National Strategy for Trusted Identities in Cyberspace

Enhancing Online Choice, Efficiency, Security, and Privacy

The NSTIC envisions that:

Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation

In achieving this vision, the NSTIC identifies four guiding principles to which solutions must adhere:

Identity Solutions will be Privacy-Enhancing and Voluntary
Identity Solutions will be Secure and Resilient
Identity Solutions will be Interoperable
Identity Solutions will be Cost-Effective and Easy To Use

The problem and the approach:

In the current online environment, individuals are asked to maintain dozens of different usernames and passwords, one for each website with which they interact. The complexity of this approach is a burden to individuals, and it encourages behavior—like the reuse of passwords—that makes online fraud and identity theft easier. At the same time, online businesses are faced with ever-increasing costs for managing customer accounts, the consequences of online fraud, and the loss of business that results from individuals' unwillingness to create yet another account. Moreover, both businesses and governments are unable to offer many services online, because they cannot effectively identify the individuals with whom they interact. Spoofed websites, stolen passwords, and compromised accounts are all symptoms of inadequate authentication mechanisms.

The NSTIC charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions.

Private sector-led, government supported:

Only the private sector has the ability to build and operate the complete Identity Ecosystem, and the final success of the Strategy depends upon private-sector leadership and innovation The key operational roles within the Identity Ecosystem include: subjects, relying parties, identity providers, attribute providers, and accreditation authorities For each of these ecosystem roles, the private sector will constitute the majority of the actors.

The Federal Government's role is to:

- Advocate for and protect individuals;
- Support the private sector's development and adoption of the Identity Ecosystem;
- Partner with the private sector to ensure that the Identity Ecosystem is sufficiently interoperable, secure, and privacy protecting;
- Provide and accept Identity Ecosystem services for which it is uniquely suited; and
- Lead by example and implement the Identity Ecosystem for the services it provides internally and externally.

Recent and upcoming activities:

- NIST hosted workshops on governance and privacy in June; a technology workshop is coming this Fall
- Federal Government will develop an Implementation Roadmap that identifies and assigns responsibility for near- and long-term actions that the Federal Government can perform
- Requirements and recommendations for pilots and the private sector-led steering group are coming this year.

Contact: Michael Garcia (michael.garcia@nist.gov, 202-590-0979)