Smart Card based Mobile Device Security

Nizar Jamal

NIST FIPS 201-2 Workshop

Mar 4, 2015

side
FROM TYFONE

Overview

- About Tyfone
- Problem
- Market Trends & Use cases
- Demonstration
- Standardization

side
FROM TYFONE

About Tyfone

Portland, OR | Bangalore, India

IQT
IN·Q·TEL

In-Q-Tel portfolio company

Next Generation Security Hardware that secures all use cases for all of the user's devices

600+ issued invention claims
31 issued patents, 70 pending

U.S. Intelligence Community

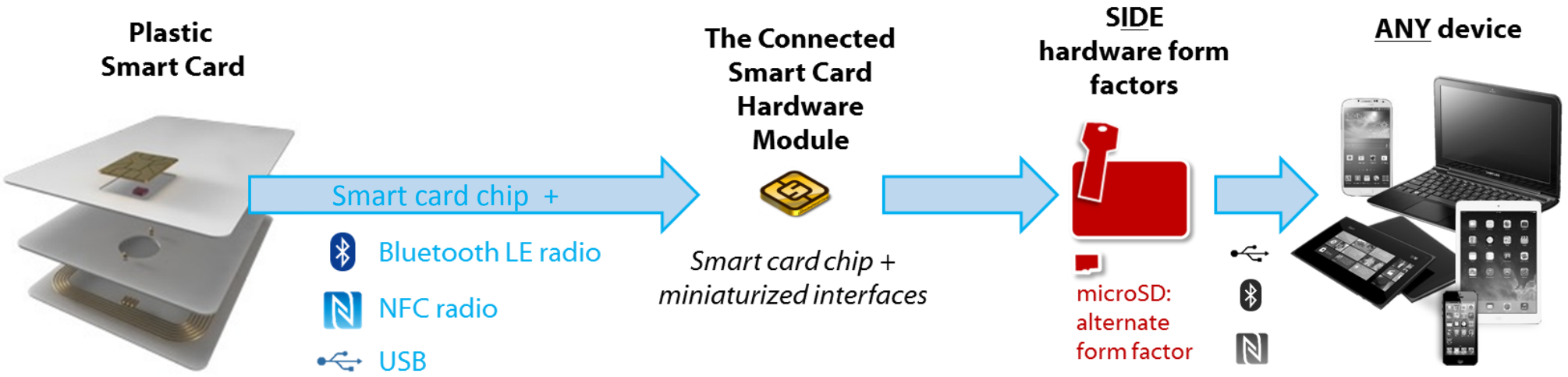
SECURITY SERVICE FEDERAL CREDIT UNION

STAR ONE CREDIT UNION

Two Top 10 Credit Unions
out of 6000+

First Data

Tyfone inventions



The Connected Smart Card ™ Module
SIDE™ Form Factors
U4ia™ Provisioning Platform

31 issued & 70 pending patents

Convenient, Consistent, Converged

side
FROM TYFONE

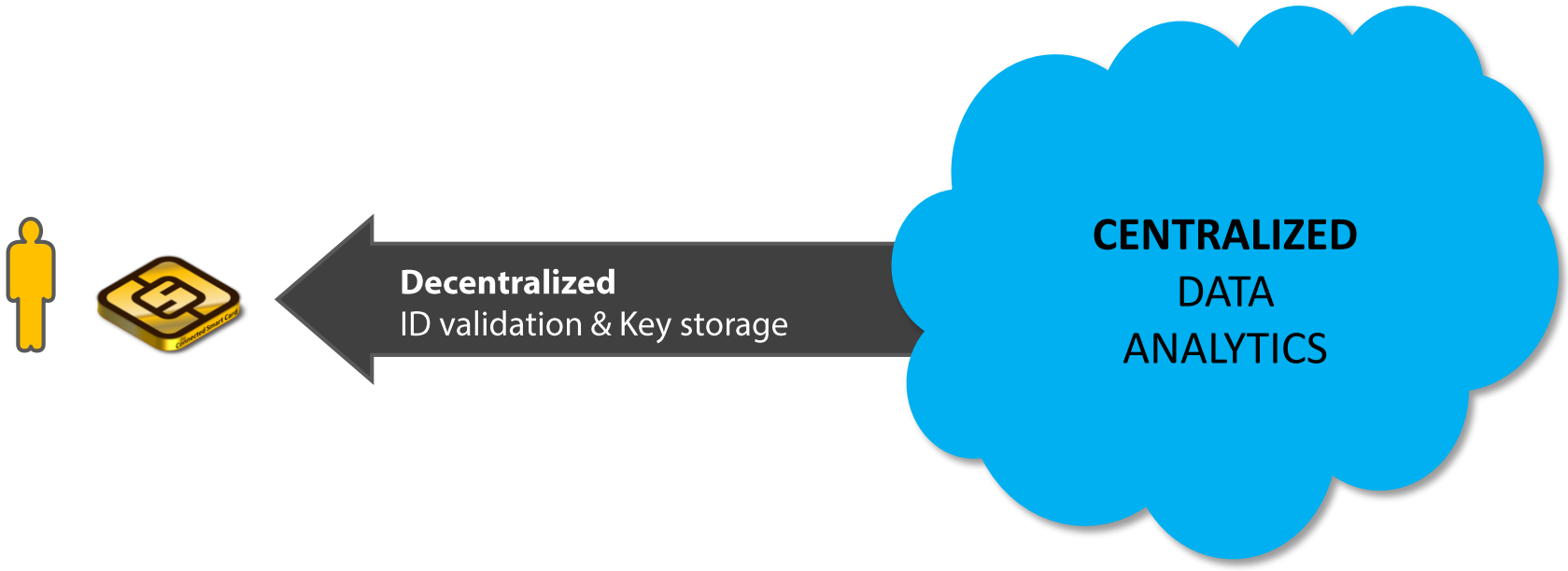
Security is centralized, insecure, inconvenient

Payments
Financial Services
Government
Health care
Critical Infrastructure
Enterprise
…

Massive loss of data and dollars – Billions of identities/records stolen and 100s of Billions of $ lost
