What is NSTIC?

Called for in President's Cyberspace Policy Review (May 2009):
a "cybersecurity focused identity management vision and strategy"

Guiding Principles

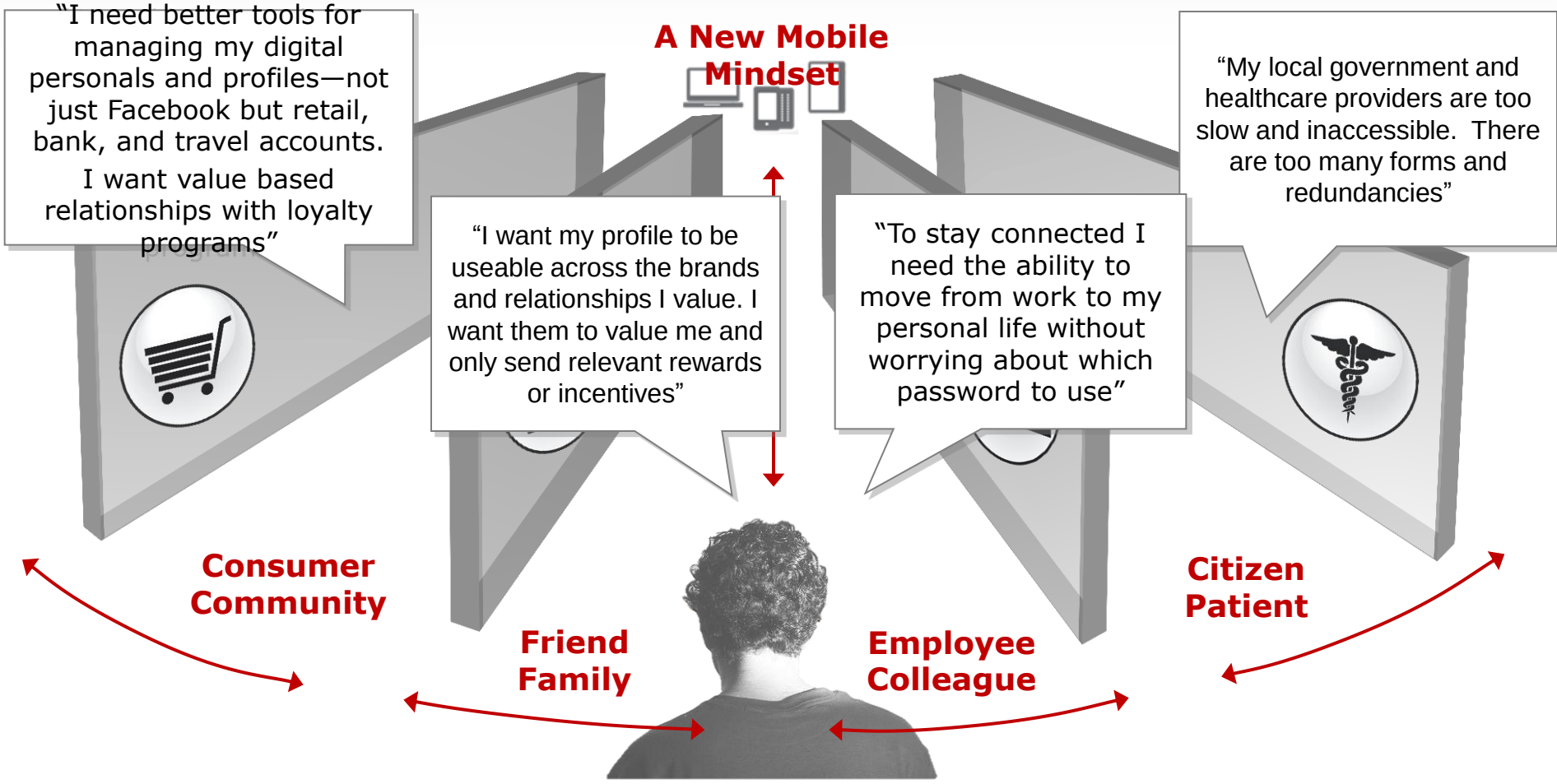
- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**,
"an online environment where individuals
and organizations will be able to trust each other
because they follow agreed upon standards to obtain
and authenticate their digital identities."

