

UN VISTAZO A LA TOKENIZACIÓN

PRESENTAN

DANIEL AYALA ZAMORANO

DAZ23AYALA@GMAIL.COM

LAURA NATALIA BORBOLLA PALACIOS

LN.BORBOLLA.42@GMAIL.COM

RICARDO QUEZADA FIGUEROA

QF7.RICARDO@GMAIL.COM

SANDRA DÍAZ SANTIAGO

SDIAZS@GMAIL.COM

PRIMERA REUNIÓN DE CIBERSEGURIDAD PARA LA INDUSTRIA 4.0
PUEBLA, 14 DE OCTUBRE DE 2018

ESCUELA SUPERIOR DE CÓMPUTO
INSTITUTO POLITÉCNICO NACIONAL



CONTENIDO

El problema de la protección de datos bancarios

¿Qué es la tokenización?

Clasificación del PCI

Métodos reversibles: FFX y BPS

Métodos irreversibles: TKR, AHR y DRBG

Resultados y conclusiones

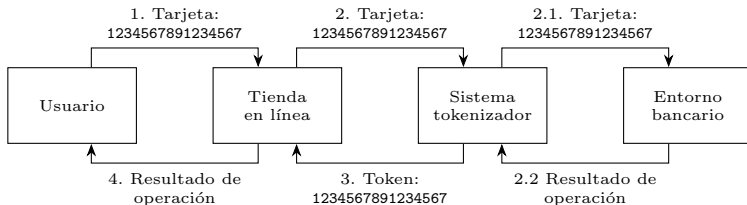
EL PROBLEMA DE LA PROTECCIÓN DE DATOS BANCARIOS

- ▶ El crecimiento del comercio en línea aunado a sistemas débilmente protegidos propició un incremento en los robos de datos bancarios.
- ▶ En el 2004 se publicó el PCI DSS¹.
- ▶ Hasta este momento el enfoque es proteger la información en todo lugar en el que se encuentre.
- ▶ A pesar de la publicación del estándar, las filtraciones de datos no han terminado.

¹*Payment Card Industry, Data Security Standard*

¿QUÉ ES LA TOKENIZACIÓN?

- ▶ 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].
- ▶ En 2011 el PCI publicó las guías para la tokenización [4].



Arquitectura típica de un sistema tokenizador.

CLASIFICACIÓN DE LOS ALGORITMOS TOKENIZADORES

Clasificación del PCI [4]:

- ▶ Reversibles
 - ▶ Criptográficos
 - ▶ No criptográficos
- ▶ Irreversibles
 - ▶ Autenticables
 - ▶ No autenticables

Clasificación propuesta:

- ▶ Criptográficos
 - ▶ Reversibles
 - ▶ Irreversibles
- ▶ No criptográficos

MÉTODOS REVERSIBLES: FFX Y BPS

MÉTODOS IRREVERSIBLES: TKR, AHR Y DRBG

RESULTADOS Y CONCLUSIONES

BIBLIOGRAFÍA I

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

BIBLIOGRAFÍA II

- [4] 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](https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf)
(vid. págs. 4, 5).

UN VISTAZO A LA TOKENIZACIÓN

PRESENTAN

DANIEL AYALA ZAMORANO

DAZ23AYALA@GMAIL.COM

LAURA NATALIA BORBOLLA PALACIOS

LN.BORBOLLA.42@GMAIL.COM

RICARDO QUEZADA FIGUEROA

QF7.RICARDO@GMAIL.COM

SANDRA DÍAZ SANTIAGO

SDIAZS@GMAIL.COM

PRIMERA REUNIÓN DE CIBERSEGURIDAD PARA LA INDUSTRIA 4.0
PUEBLA, 14 DE OCTUBRE DE 2018

ESCUELA SUPERIOR DE CÓMPUTO
INSTITUTO POLITÉCNICO NACIONAL

