Identity in Cyberspace:
Improving Trust for Health Information Exchange

Jeremy Grant

National Institute of Standards and Technology (NIST)

Imagine if…

Four years from now, 80% of doctors and patients carried a secure credential, bound to a smartphone, for identification and authentication – and organizations could trust this credential in lieu of existing username/password systems.

Interoperable with login systems

(you don't have to issue credentials)

Multi-factor authentication

(no more password management)

Tied to a robust **identity proofing** mechanism

(you know if they are who they claim to be)

With baked-in rules and technologies to **protect privacy**

What would this mean…

For Improved Security?

- 5 of the top 6 vectors of attack in 2011 data breaches tied to passwords
- Weak identity systems make it impossible to know who is a “dog on the Internet” – hindering what services can be offered online

For Breaking Down Barriers to Exchange of Health Information?

- Choice of proven, easy-to-use identity solutions for providers
- Streamlined workflow by eliminating multiple user IDs and passwords
- Secure access for patients to their own information

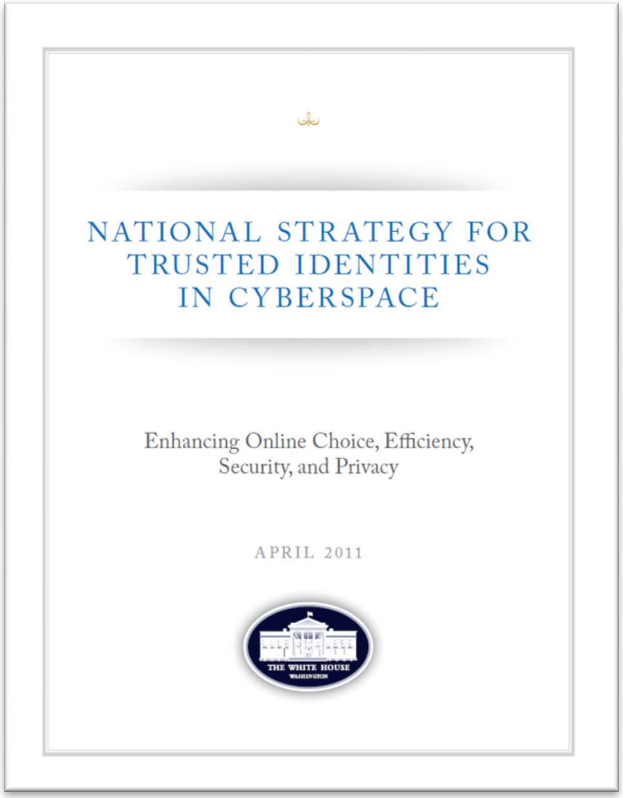
NSTIC Outlines a Path Forward

Called for in President’s Cyberspace Policy Review (May 2009):
a “cybersecurity focused identity management vision and strategy…that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation.””

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.”



