Electronic Access Control Glossary

- **Access card**: A small plastic card that stores a user’s cardholder ID information used to gain access to a physical space or network resources (cards can be magnetic stripe, proximity or smart).

- **Access control**: The process of controlling who can access an area and when, using something they have (an access card), something they know (a PIN), and/or something they are (biometrics) to enforce security policy and controls.

- **Access control panel (or ‘Controller’)**: A connection point between a reader or integrated lock and the access control software, often where the credential data is validated and an access decision is made; an intelligent (typically networked) field controller that stores and enforces the access control rules for attached devices (readers, locks, elevators, gates, etc.).

- **Access control system**: The collection of components that are used to manage access for a facility or campus, typically consisting of access control software, controllers or access control panels, readers and/or locks.

- **Aperio**: Aperio® technology is a global wireless platform from ASSA ABLOY, based on the IEEE 802.15.4 standard. Aperio utilizes local wireless communication between the lock and a communications hub to connect to an electronic access control system.

- **Authentication/dual authentication**: The process of verifying the identity of a user. Dual authentication provides an additional layer of security by requiring a second method of verification (such as card + PIN).

- **Biometrics**: The use of unique biological characteristics, such as a fingerprint or iris, to manage access.

- **Credential**: Something that is used to validate a user’s identity to grant access to a physical space or network resources. It can be something the user has (i.e., card, fob, or phone); something the user knows (i.e., PIN codes or combinations); and/or something the user is (i.e., biometrics such as fingerprints).

- **Data-on-Card**: Uses a smart card to securely manage the movement of access rights and audit history through a credential-based network.

- **Door position switch (DPS)**: A switch used to monitor whether a door is in an open or closed position.

- **Integrated lock**: Integrated locks combine several discrete access control components – card reader, lock, door position switch, request to exit sensor, access control panel, and power supply – into a single unit.

- **Intelligent lock**: An intelligent lock stores a local database of valid access credentials and is able to make decisions locally. An intelligent lock may also store a local record of events.

- **Keypad**: A set of buttons with numbers, letters or symbols used to manage access with a PIN (personal identification number) or pass code.

- **Lockdown**: An emergency protocol that will lock some or all of the doors in a building or campus, either to protect occupants from an external threat or to prevent people from entering or exiting certain areas of the building.

- **Magnetic stripe card**: An access card with a band of magnetic material that must be inserted into a magnetic stripe reader in order to gain access or complete a transaction. Often used for credit and debit cards, magnetic stripe technology is less secure than today’s credential technologies.
• **Mobile access:** The use of a mobile device, such as a smartphone, tablet or wearable, to gain access to secured doors, gates, networks, services and more.

• **Offline lock:** A lock that is not connected to the access control system and must be updated manually.

• **Online lock:** A lock that is constantly connected to the access control system (typically through an access control panel).

• **OSDP:** Open Supervised Device Protocol is the latest Access Control industry standard for hard-wired reader communications. OSDP is an RS-485, bi-directional protocol that can both support encryption and higher data speeds than its predecessor (Wiegand) as well as longer distances (4000 ft.).

• **Power over Ethernet:** A technology that uses standard LAN infrastructure to deliver power to network devices over the same cable used for network data connection.

• **Proximity card:** Low frequency, low security 125 kHz contactless RFID cards (legacy technology); often referred to as Prox cards.

• **Reader:** Either wall mounted or integrated into a lock, a reader reads the data from a card or credential and transmits that data to the controller.

• **Request to Exit (REX):** A signal that notifies the system to release the door so that someone can exit, as well as to bypass the DPS so that it does not register a forced open alarm for a valid exit.

• **Scheduling:** The ability to lock or unlock doors automatically at pre-determined times, or to restrict cardholder access to specific time periods.

• **Seos®:** The next generation of smart credential technology from ASSA ABLOY Group brand HID Global. Seos provides the highest level of security through best-in-class data and privacy protection; form factor flexibility that allows the use of mobile devices, smart cards, tags, and more; and the ability to address applications beyond physical access control.

• **Smart card:** High frequency, 13.56 MHz contactless / contact cards (current standard) that provide a higher level of security than proximity cards by using a more secure method of authentication.

• **Wiegand:** A mono-directional, unencrypted communication protocol widely accepted as an industry standard in access control equipment. Wiegand data is typically the protocol used between the reader and the host panel (limited to 500 ft.).

• **WiFi access control:** WiFi access control allows a facility to leverage its existing WiFi (IEEE 802.11) network infrastructure to connect to the access control system. WiFi locks are intelligent edge devices that are offline most of the time, “coming to life” briefly when a credential is presented, to announce user specified alarm conditions, and at regular intervals to update access rights and transmit audit trails. They do not require panels, hubs or gateways.

• **Wireless access control:** Access control devices that connect wirelessly to access control software. These devices may use proprietary or open wireless standards, and may connect to an intermediary wireless gateway or hub.