User inconvenience – Stolen identities, canceled credit cards, cumbersome Q&A, password resets

side
FROM TYFONE

Security with decentralized hardware



Protect

- Identity
  - Privacy
- Data
  - At Rest
  - In Transit
  - In Use

Dimensions

- Security
- Convenience
- Cost
- Risk Tolerance
- Legacy

DRAMATICALLY

Increases Convenience & Awareness | Lowers scale of loss | Increases scope of law enforcement

side
FROM TYFONE

Recent Market Trends

Sep 2014

Smart card hardware
Biometrics / PIN
iOS only

Oct 2014

Google

Smart card hardware
Password
PC only

By Oct 2015

Smart card hardware
Optional PIN
Point-of-Sale only

Applets: EMV, Tokenization…

Consumer Use Case

Apple Pay

SE + NFC + BLE

iPhone only

Secure Hardware Inside iPhone6

Outside (any iOS device)

SIDE from Tyfone

SE + NFC + BLE + USB

Any device

Outside (Any device)

SE = Secure Element
NFC = Near-field Communications radio
BLE = Bluetooth LE radio

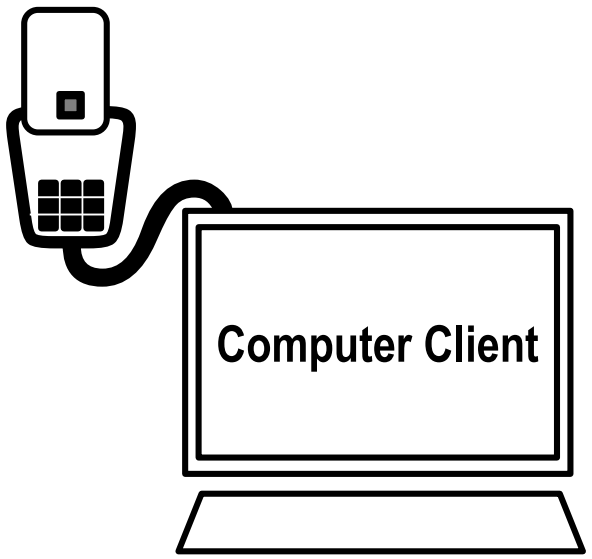
Applets: CAC, PIV, PKCS, Derived Credential