NATIONAL STRATEGY FOR
TRUSTED IDENTITIES
IN CYBERSPACE

Enhancing Online Choice, Efficiency,
Security, and Privacy

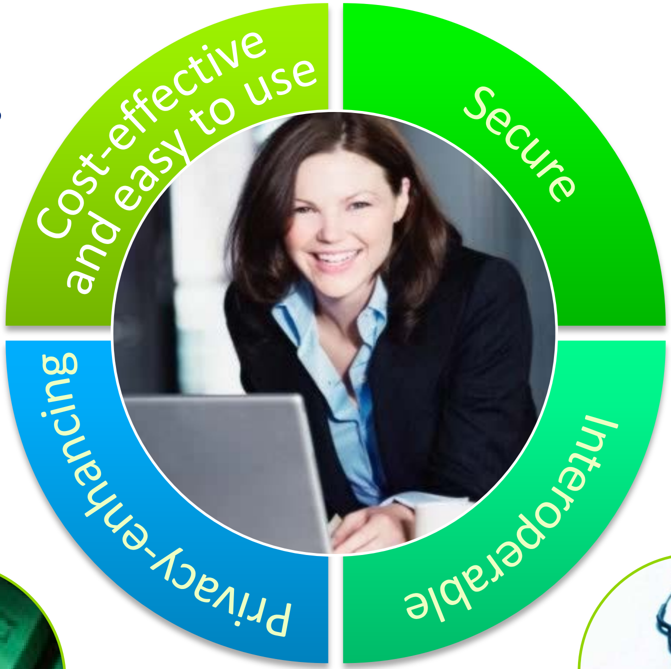
APRIL 2011

THE WHITE HOUSE
WASHINGTON

January 1, 2016

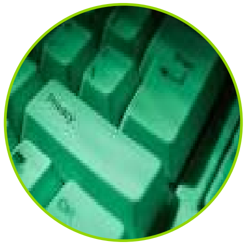
The Identity Ecosystem: Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime.

Streamlined provider access to multiple systems



Secure, online patient access to health information

Ability to include identity attributes will enhance privacy



Improved care through secure exchange of electronic medical records

Privacy and Civil Liberties are Fundamental

Increase privacy

- Minimize sharing of unnecessary information – shifting focus to sharing only “need to know” attributes
- Minimum standards for organizations - such as adherence to Fair Information Practice Principles (FIPPs)

