NextgenID®

NextgenID.com

Trusted Transactions

27 January 2015

The Global Leader in Biometric Intelligence

Today’s discussion….

Provide a context –

Operational & threat environment

Trust Framework – Public & Private Efforts

State & Federal Coordination

Quick Overview

Drivers..

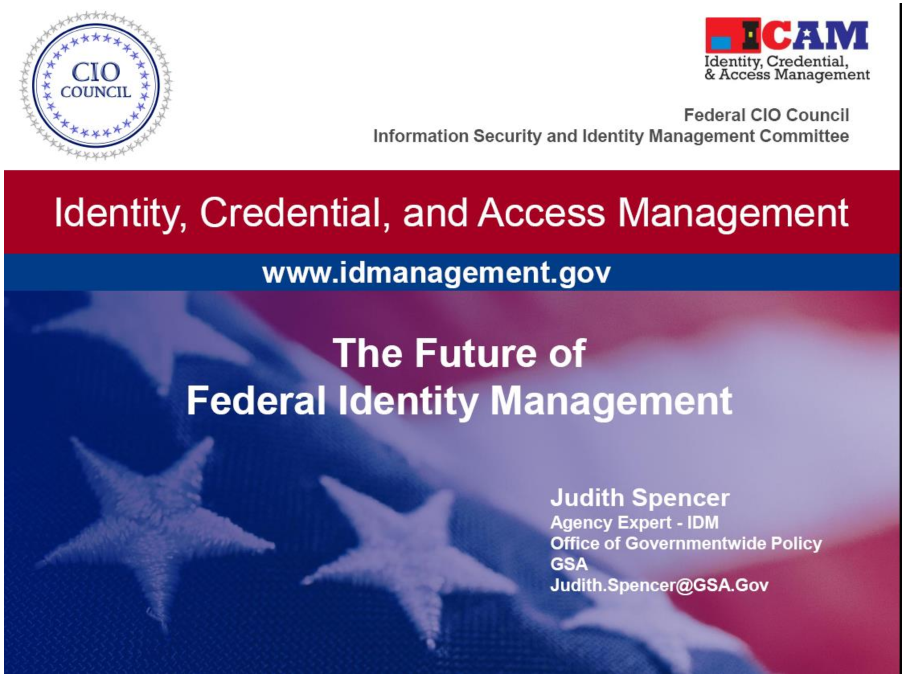
Selected
Zoom Out
Select:
Checking – S Smith
Checking – J. Benton
Suzie Smith
12395 Cedar Road, Apt 225, Cleveland
John Benton
CO Loan – J. Benton
Ph: 440-525-6565
SIU - Loan – J. Benton
Checking – J Wilson
Ph: 216-525-6565
BALTIMORE
CITISTAT
Disease Surveillance Network
Fully identified records
Deidentified records
Deidentified data sharing
Radiology
Diagnostic laboratories
Poison control
Prescriptions
Physician office visits
Over-the-counter sales
Nurse call center
Hospital EDs
District of Columbia
ESSENCE
Pharmacy data
Tri-s outpat
NCR Military ESSENCE
Aggregated NCR ESSENCE
Virginia
ESSENCE
Hospital EDs
Absenteeism
Maryland ESSENCE
Figure 1. NCR Syndromic Surveillance Network.
Incident Manager: All open incidents
Page Refreshed Feb 28, 2011 9:35:57 PM UTC
Views
Search
View
View search criteria
Standard
My open incidents and problems
Unassigned incidents
Unacknowledged incidents
Escalated incidents
All open incidents
Unassigned problems
All open problems
Events without incidents
Custom
Create...
Manage...
No view available
Getting Started
Severity
Summary
Target
Priority
Status
Last Updated
Owner
Type
The heap usage is 92%.
[redacted]
None
New
Feb 28, 2011 9:28:59 PM
Incident
The heap usage is 92%.
General
Events
My Oracle Support Knowledge
Updates
Related Events And Incidents
Incident Details
Metric Heap Usage (%)
Target
[redacted]
(Oracle WebLogic Server)
Summary The heap usage is 92%.
Event Type Metric Alert
Category Unclassified
Tracking
Acknowledge
Add Comment...
Manage...
More
Guided Resolution
Diagnostics
Actions
Edit Thresholds
Views for filtering
Manage incident workflow
Details of selected incident
Guided diagnostics and resolution
30 Days)
ult Firearm
sidential
251
25
253
24
26
221
BREAKING NEWS
SUSPECTS' VEHICLE HAS BEEN TOWED TO MONTGOMERY CO.
S&P
2.07
© AFP/Getty Images
er questions
a Visualization
Forage for Data
Explore
Task
Visualize
Act
Develop Insights
CYBER
ATTACK

Requirements Framework ….