Government and Enterprise Use Case

PC only

Plastic Smart Card

Trusted PIN Pad



Not mobile friendly

Mobile enabled with Tyfone's SIDE

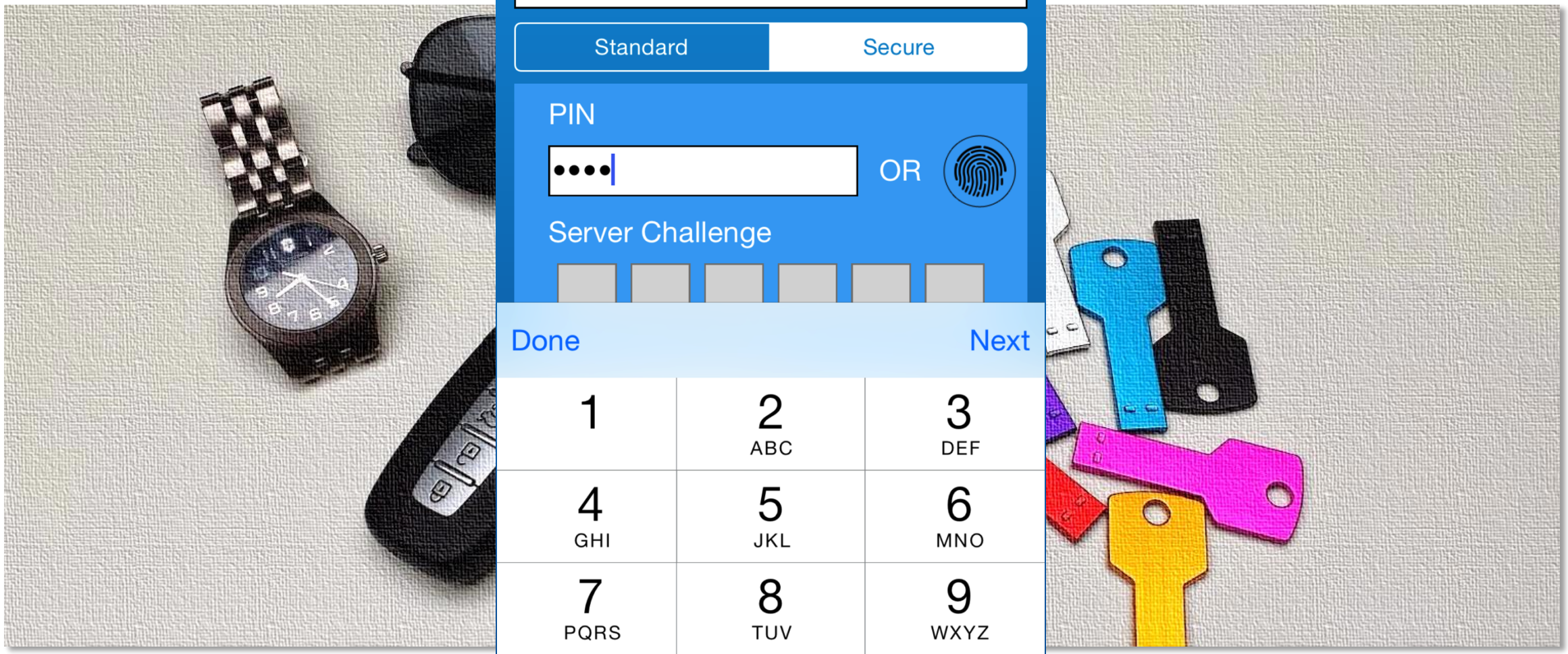
SideTap memory card with smart card controller & 60X smaller 13.56Mhz antenna