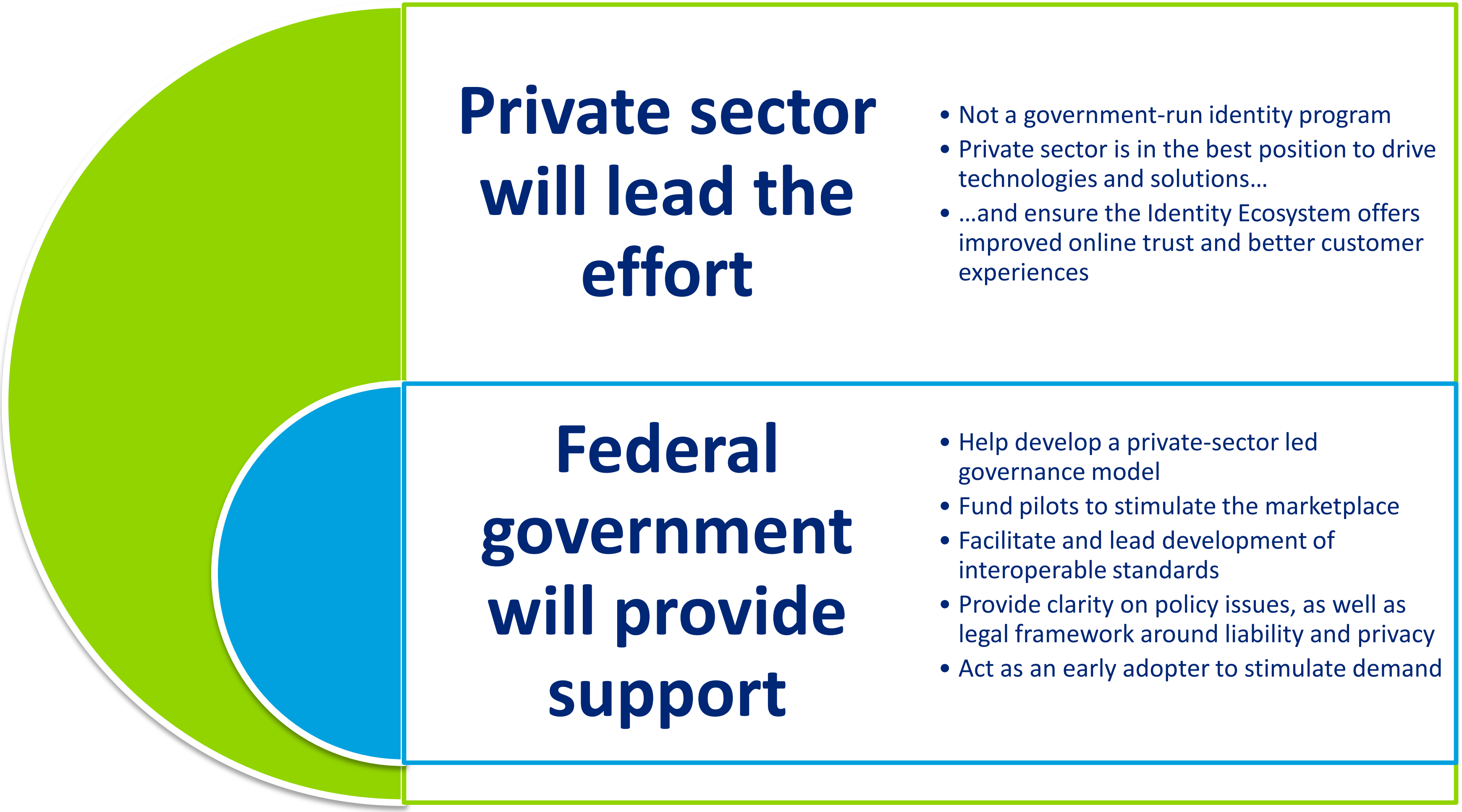
Voluntary and private-sector led

- 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

What does NSTIC call for?



Private sector will lead the effort

- Not a government-run identity program
- Private sector is in the best position to drive technologies and solutions…
- …and ensure the Identity Ecosystem offers improved online trust and better customer experiences

Federal government will provide support

- Help develop a private-sector led governance model
- Fund pilots to stimulate the marketplace
- Facilitate and lead development of interoperable standards
- Provide clarity on policy issues, as well as legal framework around liability and privacy
- Act as an early adopter to stimulate demand

NSTIC lays out a path for the future…

…FICAM Trust Framework Providers offer solutions today

- Secure, interoperable and privacy-enhancing process by which federal agencies (and others) can leverage commercially issued digital identities and credentials
- Craft "approved profile" of widely used commercial identity protocols like **OpenID** and **SAML** to maximize security and privacy.
- Privacy criteria based on the **FIPPs**: Opt in; Minimalism; Activity Tracking; Adequate Notice; Non Compulsory; and Termination
- Non-federal organizations are approved to be **Trust Framework Providers** (TFPs) – who then assess and accredit commercial identity providers who embrace the USG profiles and abide by the privacy criteria

-Kantara *-InCommon*
-SAFE Bio-Pharma *-Open Identity Exchange (OIX)*

Federal IdM activities are aligned through the Federal CIO Council Identity, Credential and Access Management (ICAM) Subcommittee

The good news: there is an emerging marketplace for FICAM-approved multi-factor credentials today

3 years ago

- Solutions limited to just a few technologies and form factors, no accreditation process

Today

- The marketplace is producing a wide range of new solutions – smashing through previous cost and usability challenges, making strong authentication easier to deploy and use.
- FICAM "Trust Framework Provider" certification process is providing a foundation for a marketplace of certified multi-factor authentication solutions*

*Found at http://www.idmanagement.gov/pages.cfm/page/ICAM-TrustFramework-IDP

Key drivers

1. DEA ePrescribe rule calls out NIST SP 800-63-1 LOA 3 (March 2010)
2. NIST recognizes GSA's FICAM Trust Framework Provider Adoption Process (TFPAP) as the only certification process for 800-63-1 (December 2011)
3. GSA certifies Kantara and SAFE BioPharma as first two Trust Framework Providers for non-PKI LOA3 (November 2011 and Spring 2012)
4. Verizon becomes first non-PKI LOA3 certified IdP; several others in the queue (November 2011)
5. CMS outlines plans to support all FICAM approved external credential providers (February 2012)
6. Experian approved as an identity proofing provider at LoA3 (July 2012)

