

## Does the work related to the I3P project directly counter identity theft?

Yes, I3P researchers are developing technologies that reduce the likelihood identity thieves can access digital identity information, thereby obtaining the keys that unlock sensitive personal, financial and health-related information

## What makes the I3P Safeguarding Digital Identity project especially challenging?

Digital identity management is rife with complexity. Not only must a vast amount of data be safely collected, transmitted, stored and shared, but the data must be handled in ways that preserve privacy expectations and adhere to fair information practices.

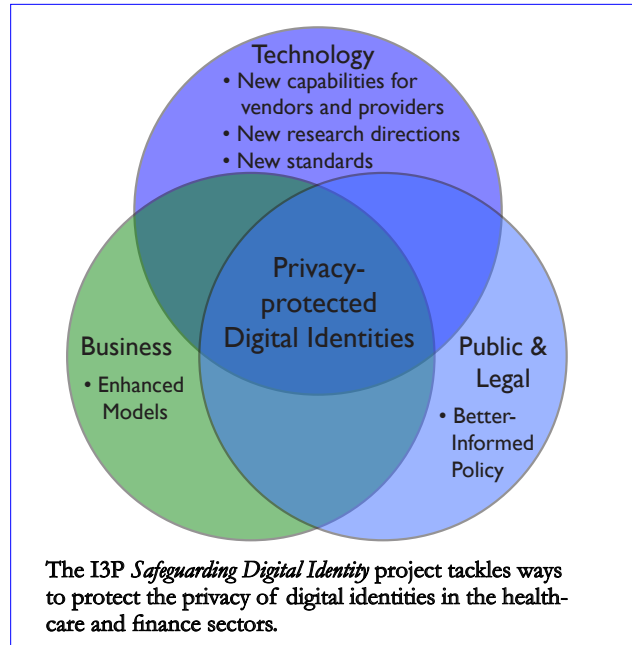
In addition, ease of use must be balanced against security needs; interoperability must be assured within large enterprises; solutions must be developed within a legal, social and political context that satisfies different cultural and regulatory regimes; and trust must be established among the people and organizations that share identity information.

## About the I3P Safeguarding Digital Identity project

The I3P digital identity management team has embraced an ambitious mission: to research, analyze and develop prototype solutions that allow organizations to securely and efficiently share identity-related information, without any loss of accuracy or privacy. More than 25 researchers from Cornell, Georgia Tech, MITRE, Purdue, SRI International and the University of Illinois are collaborating on increasing the security of digital identities.



Bruce Bakis, Team Leader



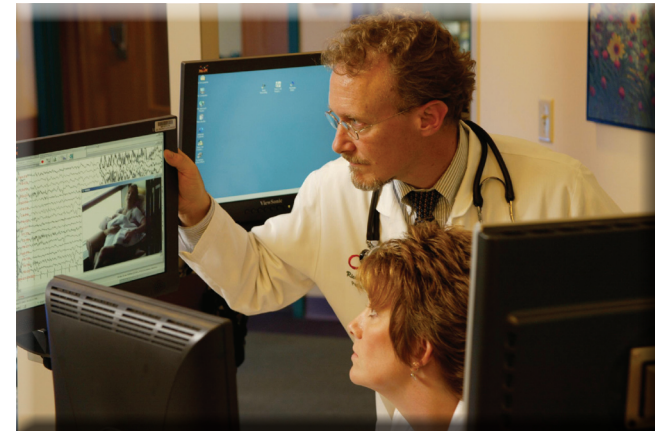
## What is the I3P?

The Institute for Information Infrastructure Protection (I3P) is a 27-member consortium of universities, federally funded labs and research institutions, managed by Dartmouth College. In addition to guiding and supporting research, the I3P is committed to finding solutions to infrastructure vulnerabilities, facilitating technology transfer and forging collaborative alliances with key stakeholders.

