

GLOSSARY OF TERMS

125 kHz: Radio waves operating at 125 thousand cycles per second. This technology has historically been the standard in proximity card/reader but is beginning to be replaced by faster, more secure 13.56 MHz technology.

13.56 MHz: Radio waves operating at 13.56 million cycles per second allowing read/write and secure, encrypted card and reader communication. Because of the faster communication (compared to 125 kHz proximity technology) between a card and reader, this technology is better suited for biometrics and secure, authenticated transactions.

Anticollision: The process built into an RFID system that protects multiple cards from crashing into each other (being read at the same time) within a reader's field.

Application Field: Areas like pages in a smart card that house different uses or applications (such as access control, cashless vending, public transportation, etc.) and are protected by security keys.

ASK: Amplitude Shift Keying or modulation – Refers to the process of altering the height of the radio waves to signify the zeros and ones in the binary communication
– ASK is the most common form of modulation used in RFID. It is used in both ISO 14443 and ISO 15693 specifications for reader to card communication.

Badge ID: The unique identifier for each card/credential within an access control system (similar to a license plate number).

Biometrics: The biological identification of a person, including characteristics of structure and of action such as iris and retinal patterns, hand geometry, fingerprints, voice responses to challenges and the dynamics of hand-written

signatures. Biometrics are a more secure form of authentication than using cards or typing passwords, however, some forms have relatively high failure rates. Biometric authentication is often a secondary mechanism in two-factor authentication.

Bits/Bytes: A binary system of information or data represented by the number 1 or 0. This binary system of communication, called digital communication, is how computers or microprocessors talk to each other. The smallest piece (represented by a 1 or 0) of information is called a bit. A packet or string of 8 bits = 1 byte.

CE Mark: European certification that products meet RF interference standards (see also FCC certification).

Contactless: A card/credential and reader system utilizing RFID technology in which the credential and reader utilize microprocessors and antennas to communicate without having to come in contact with one another. This technology is usually associated with 13.56 MHz read/write capabilities that make this technology superior to standard 125 kHz proximity technology in implementing security authentication, biometrics, and smart cards.

DESFire: A flexible, high security, ISO 14443 compliant, contactless smart card technology by Philips Electronics. DESFire was chosen by the U.S. Government to become the basis for their contactless card and reader interoperability standards.

EEPROM: Electrically Erasable Programmable ROM - A rewritable memory chip that holds its content without power.

Encryption: The reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format as a mechanism for

protecting its confidentiality, integrity and sometimes its authenticity. Encryption uses an encryption algorithm and one or more encryption keys.

Ethernet: The most popular communication system for LANs.

F2F: Two-way communication system/protocol between the host and the reader typically used in a CASI (GE Security) access control system.

FCC Certification: U.S. certification indicating that a product meets FCC standards regarding RF signal interference.

Firmware: Essentially software in the form of ROM or EEPROM that does not lose memory when power is not maintained.

Format: How a card is encoded with information. A format dictates how a number is used and what it means. An access control panel is programmed to recognize the order of information in a bit stream, such as parity bits, badge number, and facility codes.

Frequency: The measure of the number of radio wave cycles completed in a period of time.

FSK: Frequency Shift Keying or modulation – the process of altering the frequency of radio waves to signify the zeros and ones in the binary communication.

Hash Function: Blending or mixing information in the encryption process to ensure security in the RFID during transmission.

IP address: A series of four numbers ranging between 1 and 256 each separated by a decimal – essentially a computer street address identifying a particular computer from others during communication over the web.

ISO 14443: International standard regulating contactless, proximity technology, typically representing a read range distance up to 10 centimeters. The advantage products utilizing ISO 14443 have over those utilizing ISO 15693 is that the transaction speed is faster, making

security and transaction speed superior for large packets of information such as biometric templates. ISO 14443 is actually divided into two sub-divisions of the standard, A & B. Without going into great detail, 14443A has grown to be the leading standard for access control and transportation and 14443B for banking.

ISO 15693: International standard regulating contactless, vicinity technology, typically representing a distance over 10 centimeters. The advantage ISO 15693 has over ISO 14443 is greater convenience due to longer read ranges and less power consumption.

Keyfob: A keyfob is a unique credential serving purposes similar to a card. It can take many shapes and is often used as the fob or extension on a key chain. Keyfobs can be used for access control, smart card applications, etc.

Key Management: Much like the key control of masterkeyed codes in a mechanical key system, key management in an electronic system is the process of controlling badge IDs, facility codes, and ensuring the security and integrity of extensions in a system to avoid distributing duplicate codes.

LANs: Local Area Networks are typically used to connect computers separated by short distances.

MIFARE®: A proprietary contactless and dual interface smart card chip technology produced by Philips. Mifare is a well proven RF communication technology for transmitting data between a card and a reader device and is fully compliant with ISO 14443A.

Modulation: The changing of radio waves in a specific manner in order to represent data.

Mullion: A vertical bar or divider in the frame between doors or other openings such as the metal narrow rail between glass storefront doors.

Multi-Technology Cards: A card or credential utilizing two or more technologies such as magnetic stripe and proximity (RF).

Multi-Technology Readers: A reader utilizing two or more technologies such as proximity (125 kHz) and contactless (13.56 MHz).

NFC: Near Field Communication is a wireless communication system developed in conjunction between Philips and Sony to compete with Bluetooth wireless communication.

OEM: Original Equipment Manufacturer – A manufacturing company of a data control system such as an access control system that provides software to connect many devices, including readers.

PKI: Public Key Infrastructure – A framework for creating a secure method for exchanging information using cryptography and a 3rd party certificate authority to authenticate individuals and organizations.

Protocol: How computers talk to each other – a communication system.

Proximity: A card/credential and reader system utilizing RFID technology in which the credential and reader utilize microprocessors and antennas to communicate without having to come in contact with one another. This technology is usually associated with 125 kHz frequency readers, the historical standard RFID technology in access control.

RS232 or RS485: Standards for serial multipoint communications lines. These standards represent faster, two-way communication lines rather than the standard Wiegand one-way communication lines prevalent in the access control industry.

Smart Card: A card or credential that contains a built-in microprocessor and memory used for identification and transactions in a number of applications (security, financial, etc.). The card has read/write capability to transfer data from a reader typically to a panel or computer.

TCP/IP: Transmission Control Protocol/Internet Protocol is the most common protocol system

computers use to communicate over the internet.

UID: Unique Identifier – The unique number given to a card/credential making it different from any other card/credential – like a VIN# of a car.

UL Listed: Underwriters Laboratory". Originally an insurance industry organization, UL is now an independent and non-profit organization that tests electrical components and other equipment for potential hazards. When something is UL-listed, it means that UL has tested the device and it meets their requirements for safety - ie: fire or shock hazard.

VPN: A Virtual Private Network is configured within a public or internet network to take advantage of economies of scale.

WANs: Wide Area Networks connect computers separated by large distances.

Wiegand Cards: An access control card which, in principle, works much like a magnetic-stripe card. A Wiegand card contains a set of embedded wires that contain data and are made of a special alloy with magnetic properties that are extremely difficult to duplicate.

Wiegand Format: The most common data format in an access control system consisting of 26 bits of information (also see format definition).