su estado anterior y se eliminan los tokens que no fueron actualizados y las llaves anteriores.

Refresco de llaves y retokenización

Retokenización

La retokenización permite obtener la versión actual de los tokens:

1. El cliente envía el token anterior.
2. El servicio detokeniza el token recibido.
3. El servicio tokeniza el PAN obtenido en el paso anterior.
4. El servicio envía el token actualizado al cliente.

La retokenización está permitida solamente durante un refresco de llaves.

Demostración

Tienda en línea (caso de prueba), contenido

Casos de uso

Diagrama general

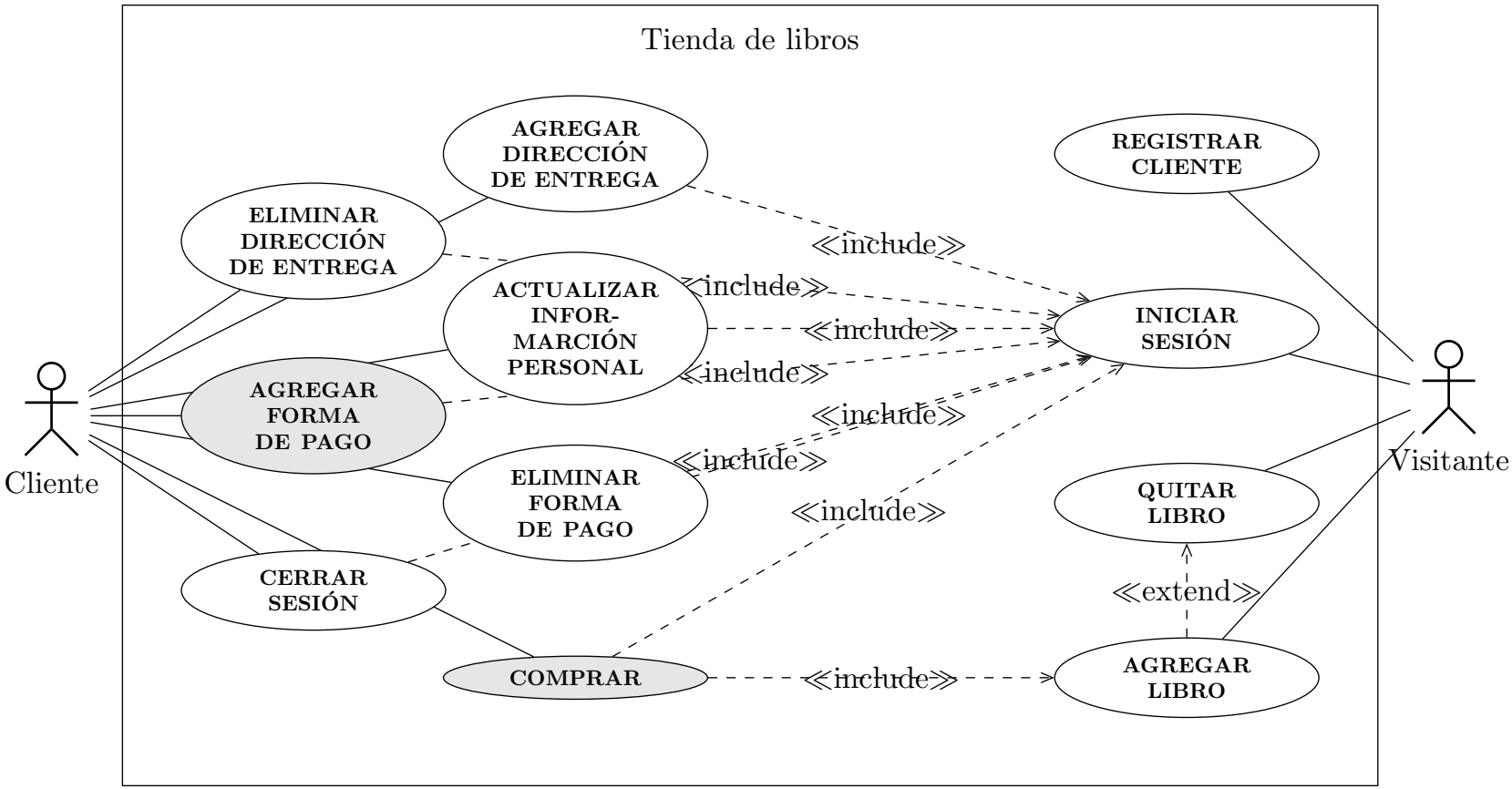


Diagrama general de casos de uso de tienda de libros en línea.