Secure and reliable forms of identification

- Issued based on sound criteria for verifying an individual identity
- Strongly resistant to identity fraud, tampering, counterfeiting, and exploitation
- Can be rapidly authenticated electronically for physical and logical access
- Is issued only by providers whose reliability has been established by an official accreditation process.
- Graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.
- Supports physical and logical access
- Open Standards, supports shared services
- Supports federation, trust, and reuse – issue once, reuse many
- Functional in day-to-day and emergency operations

Policy Framework



CIO COUNCIL

ICAM
Identity, Credential, & Access Management

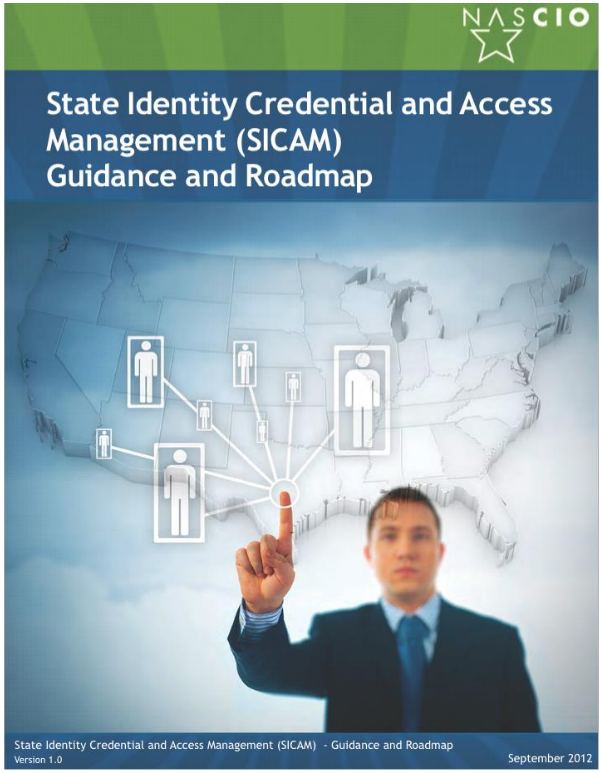
Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

www.idmanagement.gov

The Future of
Federal Identity Management

Judith Spencer
Agency Expert - IDM
Office of Governmentwide Policy
GSA
Judith.Spencer@GSA.Gov



NASCIO

State Identity Credential and Access Management (SICAM)
Guidance and Roadmap

State Identity Credential and Access Management (SICAM) - Guidance and Roadmap
Version 1.0

September 2012

NASCIO Guidance & Roadmap

http://www.nascio.org/publications/documents/SICAM.pdf

Call to Action

http://www.nascio.org/publications/documents/NASCIO-Call-to-Action-The-Necessity-for-Maturing-Identity-and-Access-Management-in-State-Government.pdf