Impact

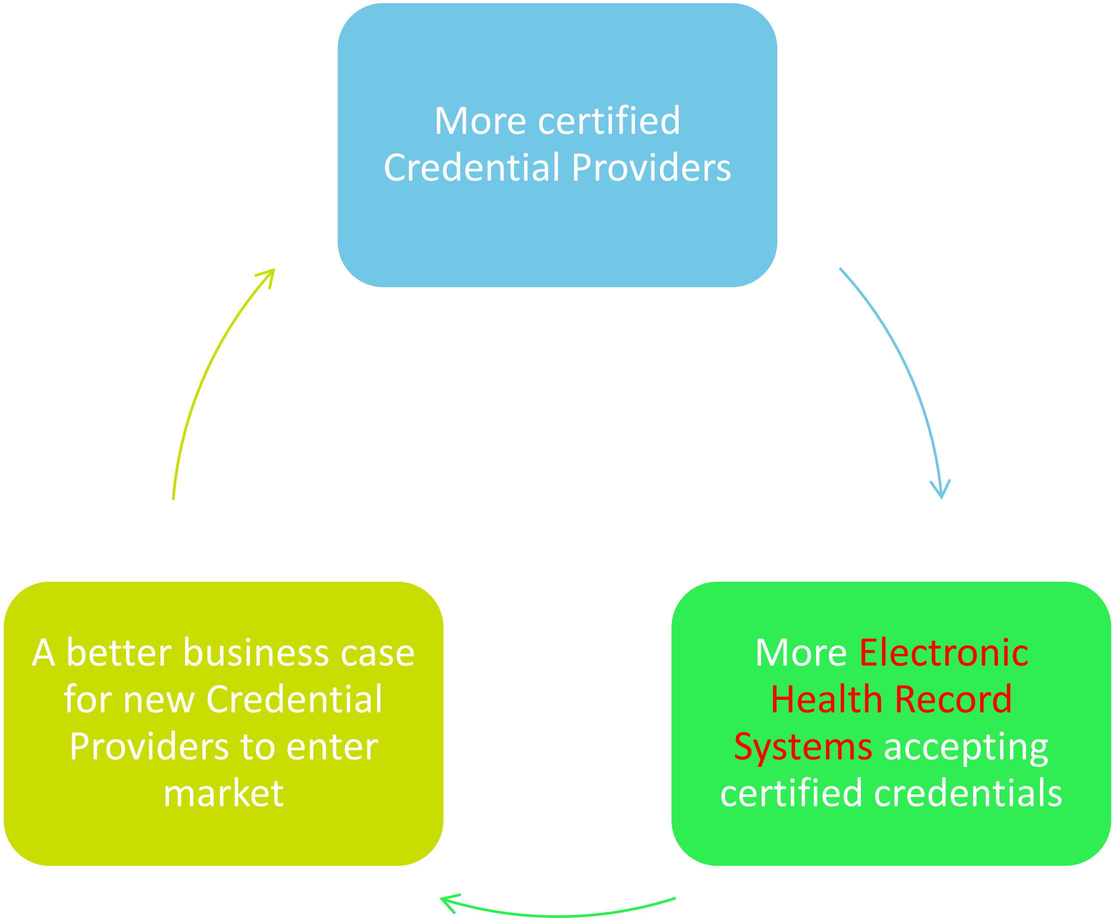
Short term:

- A physician will be able to use the same certified credential both for ePrescribe and at CMS

Long term:

- Why not leverage that same credential elsewhere in the health ecosystem?

Supporting a Standards-based Approach – The Virtuous Circle



More certified Credential Providers

More Electronic Health Record Systems accepting certified credentials

A better business case for new Credential Providers to enter market

NSTIC Next Steps

Convene the Private Sector

- New **Identity Ecosystem Steering Group (IDESG)** launched August 2012; more than 360 organizations and 230 individuals have signed up to participate. www.idecosystem.org.
- A privately-led Steering Group tasked with convening stakeholders to craft standards and policies to create an Identity Ecosystem Framework

Award Pilots

- FFO published in early 2012 for **$9-10M NSTIC pilots grant program**
- Awards expected this month
- Challenge-based approach focused on addressing barriers the marketplace has not yet overcome

Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the **Federal Identity, Credential, and Access Management (FICAM**) Roadmap
- New White House initiated effort to create a **Federal Cloud Credential Exchange** (FCCX)

How HIT Stakeholders Can Support NSTIC

Participate

- JOIN: the Identity Ecosystem Steering Group
- TALK: about the value of NSTIC to colleagues
- SUPPORT: NSTIC Pilots by volunteering to be a relying party

Be early adopters

- Leverage FICAM approved identity providers
- Consider ways to support identity and credentialing in partnership with trusted third parties

Talk to us!

- You are a key partner, we want to hear from you

Questions?

Jeremy Grant

jgrant@nist.gov

202.482.3050

www.nstic.gov

@nsticnpo

www.idecosystem.org