Tokenization "The Buzzword in Depth"

ASHOK MISRA, CISSP

About me & tokenization

- Worked on payments system architecture for more than 15 years.
- Built the main tokenization system for Amazon.com in 2001.
- epaymentsNut: PCI, Payments, Blockchain, Security.
- Currently a payments consultant based in Seattle, WA, USA.

Alina
Consultants

Session Outline

➤ What is tokenization ?

➤ Why is tokenization useful ?

➤ What are the security problems solved ?

➤ Tokenization caveats

Alina
Consultants

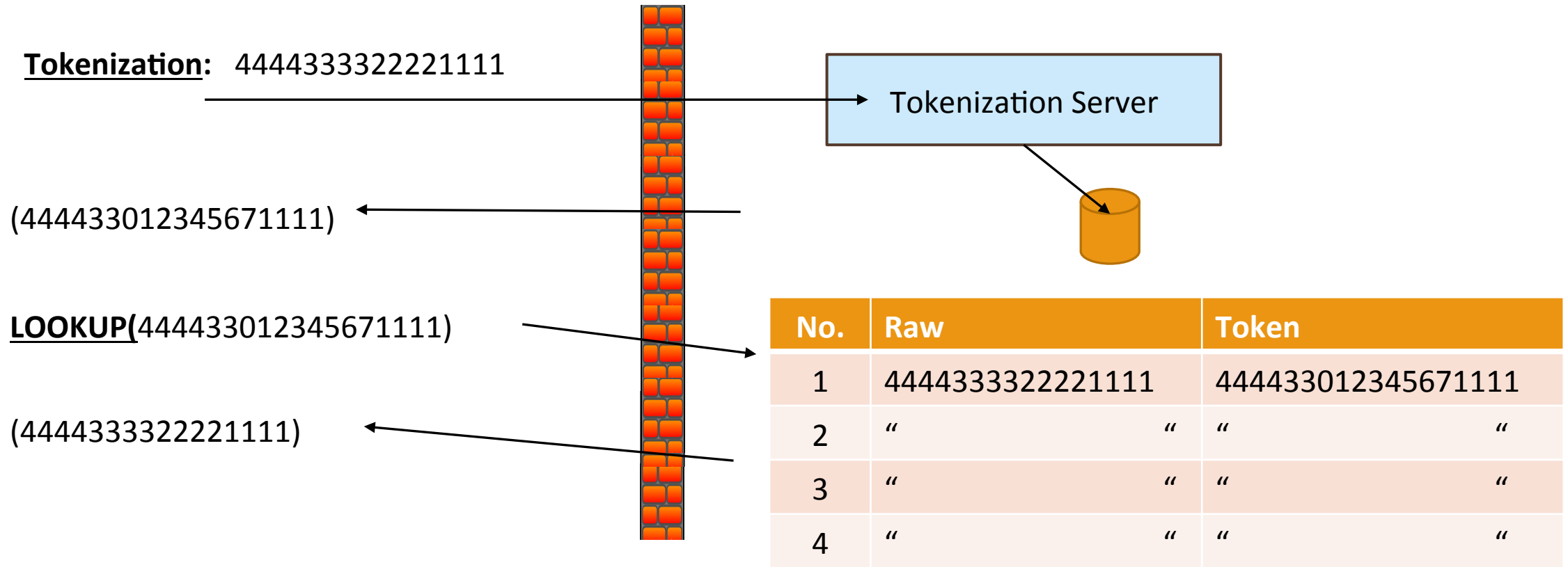# What is Tokenization?

Tokenization Primer

➤ The process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token.

➤ The token maps back to the sensitive data.

➤ Security requirements for systems that hold the token are reduced or eliminated.

➤ Implementation of tokenization may simplify the requirements of the PCI DSS.

Alina
Consultants

Tokenization 101

Tokenization: 4444333322221111

Tokenization Server

(444433012345671111)

LOOKUP(444433012345671111)

(4444333322221111)

No.	Raw	Token
1	4444333322221111	444433012345671111
2	" "	" "
3	" "	" "
4	" "	" "

Highlights: No storage outside of Tokenization

Tokenization 101

CREDIT CARD NEEDS TO BE ENCRYPTED!