Cut to the chase

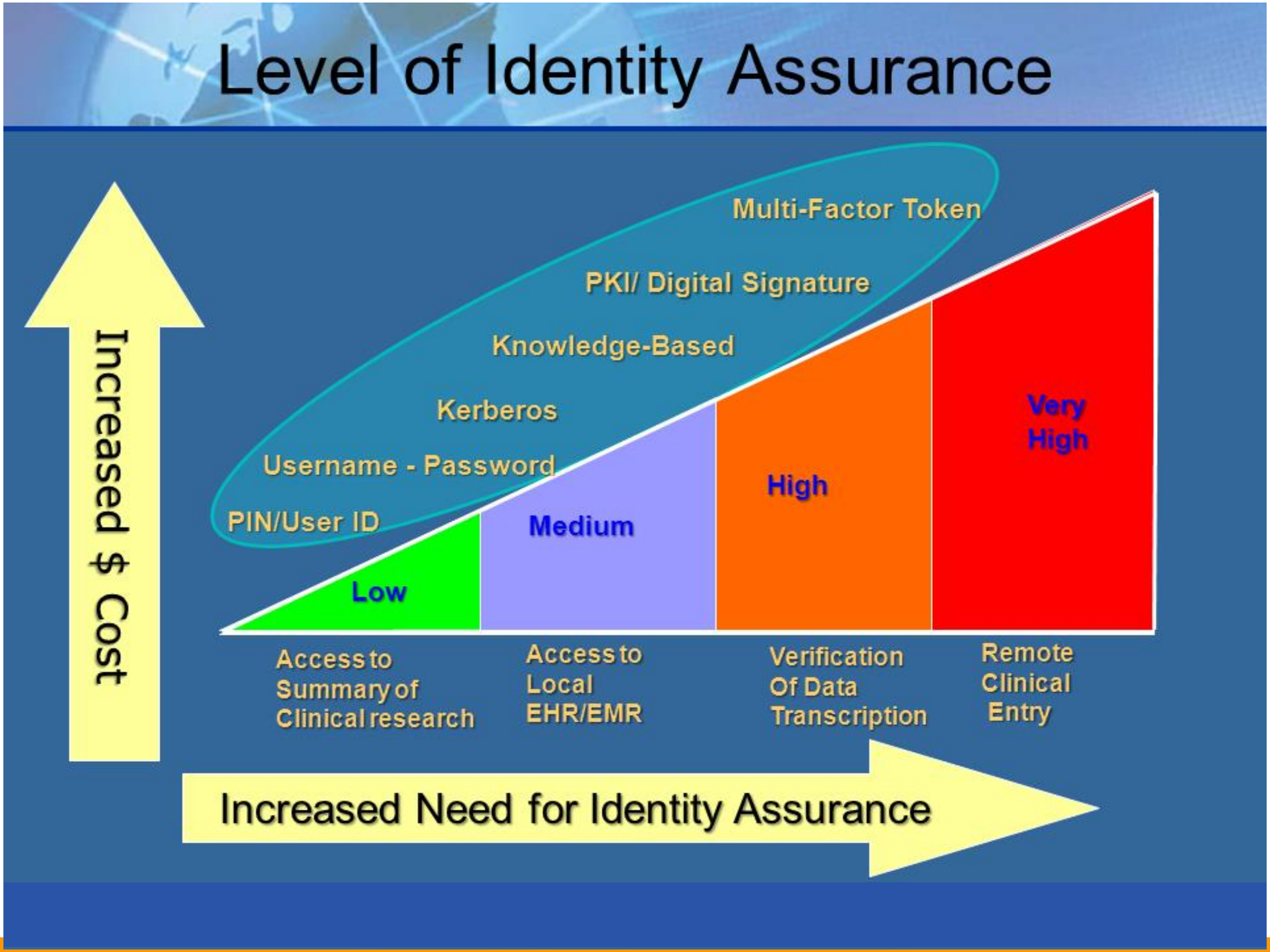
One size does not fit all

Why:

- Assurance – Risk / Certainty Needs Dictate the Need
- G2G, G2B, G2C, B2B, B2C, C2C
- Diversity of form factors, media use cases, & preferences
- Different community needs & trust frameworks

