ScanPass®
MOBILE CREDENTIAL

WHITEPAPER: The Art of ScanPass® Mobile Credentials

There are many mobile credential technologies on the market. Almost all are based upon either near field communications, NFC, or some form of Bluetooth. ScanPass differs from those technologies as it only requires optical scanning via the smartphone/tablet. In this whitepaper it will be illustrated how ScanPass Mobile Credentials are the easiest to use, easiest to install, most secure, and most economical solution in the industry.

Easiest to Use

Some mobile credentialing systems, and traditional access cards for that matter, require something to be provided or received physically by the user to enroll the credential into the access system. An administrator using a ScanPass system needs to only enter the user's name into the Connect ONE cloud-hosted management system with their required permissions and Connect ONE will automatically email the user their login information and instructions on how to download the App for ScanPass. No physical exchange of anything or any information is required.

When the user logs into the Connect ONE App, their unique credential will be securely sent to the Connect ONE cloud which will propagate down to the necessary access systems onsite of which the user has permission. At this point the user can approach an access door, press the ScanPass icon on their phone/tablet, optically the barcode on the door is identified, then the user's credential and door identifier is encrypted and sent to the access system. The transmission of this message may be sent directly via the building WIFI network and/or relayed through the Connect ONE cloud to the access system, depending on the configuration. In either case, the access system onsite will make the decision to grant or deny the user's access based upon their privileges. If granted, the user's phone will turn green and the door will unlock. If denied, the user's phone will turn red and display a message indicating why they were denied, such as an invalid area or invalid time accessing the door. This additional feedback directly to the user is unique in the industry. All of this happens in typically less than one second.

To remove or alter someone's access, they simply edit, deactivate, or delete the credential in the Connect ONE system, this propagates to all access systems the user had access. The administrator still does not need the phone/tablet and if the user attempts to use it they will simply be denied.

Barcodes may also be applied to keypads for arming/disarming functions, which also give the necessary armed/disarmed feedback to the user on their phone/tablet. Barcodes can also be used for checkpoint tours and many other functions too.

Easiest to Install

All other mobile credential systems require a reader to be installed at the access door. ScanPass only requires a barcode to be placed on the door and therefore the only wiring necessary is power to the electronic lock. This could also be simplified with installing a local power supply at the door and a wireless relay connected back to the access system onsite to trigger the lock upon requested. A wireless transmitter may be installed to monitor the power supply for ac power failures or low battery.

The barcode may be placed on the inside glass or the outside of the door and can also be further protected by clear plexiglass and tamper-resistant screws.

Most Secure

Since ScanPass is the only solution without readers, this is a major security benefit. Most even high-grade readers still send the wiegand protocol back to the access system. These readers can easily be tampered with and compromised for someone to connect to the wiring on the back of the reader and essentially scan in many cards at once using a PC. This can be limited since most access systems employ a lockout period after so many unsuccessful attempts but since this can be done on the unprotected side of the door and many times outside of the intrusion protection, someone would have plenty of time to be at work. There are also devices on the market which may be tapped onto the reader wires for a short time which will detect and store valid card reads. Then all someone needs to do is comeback with their smart phone and replay those same reads. There is a new technology on the market called OSDP, this is set to replace the wiegand standard but it is not fully adopted and it only improves this situation when encryption is enabled, which is not currently the standard. Another backend reader technology may use Ethernet rather than traditional wiegand or OSDP. Here again, someone tampering with the reader can easily connect to the Ethernet line on the reader and now they have point-of-access into the network. A competent installation would segment the security network from the customer's business network but still at the very least the attacker now has access to the security network to do as they wish and again outside of the intrusion protection, so they have all the time they need.

Many other mobile technologies simply "move" the standard 26-bit wiegand identifier from the card to the phone. It is still theoretically possible for this identified to be re-used. ScanPass uses a unique 64-bit (Android) or 128-bit (iOS) credential which can never be duplicated.

ScanPass also ensures replay protection is enforced by a unique registration mechanism which must remain in-sync with the access system onsite. If someone were to sniff the data sent from the phone over-the-air it would not be possible to simply resend the same encrypted data to achieve access, as resending the same data would break the registration sequence. Only the authenticated user's phone/tablet has the necessary registration to send another request.

All access decisions are always made onsite by the access system, even during the method of which the access request is relayed via the Connect ONE cloud. The cloud itself makes no determination of privilege; the access system onsite always makes the decision. This allows for another security benefit as the user does not need to remain logged into Connect ONE for ScanPass to operate. The user's phone/tablet can continue to request access to systems it last knew about and the access system onsite will make the decision. If the user's credential was revoked from the access system, the user will be denied since the access system knows about this already.

ScanPass may be used with a configurable setting of how to allow access requests to be sent to the access system onsite. They can be restricted to WIFI only, meaning the user must first be connected to the WIFI network prior to being able to request access. They may also be firewalled to an approved whitelist of IP addresses which adds another element of protection.

Most Economical

As already stated, ScanPass is the only mobile credentialing system on the market without readers, this is a cost savings in itself but there is more. Since there are no readers, there are also no door controllers. All equipment needed is: a barcode sticker, lock power, and a simple relay output control on the access system.   The users' phone/tablet takes care of the rest of being the credential and barcode reader in the same device. Using only simple relays, many doors can be handled on the same access system for a very low cost.

It can also be stated that since ScanPass does not require NFC or Bluetooth enabled on the phone/tablet, but simply requires a camera, the phone/tablet can be inexpensive and will not drain the battery as much as if in the case of the other technologies needed to be always-on. The phone/tablet does not require cellular service so it may not have any monthly fee associated with it.

ScanPass mobile credentials typically cost far less as well. Most other mobile credentials are purchased in blocks which can only be used one-time and for one system. If the user gets a new phone/tablet then they will need to purchase a new credential. ScanPass credentials are sold in blocks but if the user needs to be issued a new credential the old one can be replaced with a new one without a fee. Also, the same credential may be used for an unlimited number of systems. The only time more than one ScanPass credential is necessary for a given individual is when that same individual has multiple devices, such as more than one phone or a phone plus a tablet.