SideKey with smart card controller & 13.56Mhz reader

NFC Tap
BTLE Leashing

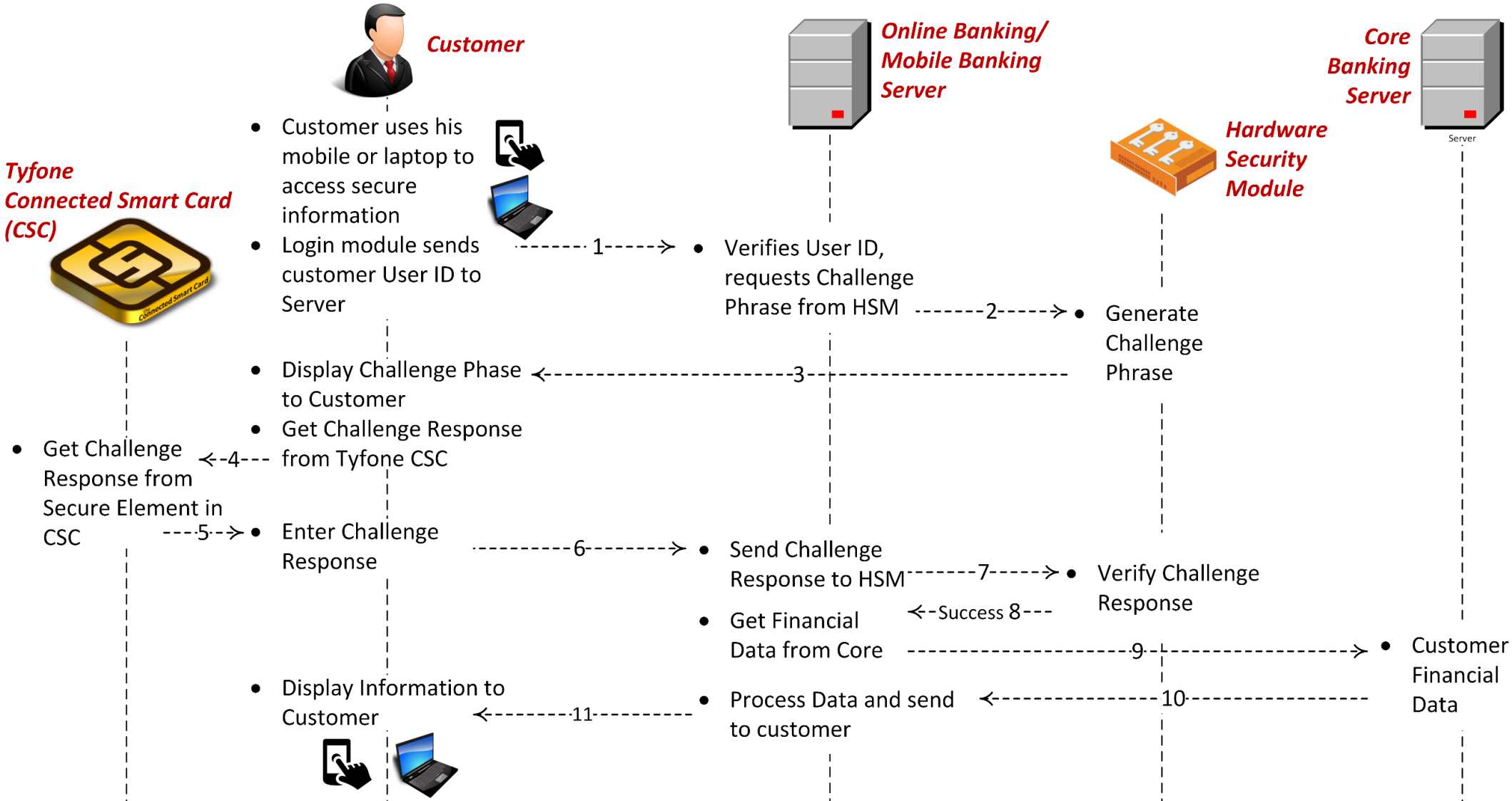
side
FROM TYFONE

Demonstration o uthentication



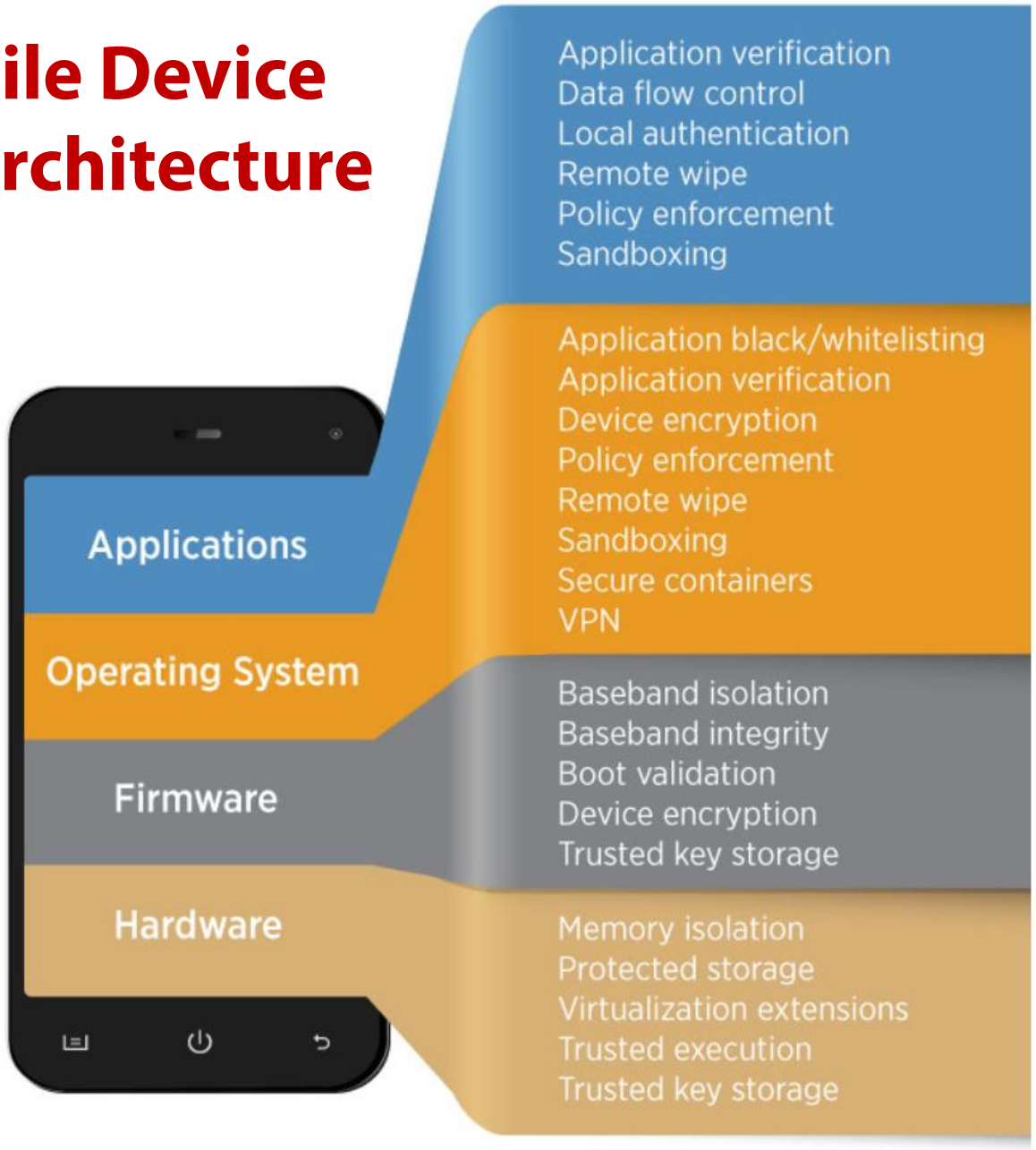