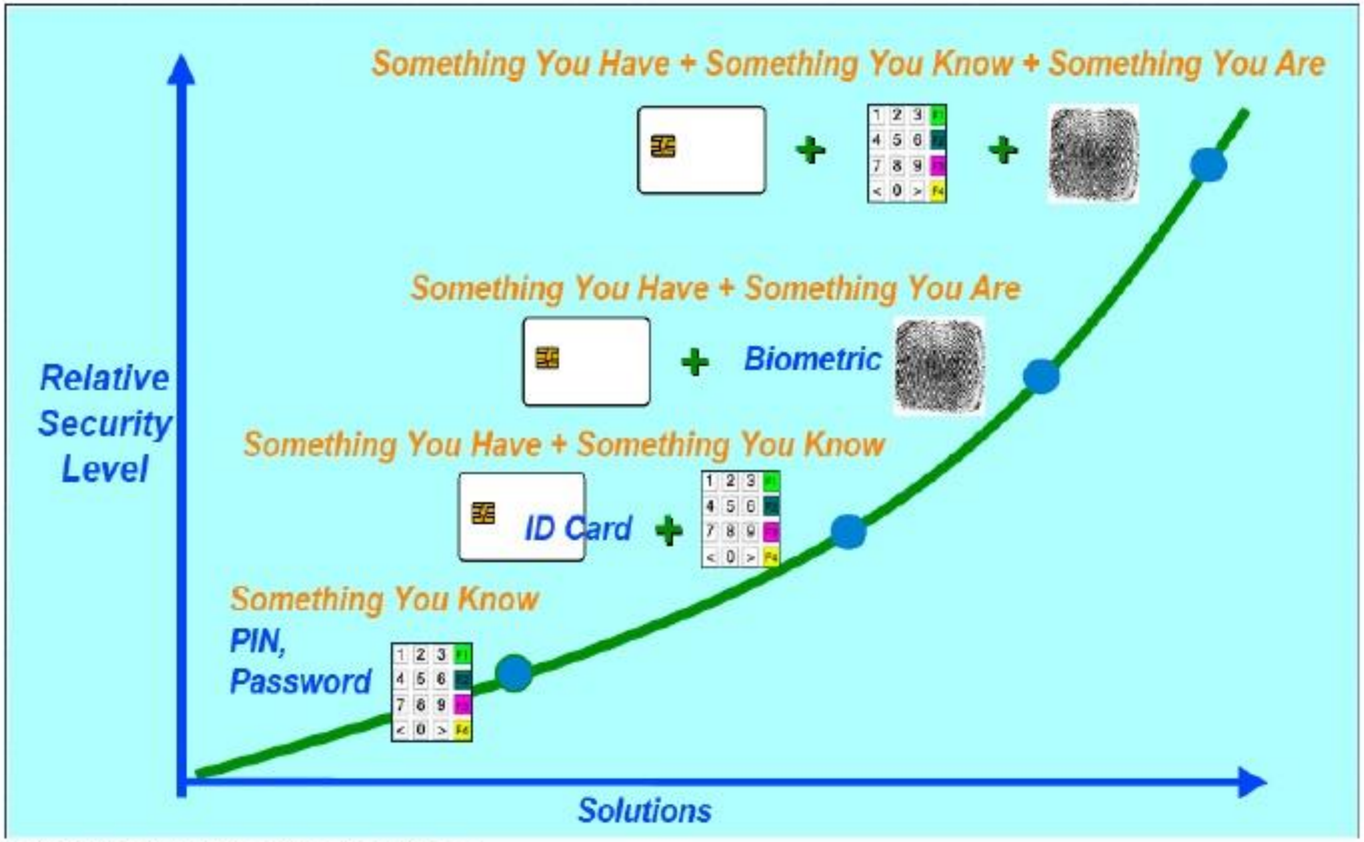
  - Access to Federal Data and Systems?
  - Access to Healthcare Records and Systems?
  - Access to DMV Systems to Register My Car(s)?
  - Access to State Systems to Pay my Taxes…?
  - Ability to Securely Send Digital Data Securely?

