



Convergence in the US – FIPS 201

Salvatore D'Agostino, Executive Vice President
Digital Identity Forum, London, 20 November 2007

CoreStreet - Introduction



- **Founded October 2001**
 - MIT spin-off
 - Silvio Micali, Chief Scientist
 - Prof Computer Science @MIT
 - Recipient Goedel Prize
 - Inventor of zero-knowledge and interactive proofs
- **Headquarters: Cambridge, MA**
 - Offices in Washington DC & London
- **Patented Intellectual Property**
 - 15 issued & several pending patents on certificate revocation
- **Institutional funding from leading venture partners**
 - Udata and POD Holding
 - Strategic convertible note



CoreStreet - Sustained Growth

- **Revenues**
 - Growth rates of 50-100%/yr
- **100+ Customers in**
 - US Government
 - DoD, GSA (62 Agencies), Veterans Affairs, HHS, DHS, SSA, State, NASA, ...
 - States: MD, PA, IL ...
 - Local: DC, SF, Ports of LA, Jacksonville
 - US Enterprise
 - Finance, Bio-Pharma, Consumer Goods, Telecom
 - EMEA Gov't & Enterprise
 - UK MoD, BAA, Soc Sec Spain, UK Land Registry, Poste Italien, Norway MoD, Statoil, Union Bancaire, BBS, ClearStream, LuxTrust, TDC....
- **Partners**
 - Entrust, CyberTrust, VeriSign
 - DAP - Roper Mobile, LabCal, Symbol
 - Kaba, Assa Abloy, Lenel, Honeywell
 - LMCO, GDIT, EDS, IBM Global, Atos, Logica



The Big Change - Two types of historical credentials

Identity Credential



- Issued by a well regulated, central authority
- Large populations
- Complex, federated authorizations
- Significant anti-fraud protection
- Typically used to determine *identity*
- **Very few electronic transactions**

Transactional Credential



- Issued by ad-hoc, local authorities
- Small populations
- Simple, local authorizations
- Little anti-fraud protection
- Typically used to determine a single *privilege*
- **Many electronic transactions**

The Big Change – Credentials are converging

Identity Credential



Transactional Credential



Smart Credential



- Issued via **standard** regulated, central authority
- Large, interoperable populations
- Complex, federated authorizations
- Strong authentication (up to 4 factors)
- Typically used to determine *identity* and *multiple privileges*
- **May be used for physical and logical security**
- Some people will carry one smart credential, other may have multiple
- **Many electronic transactions, every day**



This Changes Everything

Smart Credential



- The move to fully utilize smart credentials touches every corner of IT and physical security:
 - Identity Issuance
 - Databases
 - Access Control
 - Networks
 - Installation
 - Analytics
 - ...
- The required changes will be even more profound than the shift from client-server to web-based computing.
- In effect, this creates a new **Infrastructure for Convergence and Identity Services**.

Federal Information Processing Standard (FIPS) 201

- **Standard for interoperable credentials**
 - Logical
 - Physical
 - Device
- **Result of Homeland Security Presidential Directive (HSPD) 12**
- **Contact – ISO 7816**
- **Contactless – ISO 14443**
- **2D Bar Code – PDF 417, Code 39**
- **Magnetic Stripe**
- **PKI – x.509, RFC 2560**



Programs/Population

- **HSPD-12**
 - Executive Agencies
 - Contractors
 - Intelligence (opt in)
 - Post Office (opt in)
- **Transportation Workers Identification Credential (TWIC)**
 - Port Workers
 - Seaport, Airport, Rail
 - Transport Worker
 - Truck Drivers
 - Terminal Operators
- **First Responder Authentication Credential (FRAC)**
 - Emergency Support Functions (ESF)
 - National Infrastructure Protection Plan (NIPP)

Other Programs

- **DHS**
 - 47 Programs
 - Registered Traveler
 - Western Hemisphere Traveler Initiative
 - Real ID
 - FAST
 - Etc.
- **State**
 - e-Passport