Integración con el servicio web

Esta tienda en línea se desarrolló con la finalidad de ser el caso de prueba del servicio web de tokenización.

Las partes donde se integra el servicio son:

- **El registro de una forma de pago.**
  Se necesita el servicio de tokenización dado que no se desea guardar el número de tarjeta ingresado, sino su token.

- **La realización de una compra.**
  Requiere de la detokenización, ya que se tiene almacenado el token de la tarjeta y se requiere el número original para la transacción bancaria.

Diagramas de secuencia

Caso de uso: compra

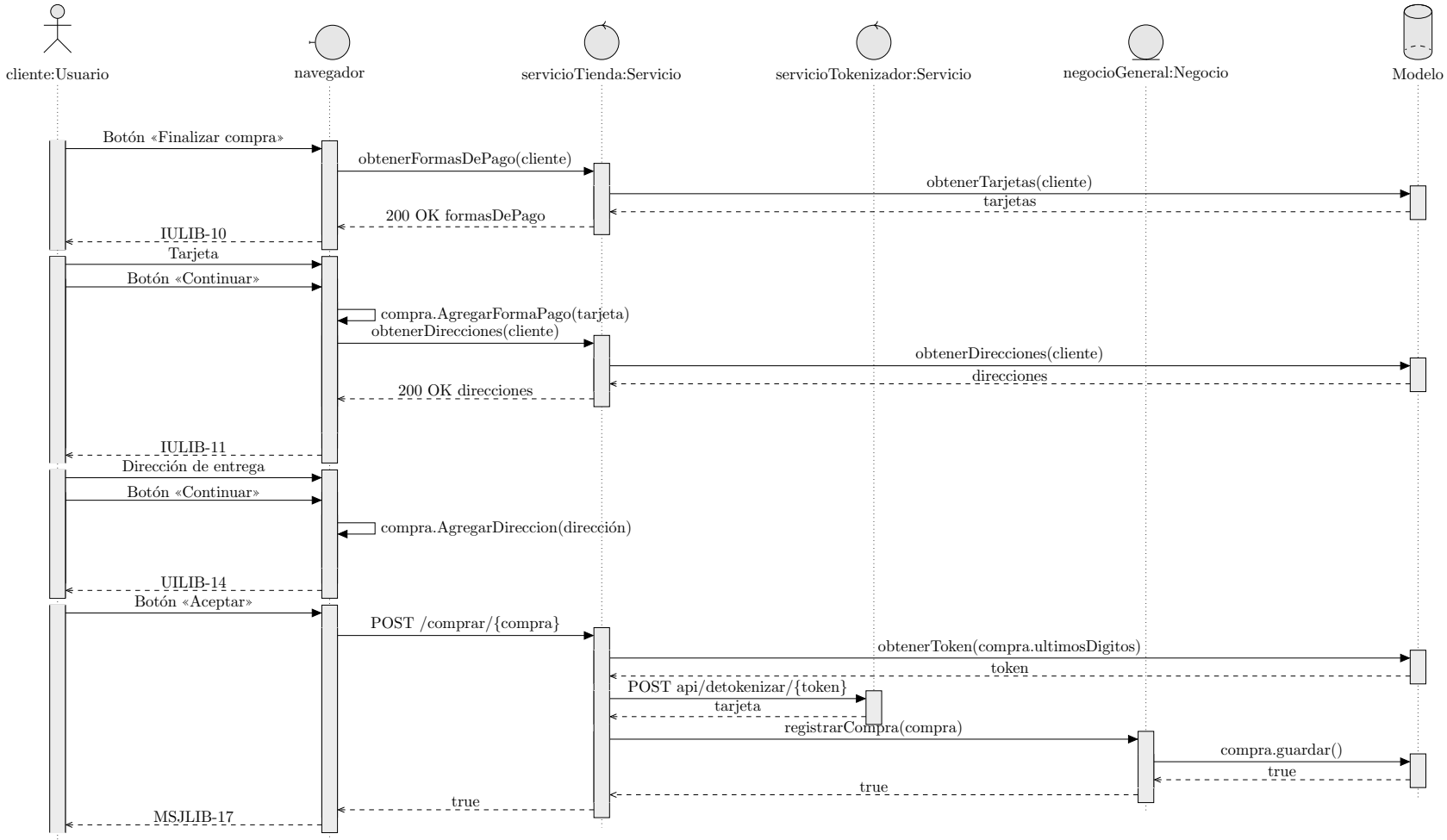
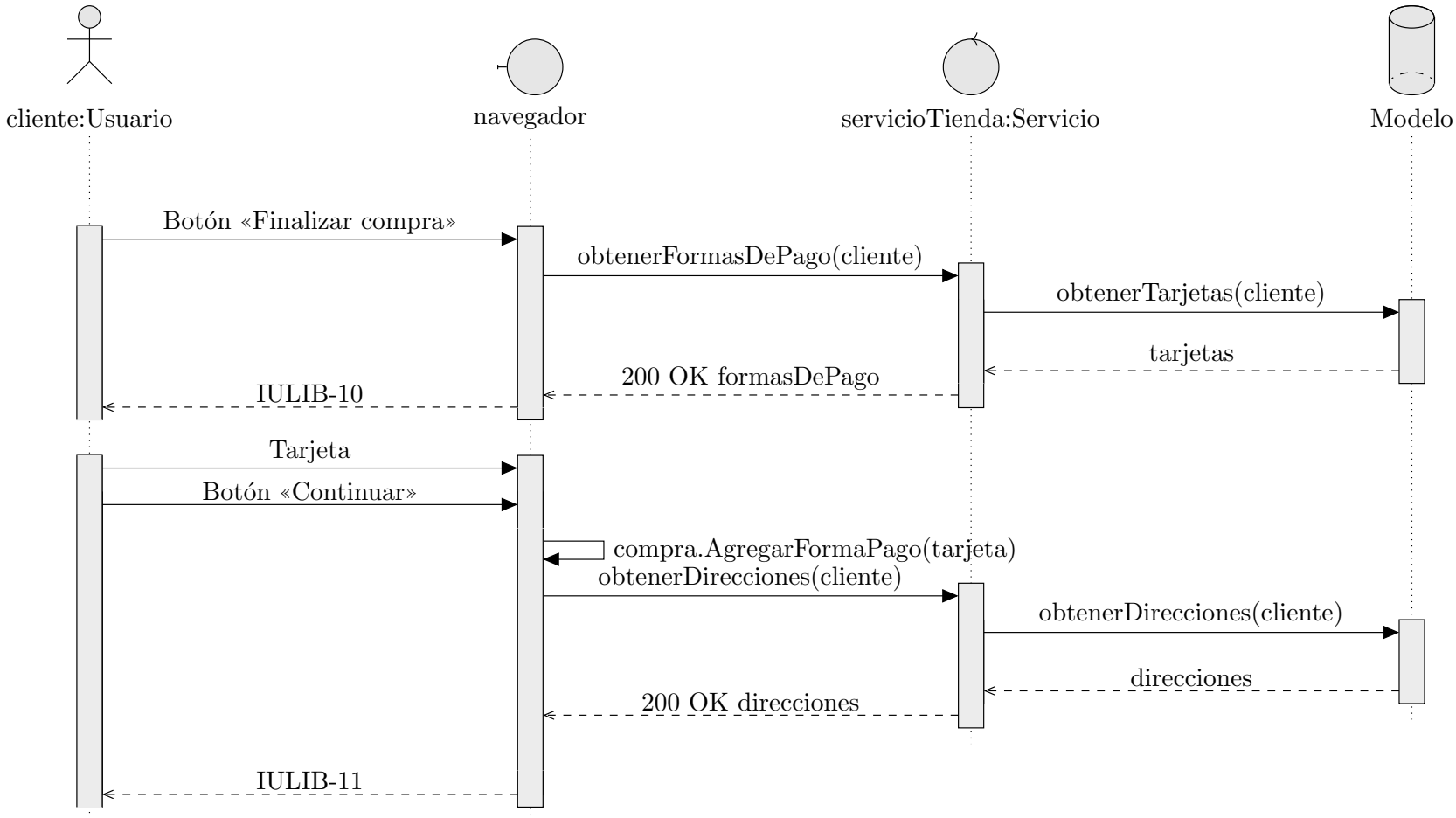


Diagrama de secuencia del caso de uso de compra.