Healthcare example



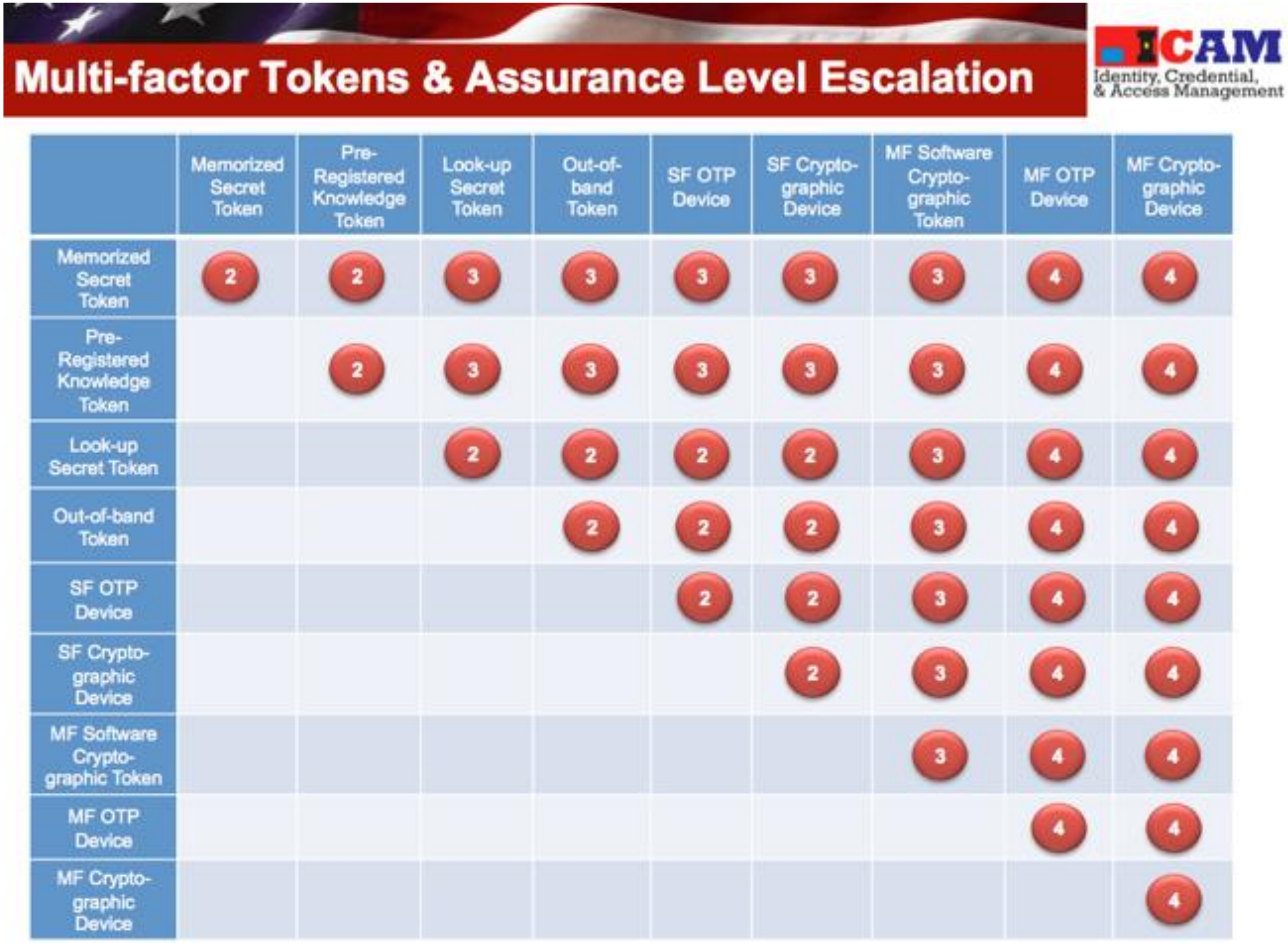
Identity Assurance Levels

Security Levels vs. Identity Assurance


Something You Have + Something You Know + Something You Are
Something You Have + Something You Are
Biometric
Something You Have + Something You Know
ID Card
Something You Know
PIN,
Password
Relative Security Level
Solutions

Courtesy: Randy Vanderhoof, Smartcard Alliance

Identity Assurance Escalation



Multi-factor Tokens & Assurance Level Escalation

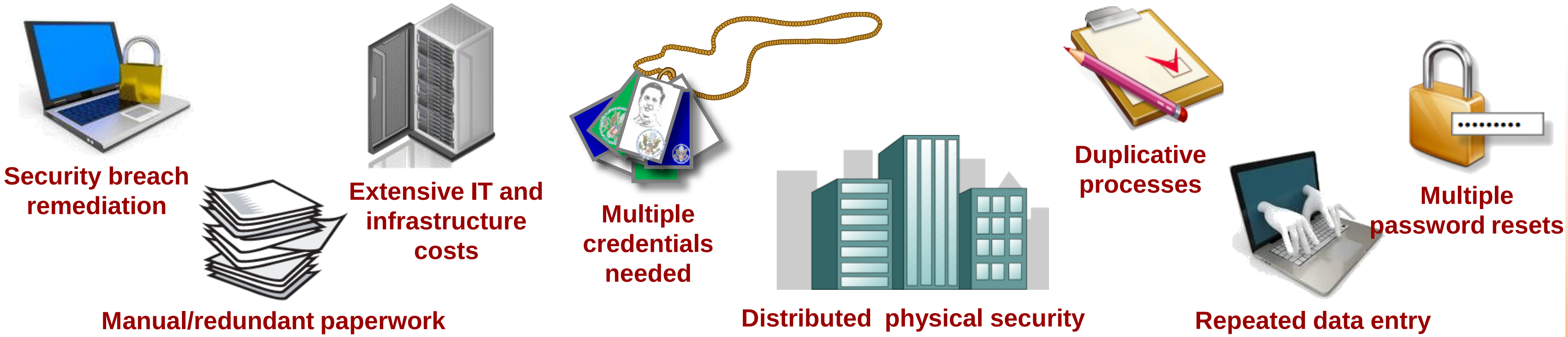
ICAM
Identity, Credential, & Access Management

	Memorized Secret Token	Pre-Registered Knowledge Token	Look-up Secret Token	Out-of-band Token	SF OTP Device	SF Cryptographic Device	MF Software Cryptographic Token	MF OTP Device	MF Cryptographic Device
Memorized Secret Token	2	2	3	3	3	3	3	4	4
Pre-Registered Knowledge Token		2	3	3	3	3	3	4	4
Look-up Secret Token			2	2	2	2	3	4	4
Out-of-band Token				2	2	2	3	4	4
SF OTP Device					2	2	3	4	4
SF Cryptographic Device						2	3	4	4
MF Software Cryptographic Token							3	4	4
MF OTP Device								4	4
MF Cryptographic Device									4

PIV-I & CIV Streamlines Operations & Reduces Duplication

By implementing and standardizing on PIV-I and CIV, agencies experience significant cost-savings and added value.