Privacy and Civil Liberties are Fundamental

- **Increase privacy**
  - Minimize sharing of unnecessary information
  - Minimum standards for organizations - such as adherence to Fair Information Practice Principles (FIPPs)
- **Voluntary and private-sector led**
  - Individuals can choose not to participate
  - Individuals who participate can choose from public or private-sector identity providers
  - No central database is created
- **Preserves anonymity**
  - Digital anonymity and pseudonymity supports free speech and freedom of association

Our vision is to empower individuals with seamless and secure access



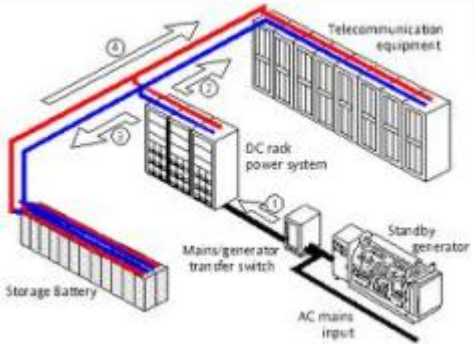
Identity Providers

- Semantic problem – we're really "Privacy Protectors"
- Authenticating the Relying Party is more important
  - Transaction Type
  - Business required vs. discretionary attributes
  - Persona in context
    - Pseudonymous Identity
    - Legal Identity
    - Strong Anonymous Identity

- Desired characteristics
  - Trust – Individual, Commericial, Government
  - Critical Infrastructure Provider – carrier grade
  - Global scale & localization

Verizon Experience & Assets

Privacy Protector



Carrier Grade

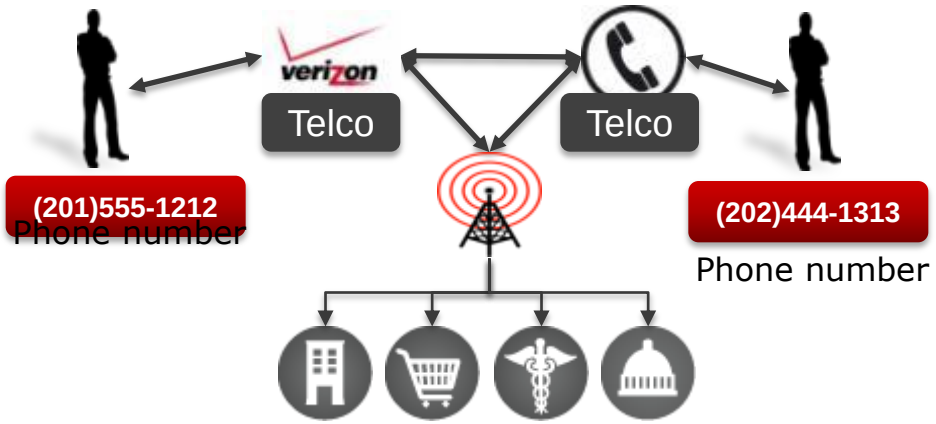
Technology Innovator

Security Pioneer

Vision: Identity is the New Phone Number

Telecommunications Model

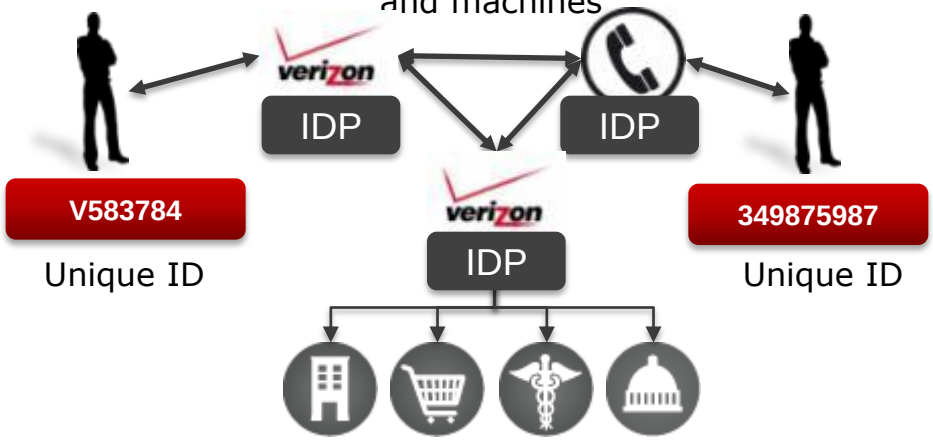
Phone companies operate a network of networks to connect people and machines



- Simple user experience: Works everywhere
- ~3 phone numbers per person. Home, Cell, Work
- Reliability and world class infrastructure
- Standards based
- Global scale
- Value added services built on the network

Secure Communications Model

Trusted Identity Providers (IDP) operate a trusted network of networks to connect people and machines



- Simple user experience: Works everywhere
- 1 person 3 types of identity: Legal, Anonymous, Pseudonymous
- Reliability and world class Infrastructure
- Standards based
- Global scale
- Value added services built on the trust platform