Diagramas de secuencia

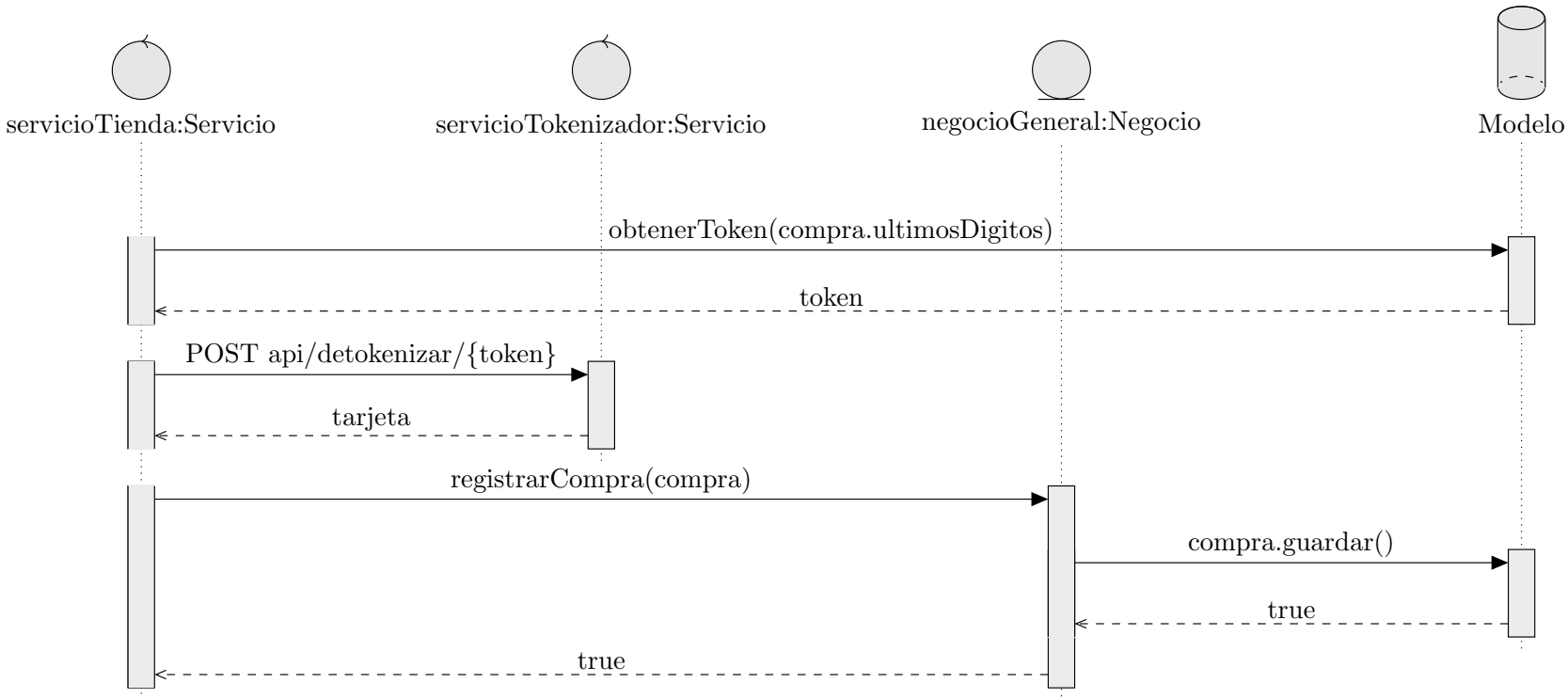
Caso de uso: compra - obtención de datos



Acercamiento del diagrama de secuencia: obtención de datos.

Diagramas de secuencia

Caso de uso: compra - finalización de compra



Acercamiento del diagrama de secuencia: interacción con el servicio de tokenización.