Current State in North Carolina



Security breach remediation

Extensive IT and infrastructure costs

Multiple credentials needed

Duplicative processes

Multiple password resets

Manual/redundant paperwork

Distributed physical security

Repeated data entry

In an Administrative Environment

Cost-savings from:

- Minimized password resets
- Reduced infrastructure and hosting costs on other credential types
- Minimized security breaches
- Phasing out duplicative processes and IT investments

Added value from:

- Minimized paperwork/manual processes
- Enhanced information-sharing
- Dramatic time reduction & handling savings through Digital Signatures
- Improved user-satisfaction with a single PIN vs. multiple passwords

PIV-I & CIV Credential Overview

The PIV credential has a variety of security features, notably the use of Public Key Infrastructure (PKI) cryptography to provide strong identity assurance in an interoperable manner.

Common Processes

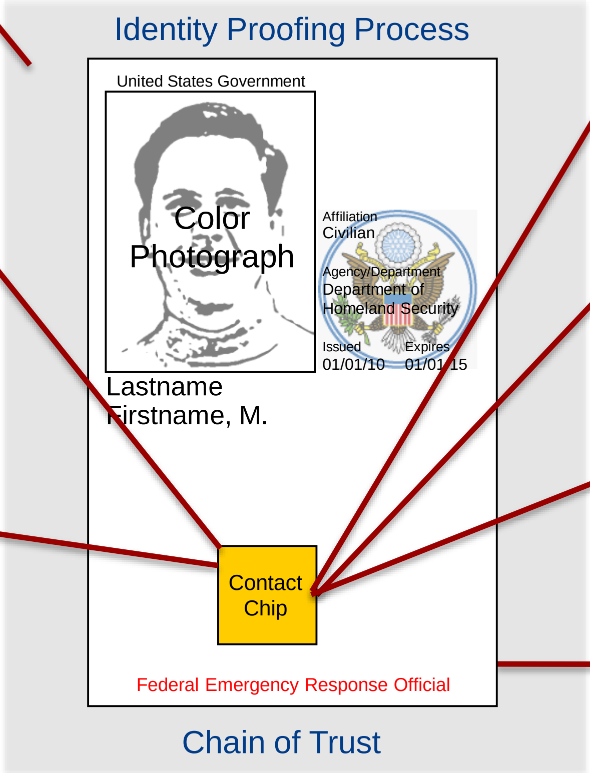
Identity proofing and background investigation processes that build a chain of trust.

Biometric Authentication

Fingerprint and/or iris information used for authentication that binds the identity of the user to the credential.

PIN

Something that only the user knows and is used to access various applications. Replaces cumbersome and insecure passwords for applications.



PKI Authentication

Digital certificate on the card that supports electronic verification of the cardholder.

PKI Digital Signature

For electronically signing documents to provide non-repudiation and message integrity.

PKI Encryption

For cryptographically protecting data at rest and in transit in order to provide confidentiality.

Physical Features

Strong anti-counterfeiting features (e.g., laser etching, holographic images).

Trusted Identity is Multifunctional

Physical Token, Enterprise Identity, Mobil Devices

Derived Credentials

We live in “Mobile Times” –

Challenge: Public and Private Sectors need to protect mobile devices, employees use of smart phones and tablets.

How to securely authenticate users on mobile devices.

CIO Council Charged NIST to develop a response to the challenges encountered in authenticating mobile devices

- Cryptographic credentials derived from a Personal Identity Verification (PIV) card or Common Access Card (CAC) that are carried in a mobile device instead of the card (Derived Credentials).
- Special Publication (SP) 800-157,
  - Defines technical specifications for implementing and deploying Derived PIV credentials to smartphones, tablets, iPads and other mobile devices.

Operational value

Implementation Directly

Workstation Identification/authentication

Digital Signing (Microsoft Office; Data, Objects)

Encryption - Files and Data object

Physical Access Control- Replace/Consolidate Multiple Systems

Individual Multi-Factor Authentication

- Identity and Attribute
- Physical & Logical Network/System Access
- Decision & Delegation

Derived Credentials

Mobile Device Protection & Capability

Enterprise & Inter-Enterprise Federation

Enterprise/Federated Identification/Authentication

Workflow Processes & Enablement - Multiple Commercial Products (Adobe, DocuSign..)

