Federated Identity, Strong Authentication, NSTIC and the Identity Ecosystem

Rajesh Shenoy
Director, Head of Global Identity Solutions
Citi
Implications and considerations of security on privacy

Digital identity in financial services

Security platforms in use and under exploration

Use of existing credentials within NSTIC* identity ecosystem

*NSTIC: National Strategy for Trusted Identities in Cyberspace
Identity Data: Ecosystem of a Fast Growing Asset Class

Global digital data is expected to grow **4400%** in 10 years*

*Source: World Economic Forum, SWIFT*
Privacy must be prioritized as digital identity is used in new applications.

**New Challenges**
- Increased Digitization
- Expanding Client Base
- Regulation

**New Opportunities**
- Leverage data
- Develop new services
- Enhance security
- Facilitate financial inclusion
Agenda

I Implications and considerations of security on privacy

II Digital identity in financial services

III Security platforms in use and under exploration

IV Use of existing credentials within NSTIC identity ecosystem
Trusted digital identity is central to global electronic banking

$800Bn
Fraudulent Payments per year
Security concerns by clients demand identity solutions

- Multiple banks and accounts
- Coexistence of processes
- Compliance, regulatory, and audit requirements
- Internal fraud mitigation
- Fragmented security
- Client and end-user considerations
Agenda

I Implications and considerations of security on privacy

II Digital identity in financial services

III Security platforms in use and under exploration

IV Use of existing credentials within NSTIC identity ecosystem
Several traditional and emerging authentication solutions can be used

**Something You Know**
- User-Password every time user logs in
  - Weak
  - Strong (incl. numbers, symbols etc.)
- User-password entered once / encrypted
  - Decryption stored on device
  - Decryption stored on server

**Something You Have**
- Hardware token that generates one-time-password (OTP)
- PKI certificates (hardware tokens)
- Software / Device-generated OTP
- SMS OTP
- Out-of-Band Authentication (phone call)
- SIM-based (credential securely stored)
- Geolocation / location-based

**Something You Are (Biometrics)**
- Biometrics are intrinsic to an individual, making it more difficult to share / copy / steal
- Very few implementations, mostly in R&D (voice, facial, iris)
- No standard mobile interface on which biometric data can be collected
- iPhone 5s fingerprint sensor demonstrates initial market potential for biometric authentication
Authentication methods have varying levels of security and convenience.

Generally, as security risk increases, solution complexity increases as well.
What’s under exploration?

Methods of Identity Verification

**Something You Know**
- Password + PIN

**Considerations**
- Many passwords are easy to guess, can be easily forgotten
- No way to positively link usage of the system to actual user

**Something You Have**
- Key / Card

**Considerations**
- Can be lost, stolen, or duplicated

**Something You Are**
- Finger, Eye, Voice, Heartbeat

**Considerations**
- Cannot be lost, unique to individual, and difficult to forge
- Provides more accurate and reliable user authentication
Case Study: Cost of Payment Fraud

Pension Expenditure: W. Europe

% of GDP

Belgium, Denmark, Germany, Spain, France, Ireland, Italy, Luxembourg, Netherlands, Australia, Portugal, Finland, Sweden, UK

2010, 2050

Sources: Eurostat (2010 Pension figures), US Bureau of Census & Europa (2050 Pension figures)
Agenda

I Implications and considerations of security on privacy

II Digital identity in financial services

III Security platforms in use and under exploration

IV Use of existing credentials within NSTIC identity ecosystem
Currently, clients cannot use their own client credentials to authenticate themselves on most external bank channels. Single-purpose hardware tokens are primarily.

Clients will have the option to use their own credentials and/or software OTP (e.g. MobilePass) to authenticate on bank channels, as well as for countries that require separate authentication mechanisms.
Public sector digital identity ecosystem opportunity

Why not integrate financial services with government credentials?

The expanding reach of standard credentials

All Public Sector Agencies

Total Reach: 7 million Individuals

Total reach: 25-30 million Individuals

Total reach: 50-60 million Individuals

Adding Interoperable Standards: Contractors and Guest Workers to Agencies

Adding Interoperable Programs
Rajesh Shenoy
rajesh.a.shenoy@citi.com

Smart Card Alliance
191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556–6828
www.smartcardalliance.org
Citi believes that sustainability is good business practice. We work closely with our clients, peer financial institutions, NGOs and other partners to finance solutions to climate change, develop industry standards, reduce our own environmental footprint, and engage with stakeholders to advance shared learning and solutions. Highlights of Citi’s unique role in promoting sustainability include: (a) releasing in 2007 a Climate Change Position Statement, the first US financial institution to do so; (b) targeting $50 billion over 10 years to address global climate change; includes significant increases in investment and financing of renewable energy, clean technology, and other carbon-emission reduction activities; (c) committing to an absolute reduction in GHG emissions of all Citi owned and leased properties around the world by 10% by 2011; (d) purchasing more than 234,000 MWh of carbon neutral power for our operations over the last three years; (e) establishing in 2008 the Carbon Principles; a framework for banks and their U.S. power clients to evaluate and address carbon risks in the financing of electric power projects; (f) producing equity research related to climate issues that helps to inform investors on risks and opportunities associated with the issue; and (g) engaging with a broad range of stakeholders on the issue of climate change to help advance understanding and solutions.

Citi works with its clients in greenhouse gas intensive industries to evaluate emerging risks from climate change and, where appropriate, to mitigate those risks.

efficiency, renewable energy and mitigation