Demostración

Resultados, contenido

Pruebas de desempeño

Especificaciones del equipo

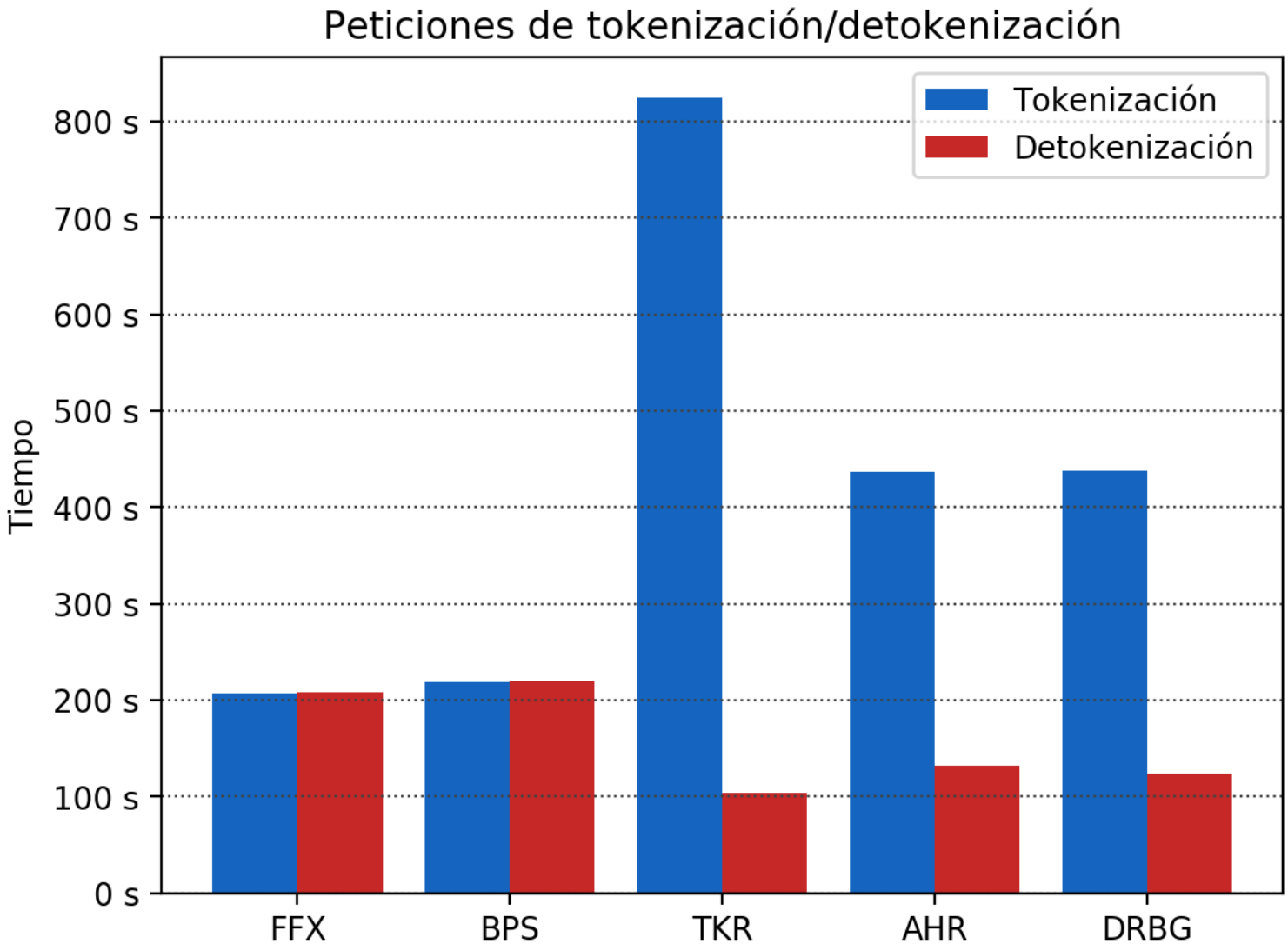
Las pruebas mostradas a continuación se realizaron en una computadora Acer Spin-5 con las siguientes especificaciones:

- Procesador Intel Core i5-8250U.
  - 6M caché, hasta 2.2GHz.
  - 8 núcleos.
- 8GB de RAM.
- En los casos pertinentes, se utilizó AES-NI[5].
- Se utilizó el compilador GCC versión 7.3.1.