Automatic Encryption - Data within applications

Federated Logical & Physical Access Empowerment

Federated & Enterprise Authentication Strategies

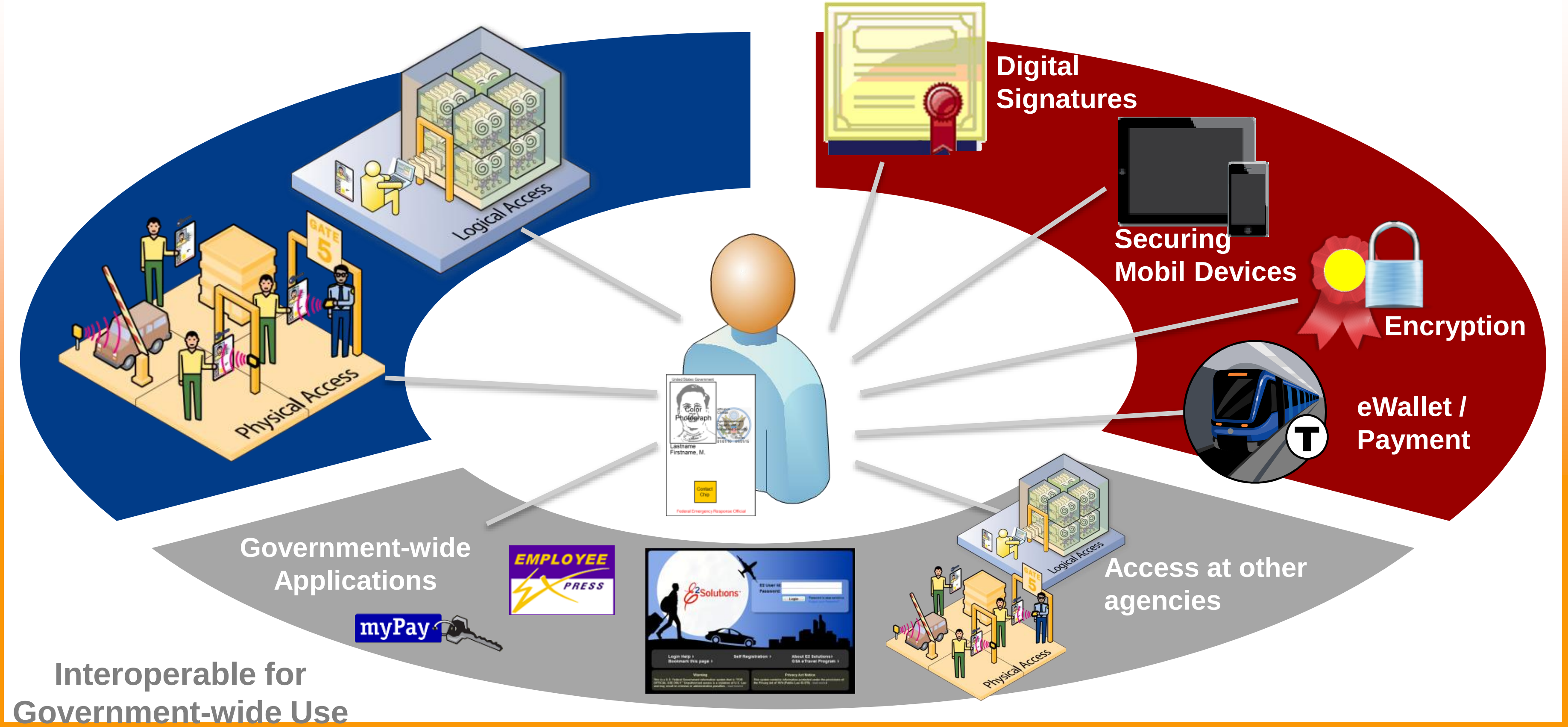
- Federated Identities and Attributes
- Physical & Logical Network/Enterprise
- Federated Decision & Delegation

Derived Credentials & Enterprise Mobility

- Mobile Device Protection / Capability

Using the PIV-I & CIV Credential

A single credential gets you in the front door to your office, onto your computer, allows you to securely sign and encrypt data, and access government-wide tools and resources at other agencies. This is possible today with PIV-I & CIV credentials.



PIV-I & CIV Credentials vs. Other Credentials

PIV-I & CIV credential provides many features and benefits that other credentials are unable to offer

	Password	OTP Tokens	PIV-I / CIV
User vetting	✓	✓	✓
High identity assurance		✓	✓
Interoperability			✓
Accredited issuance processes			✓
Cross-agency trust			✓
Use for physical and logical access			✓
Encryption			✓
Digital Signature			✓
Efficiencies			✓
Biometric binding of identity			✓

PIV-I & CIV / Trusted-Identities are Enablers

The trusted credentials are enablers for efforts across Government to move toward a stronger, more secure, and more efficient presence.

Cybersecurity

Strengthens the security and resiliency of critical infrastructure against evolving threats to safeguard the government.

E-Government

Promotes the use of electronic forms and offers online-based government services for strong authentication.

Information Sharing

Encourages sustained, responsible, and trusted collaboration to support interoperability across the government.

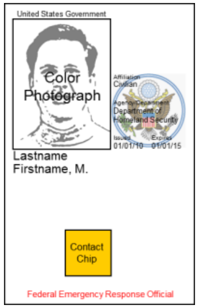
Good Steward of IT Resources

Emphasizes planning and spending control processes for investment in information systems to support agency missions.

