How are we doing? *Did we answer your questions?* Thinking about smart cards but need more information? *Click here to send feedback to HID's Smart Card team.*

Authentication - A technique to confirm the identity of a card or a computer system.
Biometrics - The technique of studying physical characteristics of a person such as finger prints, hand geometry, eye structure or voice pattern.
CA - Certificate Authority - A third party that verifies user identity through a series of requirements, resulting in the issuance of a digital certificate. CAs have degrees of classes of assurance they offer, based on the due diligence performed to verify an individuals identity.

Certification - The process by which a trusted third part attests to the authenticity of a user's identity.

Cryptography - The science of keeping information secure.

DES - Data Encryption Standard - The name of the Federal Information Processing Standard (FIPS), which describes the data encryption algorithm (DEA). DES and DEA are interchangeable. The DEA has a 64-bit block size and uses a 56-bit key during execution (8 parity bits a re stripped off from the full 64-bit key. The DEA is a symmetric cryptosystem. When used for communication, both sender and receiver must know the same secret key, which can be used in encrypt or decrypt the message, or to generate and verify a message authentication code (MAC). The DEA can also be used for single user encryption; such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public key cryptography provides an ideal solution to this problem.

Triple DES (3 DES) - The same as DES except that the input data is, in effect, encrypted three times using three keys. This mode of encryption is sometimes referred to as DES-EDE. There are 3 keying options defined in ANSI X9.52 for DES-EDE: (i) The three keys k1, k2, and k3 are independent, (ii) k1 and k2 are independent, but k1=k3, or (iii) k1=k2=k3.

Digital Signature - A technique for proving that a message has not been tampered with, using public key cryptography.

Directory - In public key cryptography, a look-up table of user names and public keys based on standards such as X.509 or SPKI.

ECC - Elliptic Curve Cryptosystem - A public key cryptosystem based on the properties of elliptic curves.

EEPROM - Electrically erasable programmable read only memory.

Electronic Purse (e-purse) - A small portable device which contains electronic money. It is sometimes called the electronic wallet or the stored value card (SVC)

GSM - Global System of Mobile Communications - A pan-European standard for portable phones.

Integrity - The ability to determine that the data received is the same as the data sent.

ISO (International Standards Organization) - The ISO 7816 defines the physical, electrical, and protocol characteristics of smart cards.

Key - A parameter used in conjunction with a cryptographic algorithm that determines: (i) The transformation of plaintext (unencrypted text) data into ciphertext (encrypted text) data, (ii) The transformation of ciphertext data into plaintext data, (iii) A digital signature, or (iv) A message authentication code.

Non-repudiation - The condition whereby the sender of a message cannot deny the validity of the result of the process used to authenticate the data.

Operating System - Software designed to control the hardware of a specific data-processing system in order to allow users and application programs to employ it easily.

Personalization - Modify a smart card to represent information concerning one person. There are two sorts of personalization: graphical and electrical. Graphical personalization modifies the visual aspect of the card (holder's name, photograph) electrical personalization modifies the information held in electronic form.

PIN - Personal Identification Number - The number or code that a cardholder must type in to confirm that they are the genuine owner of the card.

PK Certificate - A document which is digitally signed by a Certification Authority, based on an identity-proofing done by a Registration Authority, containing the individual's public key, some form of the individual's identity, and a finite validity period.

PKI - Public Key Infrastructure - The integrated set of technologies required to provide public-key encryption and digital signature services.

Private Key - The key of a public key pair that is known only to an individual user.

Public Key - The key of a public key pair that is only published widely.

Public Key Cryptography - Encrypting information by using two different mathematically related keys for encrypting and decrypting. I encrypt a message with my private key and you decrypt it with my public key, which you've looked up on a directory server or I've given you. If you want to send me a message you encrypt it with my public key and I unlock it with my private key.

ROM - Read only memory (mask ROM).

RSA - An early public key algorithm developed by Rivest, Shamir and Adelman. It is an ISO standard.

Token - Security industry jargon for hardware or physical objects used for securing data or identity. Unlike software security solutions, smart cards are a "hardware token".

Transport Keys - A string of numbers used to lock the smart card during its travel from the manufacturer to the customer.