What is identity management?

Identity Management is a system to manage and define a network user's access to specific information. This is achieved through the authentication of user, allowing different access levels and restrictions to a specific user based upon settings controlled by an administrator. The identity is verified by having the correct information to gain access to the system.

What is a smart card?

Smart card technology incorporates a micro controller, or chip, that stores information in a secure and privacy enhancing way using electronic functionality and encryption capabilities. Smart cards can take many different form factors including polycarbonate or plastic cards, similar in size to credit cards; ID tokens such as key fobs or dongles; or sim-cards used in mobile devices and cable set-top boxes.

What are smart cards used for today?

Smart cards are used in many industries around the world today, including mobile communication, financial services, healthcare, ID credentials, and travel documents.

Today smart cards are used to allow the distribution of mobile TV without the fear of piracy. Smart cards provide necessary security to mobile communication divices. Smart card technology can transforming mobile phones into contactless devices for touch-and-go applications: transport ticketing, payment, loyalty and other innovative services like smart poster, peer-to-peer or access control. Smart cards are used for contactless payments. Such payments provice speed and convience for low value items, such as fast food, movie tickets, and vending machines. Additionally, smart cards allow for more secure online banking due to the user authentication they require. Smart cards in the healthcare industry have many benefits. They enable security to prevent medical identity theft and fraud and the deployment of an eHealthcare IT system streamlines the prescription process, improves the quality of care given and simplifies electronic healthcare records management through a coordinated health service process. Smart Cards are currently used in E-passports and passport cards, providing a more secure passport or passport card. By using technology our borders are stronger and our nation is safer.

What security capabilities do smart cards support?

Smart cards have advanced electronic technological features that make them more secure than other types of identity solutions. First, the card can verify the reader is authentic in addition to

the reader verifying the authenticity of the card before a transaction takes place. Second, the data on the card is encrypted to prevent the data from being compromised. Third, smart cards support biometric identification measures allowing multi-factor authentication. Finally smart cards can utilize personal firewalls to secure sensitive data and ensures only those authorized have access to the data.

How do smart cards help to protect privacy?

Smart cards protect privacy by encrypting the information they contain both at rest and in transit. They support personal identification numbers and biometrics to authenticate users. Additionally, because smart cards incorporate advance hardware and software, they are extremely difficult to counterfeit, fraud or forge.

Why are smart cards better than other ID token technologies?

Smart cards are more technologically advanced than other ID token technologies. Smart cards store sensitive personal information on the card itself, as opposed to on a server. Since the information is encrypted and never leaves the card, it is almost impossible to compromise. Smart cards can also offer three factors of authentication. The individual needs to physically have the card, know a password or pin number, and match a biometric identification. As this illustrates smart cards have superior capabilities to authenticate users and protect sensitive information.

What is a contactless smart card?

Embedded into the smart card is an antenna that enables communication with the reader without physical contact. It works by holding the card or token near the reader usually about three inches away. After an electronic hand-shake both the card and the reader agree they can trust each other and exchange information. This process provides a very high level of security.

Is contactless smart card technology the same as RFID technology?

No, contactless smart cards are a very different technology from RFID tags. Both are wireless, meaning they can communicate using radio like a cell phone, but contactless smart cards are far more advanced and secure. Contactless smart cards have small but sophisticated computers inside them. They deliver the highest levels of computer security to protect your identity, privacy or financial information. Contactless smart card technology is suitable for uses such as identity credentials, passports and payment cards.

RFID (Radio Frequency IDentification) tags and labels are used mostly in manufacturing, shipping and object-related tracking. They have minimal built-in support for security and privacy. Retailers, such as Wal-Mart and others, have been working to use RFID tags to replace bar codes on store-bought items to scan purchases and track inventory. Another important difference is how far away someone can read the cards or tags. Contactless smart card technology has a very limited read range of four inches or less to prevent tracking or eavesdropping. RFID tags can be read from much further away, at distances up to thirty feet. RFID feature lets you find items in a warehouse or identify railcars in transit.

What is contactless payment?

Contactless payment allows the cardholder to hold their card within three inches of the payment reader at an enabled checkout register, gas pump or vending machine. At the point of sale payment is sent wirelessly and securely to the register and the transaction is processed. Cardholders don’t swipe or insert credit or debit card into a reader; making the transaction faster and more convenient. Many retailers accept contactless payment including Dairy Queen, Walgreen's, McDonalds, CVS and Arby's.