Standards-based Solutions for Emerging Needs

Public and private sector workforce want and expect more flexibility in their work and workspace. Secure and Trusted transaction are allow use of mobile devices and support employee mobility.

+



United States Government

Color Photograph

Affiliation
Civilian

Agency/Department
Department of Homeland Security

Issued
01/01/10

Expires
01/01/15

Lastname
Firstname, M.

Contact Chip

Federal Emergency Response Official

=

Perform these secure transactions from any location!

- Strongly authenticate
- Digitally sign and encrypt data
- Access applications

+

=

Use mobile devices to strongly authenticate to agency resources!

Costs for Operations/Services

…Cost is relative to value… it depends on where you sit

Three Separate Audiences, each with different priorities:

"C" Suite Level - Policy & Budget

- Enterprise Strategy, implementation, legacy systems
- Trusted identities & authentication enables multiple priorities

Department Level - Competition of resources across missions

- Capability, consistency, interoperability, leveraging
- Identity buried as a minor commodity

Agency Level – Mission Orientation

- Respond to mission better, faster, cheaper
- Quality of life & service enhancements
- Competing mission shortfalls

Goal is to Align Goals & Support – Enterprise, Department, & Agency – Into an Initial Implementation Effort

Enterprise Architecture to Community Practices

Enterprise Architecture Delivers Capabilities to Common Transactions & Processes

- Multifactor Systems Authentication
- Single Sign-on; Digital Document Signature

Departments & Agencies

- Responsible for Mission Execution
- Consume & Shape Enterprise Capabilities
- Mission & Specialized or Specific Processes Drive Unique Requirements & Capabilities for Public Safety
- Support to operationalization capabilities and benefits

Agency & Execution Levels

- Resources and support to integrate into operations
- Identify specific priority use cases and value

Agencies lead Implementation & Adoption
In Mission Unique & Priority Use Cases

From a Public Safety Perspective
Preparedness, Response, Recovery & Mitigation

Day to Day

- Hardening of Critical Facilities & Systems
  - Cyber Threat, Logical and Physical Access
  - Reduction of separate and redundant systems, passwords
- Daily Operations
  - Supports integration across multiple of systems
  - Much better user experience in fused data environment
  - More effective credentialing & record keeping
  - Supports automation & maturation of ICS capabilities
  - Automation, security, and user enhancements in the field

Response

- Accelerate response, access, integration
  - “Responders” are, have, and can prove their identity, skills, authorization
  - Authentication of identity and authority for systems and facility access
  - Reduced time to gain entry, access, or assemble across systems
  - Provide Trusted Data in Coms-In & Coms-Out Environment
  - Post-Event Reimbursements (time, manpower, costs)
  - Non-repudiation / digital signature in records process

Cost Value

Credential cost vary on the number purchased, quality of the credential

High Authentication Credential that is valid for 3 years, $43 - $63 per year

…sounds expensive?

What do you spend on current credentials and multiple systems? …

What can a High Authentication Credential do that my current credential can't ...

- Single Sign-on & elimination of Password Reset - $25-100 savings a person/year
- Digital Signature – System cost savings $125 per wet signature – 3 Year Analysis conducted between HHS, US Cancer Institutes, SAFE Bio-Pharma, Hospitals
- Reduce Redundant Systems – 60-80% System Costs are redundant and a source data conflicts – DHS Architectural Review Board 2009
- System Consolidation – reduction of multiple systems, configurations, cards & credentialing systems.
- Fraud Reduction – Medicare/Medicaid. SNAP, WIC, LIHEP,
  - Benefit Programs - 12-17% of $8 Billion Medicare / Medicaid - State of Virginia-

… so what is the value per trusted identity

Takeaways

- PIV-I & CIV are **fiscally responsible IT**, provides for consolidation of investments, reduces redundancy and stove pipes, and promotes integration
- PKI is a **robust technology** that is used everyday so that websites can be trusted to conduct transactions and supports two and three level factors of authentication.
- PIV-I & CIV provides a **very high level of assurance of identity** and this **facilitates trust**.
- PIV-I & CIV provides **interoperable, crypto-based authentication** for logical and physical access.
- PIV-I & CIV credential can be used for **value-added functionality** such as digital signatures, which **reduce paper forms, and encryption**, which **protects data at rest and data in transmission.**

CIO COUNCIL

NASCIO
Representing Chief Information Officers of the States

Thank You

Points of Contact

Dario Berini,
(703) 929-5543, Dberini@NextGenID.Com

Tom Lockwood
(202) 669-8845, Tlockwood@NextGenID.Com