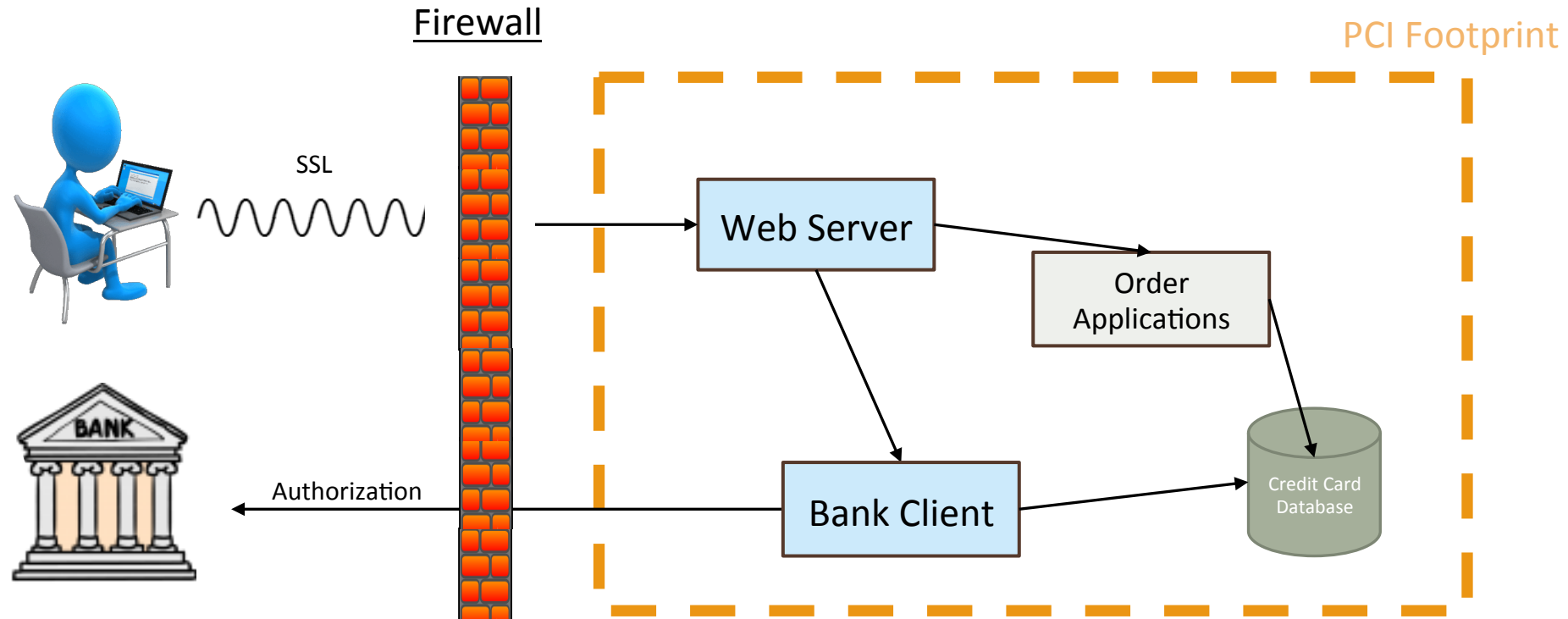| No.	Encrypted Card	Token
1	X?4AX?!QB10	4444330123457111