side
FROM TYFONE

Demo: Authentication Flow



side
FROM TYFONE

NIST: Mobile Device Security Architecture



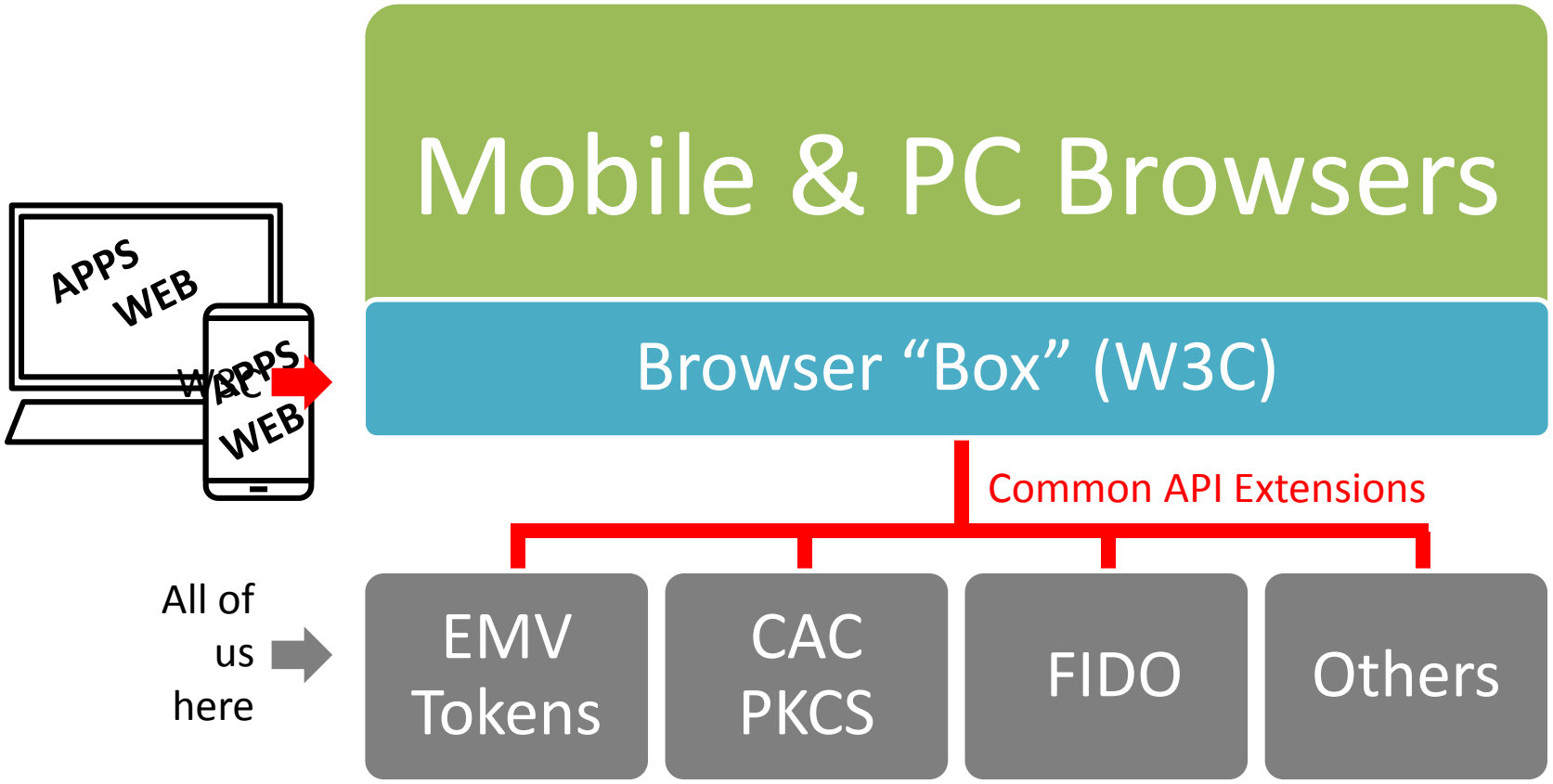
Browsers

Without Web Standards:
Requires unique middleware
Based on
Browser **x** Platform **x** Smart Card Vendor

With Web Standards:
Platform specific middleware

side
FROM TYFONE

The Case for Web Standards



Review W3C workshop minutes:
http://tinyurl.com/2014w3c