Communications Maturation

Messaging & Persistence

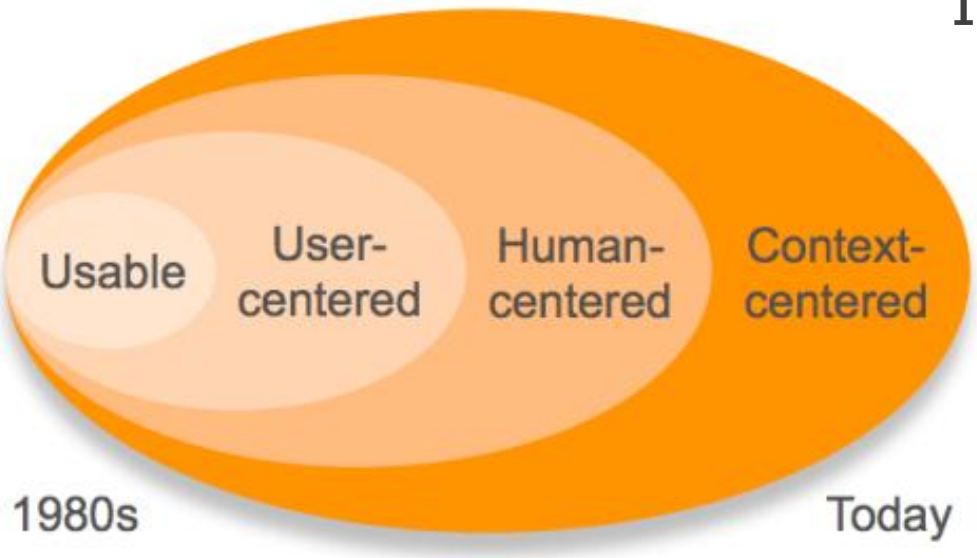
Attributes

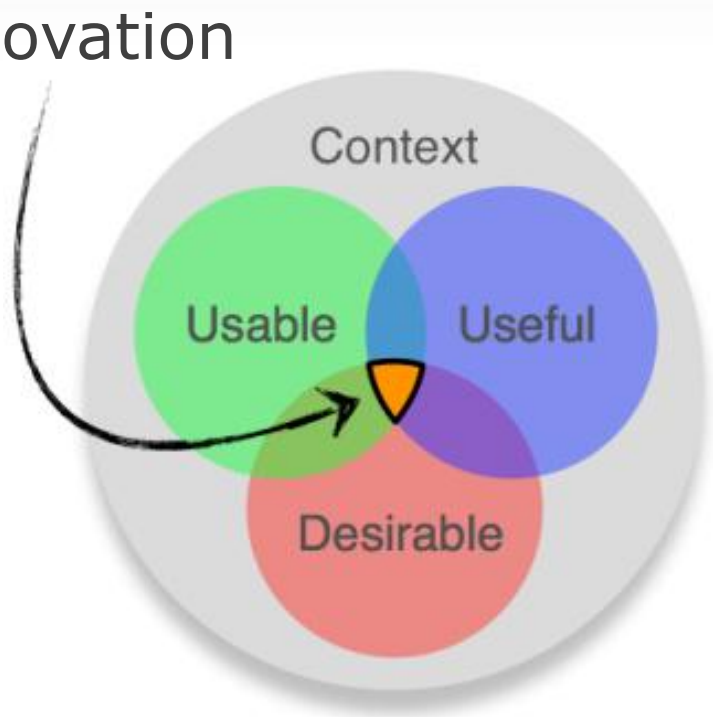
Authentication

Identity Privacy

PCI PHI CPNI PII

Understanding and Integrating Diverse Emerging Technologies





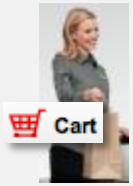
Usable: Can they perform the action?

Useful: Do they have a need for it?

Desirable: Do they want to do it?

Context: Understand the person, their surroundings, and business drivers.

UIS Market Facing Services

People	Identity Form Factors (Verizon & 3rd Party Issued)	Open Standards	Services You Need	Open Standards	Relying Parties
		LDAP X.509 SMS OTP RADIUS OATH	 Identity Issuance Services	ID Microsoft® Active Directory® WS-Trust LDAP OIX SAML RADIUS Kerberos Shibboleth X.509/OCSP	 Work Login
Devices	Identity Form Factors (Verizon & 3rd Party Issued)	Open Standards			
	RFID ECC X.509 Certificate Format Secure https 4G LTE	EEC X.509 SSL/TLS CMP/V2 IPsec	 Authentication Gateway Federation  Risk Services		 Healthcare  Shopping Banking

We need an identity ecosystem in the cloud

Conclusions

- Address Enterprise Challenges by Focusing on the Individual First
- Insure Privacy Protection and Control of Online Collaboration
- Lead/Influence/Advance – Open Standards and Ecosystem Evolution
- Deliver Innovative Carrier Grade Solutions
- Dramatically lower costs and reduce complexity