## Information and Contact

Information about the Safeguarding Digital Identity project can be found at the I3P's Website at: [www.thei3p.org](http://www.thei3p.org) or by contacting  
Bruce J. Bakis, MITRE Principal Investigator, at [bbakis@mitre.org](mailto:bbakis@mitre.org)  
or  
Charles C. Palmer, I3P Director for Research, at [charles.c.palmer@dartmouth.edu](mailto:charles.c.palmer@dartmouth.edu)

# Safeguarding Digital Identities



## Identity Theft: Frequently Asked Questions

## The Link Between Digital Identity Management and Identity Theft: Frequently Asked Questions

Reports of identity theft and data loss are increasingly common, a trend that reflects both the growth of digital information and the rising number of online vulnerabilities. The impact of these security breaches is profound, burdening individuals and organizations in numerous ways and triggering general unease about the integrity of digital transactions.



The Institute for Information Protection's (I3P)'s Safeguarding Digital Identity project lays the groundwork for reducing identity theft by making digital identities, which are the sentinels of sensitive personal information, less vulnerable to exploitation

### What is identity theft?

Identity theft—the fraudulent use of an individual's personal information to obtain money, goods, services or data—falls into several categories, including financial identity theft, as in the theft of credit card numbers; medical identity theft, which involves tampering with patients' medical records; and social identity theft, which can damage a person's reputation.

### What is digital identity management?

Digital identity management encompasses the administration and design of information that positively identifies a person, thereby authorizing them for digital transactions. Many websites, for example, ask for a user name and password combination in order to access the site or conduct a transaction such as modifying data or making an online purchase.

### How does digital identity management protect against identity theft?

Digital identity management, when effectively executed, reduces the risk that an identity has been fraudulently created or usurped, and thus can dramatically reduce rates of identity theft.

Specifically, identity management solutions set standards of good practice in the areas of identification, authentication (the process by which individuals are recognized prior to being authorized to seek funds, goods, services or information online) and identity protection.

### Why does digital identity management matter?

The amount of identity information collected and shared by organizations is growing, necessitating standards that ensure the privacy, confidentiality and interoperability of identities. When personal information is digitized (on the magnetic strip of a credit card, for example, or in the database of a large retailer, or a healthcare provider), it becomes easier to share – and to steal. And unfortunately, once a person's digital identity is compromised, other digital information associated with that person's identity becomes vulnerable to unauthorized use, disclosure, modification, destruction, or theft.

A security breach targeting an organization that manages large volumes of digital identities could affect millions of individuals. The consequences for an individual may range from identity theft to financial loss; consequences for the identity providers and their partner organizations may include both financial and legal penalties.

### Is digital identity management more critical in some sectors than in others?

Yes, depending on the sensitivity of the information. Government agencies, especially those that provide healthcare services through e-Health initiatives, as well as other healthcare and financial services, are especially concerned with identity management.

Adding to the need for better identity management is the trend toward the formation of partnerships or federations specifically to share information, thus reducing service costs. Regional Health Information Organizations (RHIOs) are just one example from the healthcare sector. Identity management solutions in these environments, with their large numbers of users and heterogeneous legacy systems, are badly needed.

### Should I be concerned about the vulnerability of my digital identity?

Yes, assuming you have—like millions of others—created one or more digital identities based on convenience rather than security. People who devise user names and passwords based on such publicly available information as, say, their initials or phone numbers, run the risk that an identity thief could eventually guess that information. As soon as the keys to the kingdom reach criminal hands, a person's assets are compromised.

### What can I do to better manage and protect my online identity(ies)?

The strength of your digital identity should mirror the sensitivity of information and criticality of services you wish to use. If you engage in online banking, for example, you should adopt the strongest digital identity and identity assurance mechanisms your bank offers. At a minimum you should base your name and password on a complex composition of letters, numbers and special characters, in addition, you should have one-time passcodes sent to your mobile phone to authorize especially sensitive transactions; you should also use identification tokens and smart cards if your bank offers them.