[5] *Intel Advanced Encryption Standard New Instructions.*

Pruebas de desempeño

Comparación de tiempos



Comparación de tiempos de 10K operaciones.

Conclusiones, contenido

Sobre los objetivos

Los objetivos planteados al inicio de este trabajo terminal fueron cumplidos:

- Implementar algoritmos generadores de tokens.
- Diseñar e implementar un servicio web que proporcione la generación de tokens a, al menos, una tienda en línea.
- Implementar una tienda en línea que utilice el servicio de generación de tokens.

Sobre la clasificación

Uno de los resultados más importantes, es la clasificación propuesta por los autores para los algoritmos tokenizadores en respuesta a la clasificación del PCI.

- La denominación de *no criptográficos* es engañosa.
- La denominación *irreversibles* no es muy útil para las aplicaciones que tokenizan números de tarjetas.

Sobre el trabajo desarrollado

- Se escribió un artículo con los resultados de este trabajo y fue presentado en la *Reunión de Ciberseguridad para la Industria 4.0* (RCI4.0 2018); será publicado en las memorias del evento.
- Las implementaciones de los algoritmos son públicas.
  - `https://github.com/RQF7/proyecto_lovelace`
  - `https://ricardo-quezada.159.65.96.59.xip.io/sistema_tokenizador/estaticos/doxygen/html`
- Tanto el servicio tokenizador como la tienda en línea pueden ser consultadas en las siguientes direcciones:
  - `https://ricardo-quezada.159.65.96.59.xip.io/sistema_tokenizador`
  - `https://ricardo-quezada.159.65.96.59.xip.io/libreria`

Bibliografía I

[1] Shift4 Payments. *The History of TrueTokenization*. https://www.shift4.com/dotn/4tify/trueTokenization.cfm. Consultado en agosto de 2018 (vid. pág. 5).

[2] Braintree. *Tokenization Secures CC Data and Meet PCI Compliance Requirements*. https://www.braintreepayments.com/blog/using-tokenization-to-secure-credit-card-data-and-meet-pci-compliance-requirements/. Consultado en marzo de 2018 (vid. pág. 5).

[3] Securosis. *Understanding and Selecting a Tokenization Solution*. https://securosis.com/assets/library/reports/Securosis_Understanding_Tokenization_V.1_.0_.pdf. Consultado en febrero de 2018 (vid. pág. 5).

Bibliografía II

[4] John S. Kiernan. *Credit Card And Debit Card Fraud Statistics*. https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/. Consultado en marzo de 2018 (vid. pág. 6).

[5] Payment Card Industry Security Standards Council. *Data Security Standard - Version 3.2*. 2016. URL: https://www.pcisecuritystandards.org/documents/pci_dss_v3-2.pdf (vid. pág. 7).

[6] Payment Card Industry Security Standards Council. *Tokenization Product Security Guidelines – Irreversible and Reversible Tokens*. 2015. URL: https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf (vid. págs. 7, 36).

[7] Elaine Barker. *NIST Special Publication 800-57 - Recommendation for Key Management*. 2016. URL: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 (vid. pág. 14).

Generación de tokens para proteger los datos de tarjetas bancarias

Trabajo terminal No. 2017-B008

Presentan

Daniel Ayala Zamorano

daz23ayala@gmail.com

Laura Natalia Borbolla Palacios

ln.borbolla.42@gmail.com

Ricardo Quezada Figueroa

qf7.ricardo@gmail.com

Directora

Dra. Sandra Díaz Santiago

Ciudad de México, 9 de noviembre de 2018

Escuela Superior de Cómputo

Instituto Politécnico Nacional

Diapositivas auxiliares

Generación de tokens

Clasificación del PCI

Clasificación propuesta por el PCI SSC [6].

- Reversibles
  - Criptográficos (FFX, BPS)
  - No criptográficos (TKR, AHR, DRBG)
- Irreversibles
  - Autenticables
  - No autenticables

Generación de tokens

Clasificación propuesta

- Criptográficos
  - Reversibles (FFX, BPS)
  - No reversibles (TKR, AHR, DRBG)
- No criptográficos