Example of Scope: The expanding reach of HSPD 12 Federal mandates

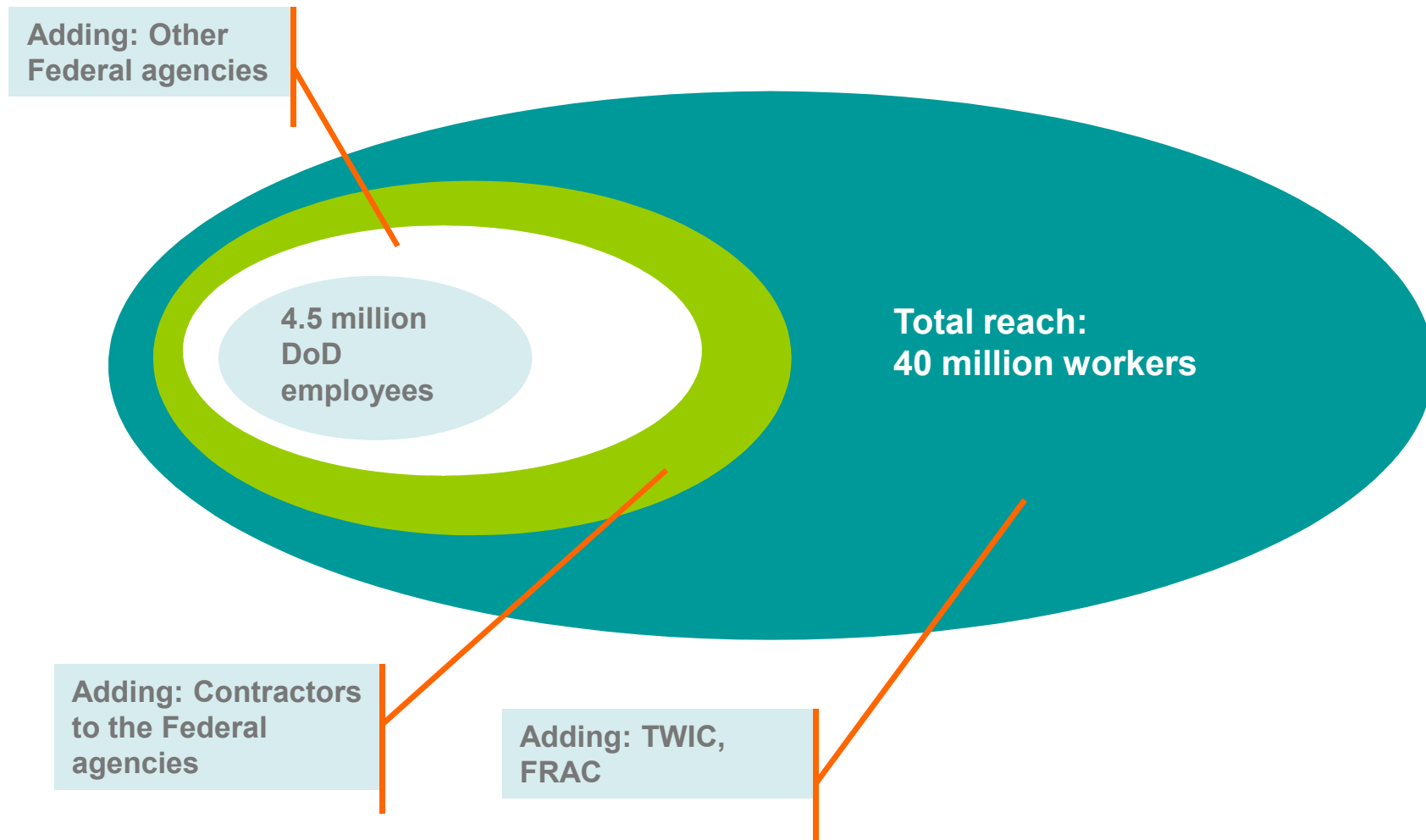


Table A — Emergency Support Functions

Category																
1	NRP ESF Code	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	ESF Description	Transportation	Communication	Public Works & Engineering	Firefighting	Emergency Management	Care, Housing & Human Services	Resource Support	Public Health & Healthcare	Urban Search & Rescue	Oil & Hazardous Materials Response	Agriculture & Natural Resources	Energy	Public Safety & Security	Long Term Community Recovery & Mitigation	External Affairs
3	General Occupation Description Affiliation	Maritime			Fire Chief, Career Firefighter, Volunteer Firefighter	COOP/COG; Director; ERG, Other			Physician; Nurse; EMT; Paramedic	Swift Water Rescue; Collapse Rescue; Wildneres s Rescue				Federal Agent; State Police; Local Jurisdiction Police		
4	NIMS Resource Typing															
5	Regional / Local Code															
6	Regional / Local Description															

If a First Responder has an ESF role or role in IP or both, ESF role takes precedence

Tables are working documents as further refined by practioner communities

Table B — Critical Infrastructure Protection

Category																		
1	NIPP Sector Code	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2	NIPP Sector Description	Agriculture & Food	Banking & Finance	Chemical	Commercial Facilities	Dams	Defense Industrial Base	Emergency Services	Energy	Government Facilities	Information Technology	National Monuments & Icons	Nuclear Reactors, Materials & Waste	Postal & Shipping	Public Health & Healthcare	Telecommunications	Transportation	Water
3	Affiliation																	
4	CIP Description																	

If a First Responder has an ESF role or role in IP or both, ESF role takes precedence

Tables are working documents as further refined by practioner communities

Strong Authentication Across the Board

- **PIV Authentication Certificate**
 - Logical Access
- **Card Authentication Certification**
 - Physical Access
 - Bidirectional readers
 - Challenge and Response Computational Capability



Industry Solutions

- **Approved Products List (APL)**
- <http://fips201ep.cio.gov/apl.php>
- **300+ products**
- **Logical and Physical Security**
- **Complete solution set**
- **Interoperability Guarantee**

