Prelude to 3millID Mobile Credentials and Readers Training

Mobile Readers - 3millID offers a family of 3 readers capable of reading standard proximity cards, secure envelope MIFARE DESFire EV1/EV2 smart cards and 3millID Mobile Bluetooth Credentials. Readers are installed like most other proximity access readers and can be wired via terminal strip connector as Wiegand output or state of the art OSDP connectivity (as long as there are OSDP compliant access panels). The readers utilize proven Bluetooth (BTLE) technology and can be connected to virtually any Wiegand output access control system. This means any access system can be upgraded to utilize Mobile Credentials regardless of the head end access software. For those systems that want to utilize existing Wiegand output readers (proximity or otherwise) that are already installed, 3millID offers a 4th Mobile reader named the Inline Reader which can be installed "inline" between the existing reader and access panel, in the general vicinity of the door (Ceiling, behind secure side of door, etc). This essentially converts that door opening into a Mobile Access door, while still using the   existing installed reader and physical credentials along with the new mobile credentials. Virtually all Wiegand output access control readers/systems installed over the past twenty years are candidates to be upgraded to Mobile Credentials.

Using the Badging Portal - The 3millID Mobile Credential functionality is enabled by the 3millID cloud or "Badging Portal". This cloud based software provides the functionality for populating 3millID Readers and Mobile Credentials for a specific Owner (End User) account and for assigning a Reseller(Integrator/Installer) to the particular Owner. From the Badging Portal, Mobile Credentials may be issued in virtual "Boxes" of Credentials. Credentials may also be returned to a "Box" and then re-issued. Credentials are paid annually, in advance.

Submitting Orders for Mobile Credentials - When a 3millID Mobile Certified   Reseller works with an Owner that desires Mobile Credentials and Readers, the Certified   Reseller submits a Purchase Order (following the Mobile Credential Order Guide) and payment to cramZ marketing services for Mobile Credentials. The orders are simply submitted to sales@cramzmarketing.com similar to a normal order for typical plastic Proximity Credentials. The information required for the order would include the typical items including Quantity of Credentials, format required (26 bit H10301 or otherwise), facility code, and card number range. The Reseller would also include the Owner (End User) account name and relevant information.

Issuing Mobile Credentials - cramZ marketing would then acknowledge the order and issue a Sales Order as confirmation and then populate the Mobile Credentials in the Badging Portal with the "virtual box of credentials". The Credential "boxes" are deposited into the Owner's Badging Portal account for Issuance. An Owner can then issue (auto email) Mobile Credentials to specific users or they can create an Admin account for their Authorized Reseller to issue Mobile Credentials to specific users on behalf of the Owner. Mobile Credentials may be issued, returned and re-issued an unlimited number of times.

Typically the first Credential issued is an "Install Credential" which is issued from the Owner to the Reseller (installer). This Install Credential is specifically used for "installing" or "Commissioning" Readers which causes the Readers to be matched with specific Credentials in the same Owner account. This essentially "keys" Readers and Credentials to be recognized as belonging to each other (although access is still only granted based on the Access Control System provisions). Readers that have the same Owner account code as Mobile Credentials will be "seen" by the 3millID Mobile App on users Mobile Phones.

Naming and Commissioning Readers - The Reseller (or Owner) is also typically responsible for assigning Reader "names" (Front Door, Back Door, etc) in the Badging Portal. These Readers will correspond with the respective Owner account Mobile Credentials. Readers are typically "commissioned" as mobile capable after installation. Commissioning involves the use of the 3millID toolkit software/Tablet and USB dongle connected to a Windows 10 tablet or laptop. An installer simply needs to be within 2 to 3 feet of the reader with the Toolkit software/dongle to commission the Reader via Bluetooth link.

Using Mobile Credentials and the Mobile App - When an Owner issues a Mobile Credential they simply select a box of virtual Mobile Credentials, type the person's name and email, along with the selected Badge ID (either next in line or specific number from the range available in the box) and click "Issue". After the Credential has been issued, usually within a few minutes, an email is received by the intended recipient. This email notfies the recipient that they have just received a Mobile Credential and provides instructions for downloading the 3millID Mobile App and activatng the Mobile Credential. Only one Mobile Credential can be installed on a given mobile phone.

At this point, so long as the Mobile Credential ID has been activated in the access control system, this user now has a valid Mobile Credential and access to specified gates/doors, as determined by the access control system. The user can then drive/walk to a Mobile Reader access point, open their 3millID Mobile app and select the gate/door by pressing the named icon. If there are multiple readers in range of the user (typically within 20 to 30') the 3millID Mobile app will generally see and list the 3 closest gate/door names. Again, the user simply selects which door they wish to access and select that specific door name icon. As a user walks/ drives through a facility with multiple Mobile gates/doors, the names appearing in the app will come and go as they are within range and then fall out of range. Operating range can easily be reduced via the Reader commissioning process or within the app itself.

The phone literally becomes the Proximity card. Administration costs for mailing badges are eliminated with a simple email and lost or forgotten badge issues are eliminated as most users cling to their phones more than their wallets. Security is typically enhanced as most users have phone passwords meaning their credential now has two factor authenticaton (Password and possession of the Credential). The system is great for traditional access systems, gate access and parking where the longer read range is beneficial.