



# NSTIC: Facts at a Glance

## **1. What is the NSTIC?**

The [National Strategy for Trusted Identities in Cyberspace](#) (NSTIC) is an Obama administration initiative that broadly defines an Identity Ecosystem that would re-establish trust and better protect online identities.

According to the Howard A. Schmidt on [the White House blog](#), "Through the strategy we seek to enable a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential (e.g., a smart identity card, a digital certificate on their cell phone, etc.) from a variety of service providers – both public and private – to authenticate themselves online for different types of transactions (e.g., online banking, accessing electronic health records, sending email, etc.)."

## **2. What was the impetus for the NSTIC?**

U.S. citizens are increasingly using the Internet for sensitive transactions, like banking, mortgage applications, buying and trading stocks, and reviewing healthcare information. Given this, there are very real problems of identity management, privacy and security in cyberspace. NSTIC aims to give individuals and organizations the ability to complete online transactions with confidence and trust, and without the threat of cybercrime.

## **3. What are the goals for the NSTIC?**

According to the [White House](#), the goals for the NSTIC are as follows:

1. Design the Identity Ecosystem
2. Build the Identity Ecosystem infrastructure
3. Strengthen privacy protections for end users and increase awareness of risks
4. Manage the Identity Ecosystem

## **4. Is the Identity Ecosystem established yet? Will U.S. citizens be required to get an online identity credential?**

The Identity Ecosystem is not yet established. The government won't require that U.S. citizens get an online credential; it will be entirely voluntary.

## **5. Who is defining the NSTIC Identity Ecosystem?**

NIST is currently leading the effort to facilitate private sector involvement in defining and establishing the Identity Ecosystem. The Identity Ecosystem will be created and run primarily by the private sector. According to the NSTIC web site: "The role of the federal government is to facilitate and help jump start the private sector's efforts by convening workshops and bringing together the many different stakeholders important for establishing the Identity Ecosystem. The government will also protect individuals by ensuring that the Identity Ecosystem meets these four guiding principles: (1) privacy-enhancing and voluntary, (2) secure and resilient, (3) interoperable, and (4) cost-effective and easy to use. Lastly, the government can help drive the market by accepting Identity Ecosystem credentials for its online services."

## **6. What is the Smart Card Alliance view of the NSTIC?**

The Smart Card Alliance [endorses NSTIC](#). In a comment on the NSTIC, the Alliance said:

"The NSTIC Framework is well conceived and written. It is intentionally broad in scope, providing a wide range of trusted identity constructs and identity protection technologies. The Framework is very

pragmatic and practical in its approach, because it limits its role to being an enabler, facilitator and accelerator of the Identity Ecosystem development. There is a clear recognition that many different public and private stakeholders will be involved in working out the specifics of the framework and ultimately, using it.”

### **7. Does the NSTIC specify using smart card technology within the Identity Ecosystem?**

The NSTIC Framework identifies smart card technology as one example of an identity medium — a card, USB token or other device storing identity credentials used to validate online identities and transactions — and one that is suitable for high-value transactions and identities.

### **8. How would smart card technology contribute to the Identity Ecosystem?**

For high assurance online identity transactions (for example, for a mortgage application or health record access), using [smart card technology](#) for an identity credential will protect identities in cyberspace in a secure, privacy-sensitive way.

### **9. How easy or hard would it be to implement smart card technology as part of the Identity Ecosystem?**

The U.S. federal government has extensive experience using smart card technology in identity applications. As a result, there is already an established set of best practices, standards and technology solutions for smart card-based identity management and authentication. This foundation for protecting identities in cyberspace can easily be adapted to fulfill NSTIC's goals.

For a guide to how smart card technology protects online identities and transactions, see the Smart Card Alliance slideshow, "[Smart Card Technology and the National Cybersecurity Strategy](#).”

### **10. Where can I find additional information on NSTIC?**

The [NIST NSTIC web site](#) has a wealth of information on NSTIC, including the [full NSTIC Strategy Document](#), NIST notices of inquiry seeking industry comment, webcasts/videos and frequently-asked questions.

Smart Card Alliance resources focused on NSTIC include:

- "[Smart Card Technology and the National Cybersecurity Strategy](#)" slide show
- [Smart Card Alliance Comments on NSTIC Governance](#), submitted to NIST on July 21, 2011

### **About the Smart Card Alliance**

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.