Alina
Consultants

Legacy E-commerce System

➢Credit cards were not designed to be used for ecommerce

➢They have been adapted for the CNP use case

➢Authentication approaches are highly limited for CNP

Legacy e-commerce System

Firewall

PCI Footprint

SSL

Web Server

Order Applications

Authorization

Bank Client

Credit Card Database

Key Points:
- Monolithic Architecture
- No encryption of cards
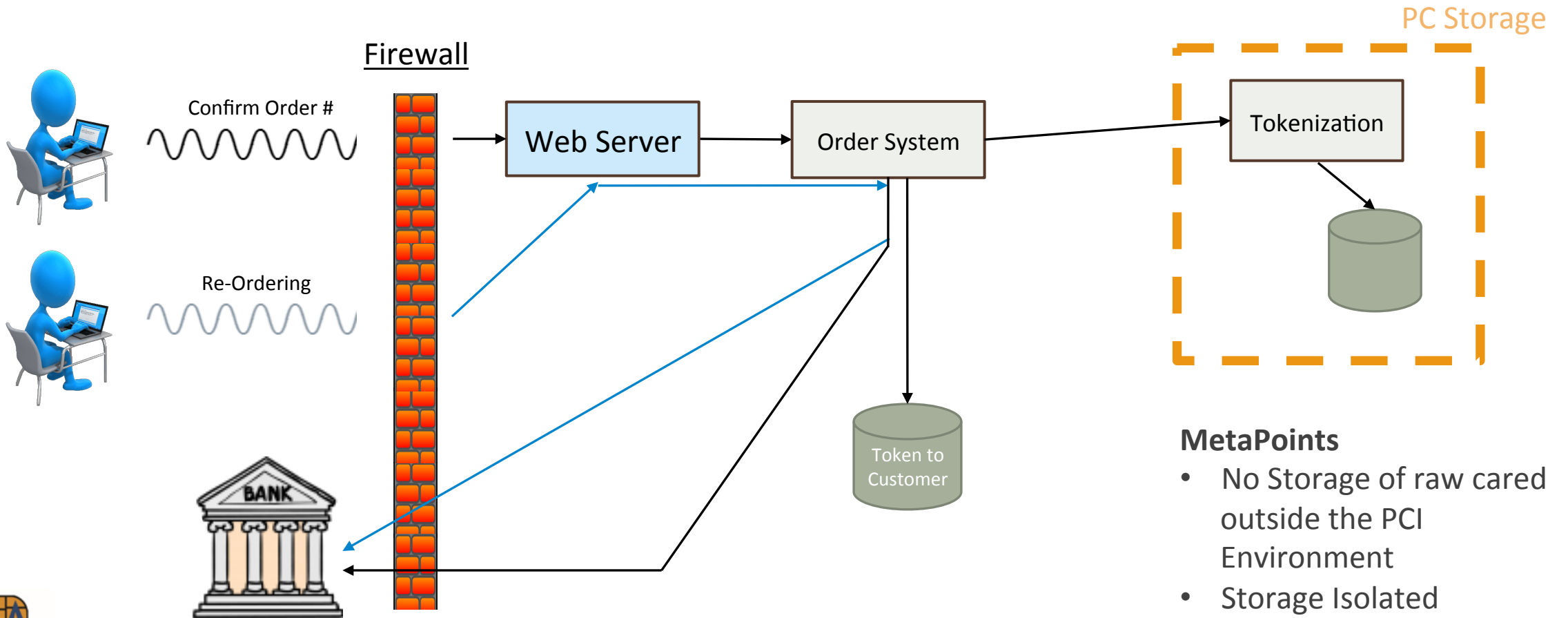- PCI Footprint spans entire e-commerce system

Alina Consultants

Why is Tokenization Useful?

When correctly implemented

➢Storage of cards isolated

➢Footprint reduced for Security policy

➢More difficult to penetrate

Example Implementation:
Tokenized e-commerce Architecture

PC Storage

Firewall

Confirm Order #

Re-Ordering

Web Server

Order System

Tokenization

BANK

Token to Customer

MetaPoints
- No Storage of raw cared outside the PCI Environment
- Storage Isolated
- PCI Footprint Reduced

Alina Consultants

What are the Security Problems Solved?

What are the Problems Solved?

➢ Storage of PANs is isolated.

➢ PCI footprint reduced for storage & access requirements.

➢ PANs are much harder to penetrate.

Alina
Consultants

What are the Problems Created?

- How can the lookup function be implemented ?
- How can one safeguard against a single point of failure ?
- How can one prevent vendor lock-in ?

Alina
Consultants

Tokenization Caveats

Some Downsides

➢Relies on trusted clients

➢Should tokenization be idempotent ?

➢How can lookup be implemented ?

➢TSP lockin

➢Can tokens run out ?

Alternate (Merchant) Technologies

➢Iframe

➢Redirect

➢Blockchain

Summary & Questions?