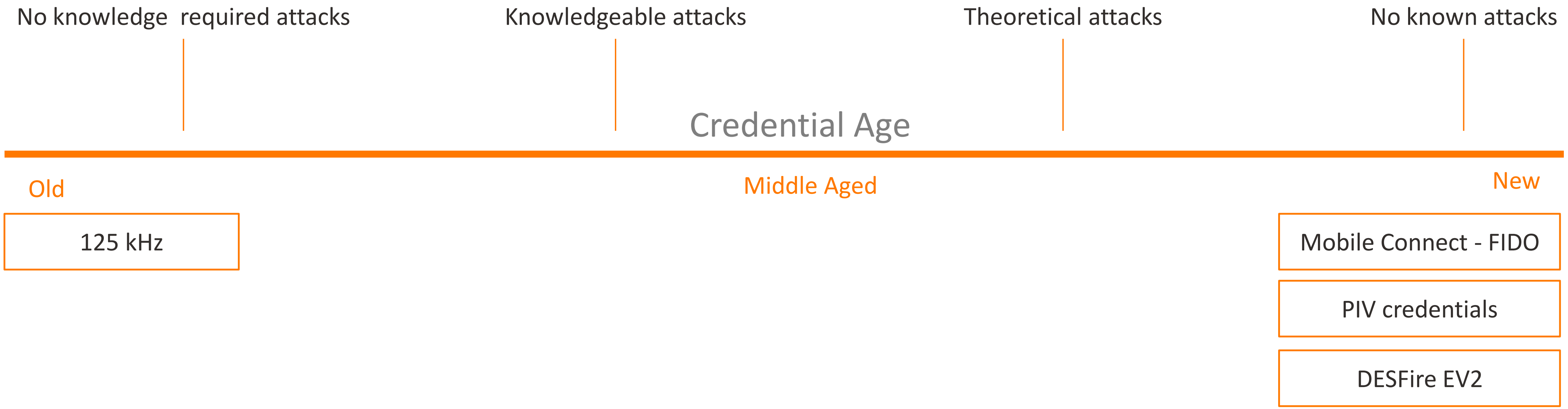
Cyber security

HOW CYBER-SECURE IS YOUR SECURITY SYSTEM?

Cyber security standards

- ISO 27001 and 27002
- NIST Cybersecurity Framework
- Payment Card Industry Data Security Standard (PCI)
- FIPS 201 (US Government)
- CSA STAR

Credential Threat Lifecycle



No knowledge required attacks

Knowledgeable attacks

Theoretical attacks

No known attacks

Credential Age

Old

Middle Aged

New

125 kHz

Mobile Connect - FIDO

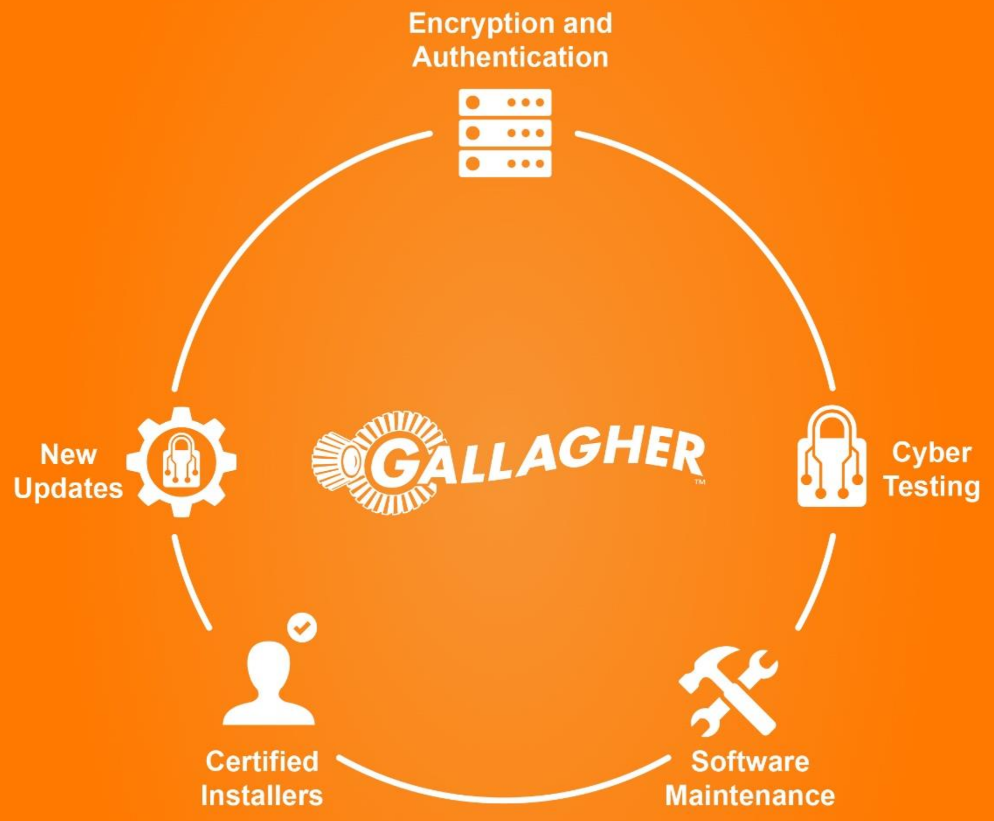
PIV credentials

DESFire EV2

The Gallagher solution

Gallagher's unparalleled cyber security protection delivers:

- End-to-end encryption (encrypted SQL database)
- End-to-end authentication
- Internal and external penetration testing (dedicated cyber team)
- System hardening and configuration advice
- Fully trained and certified installers
- FIDO authentication for mobile
- Six monthly software releases (Software Maintenance)
- Cyber security 'baked' into our software development process
- Updates can be implemented easily and applied centrally to the whole system
- A responsible disclosure policy if/when a vulnerability is found.



Cyber security baked in

Cyber security is ‘baked in’ to our software development process.

- Extremely difficult to re-engineer security back into a product once released –the sticky plaster approach does not work.
- We design for high security and enterprise security needs from day one.
- High security threats can become mainstream ones over time.

Dedicated Cyber Security Personnel:

- Information Security Manager
- Certified Internal Penetration Tester
- Security Advisory Group
- Upskilling ALL development staff

Extensive cyber testing

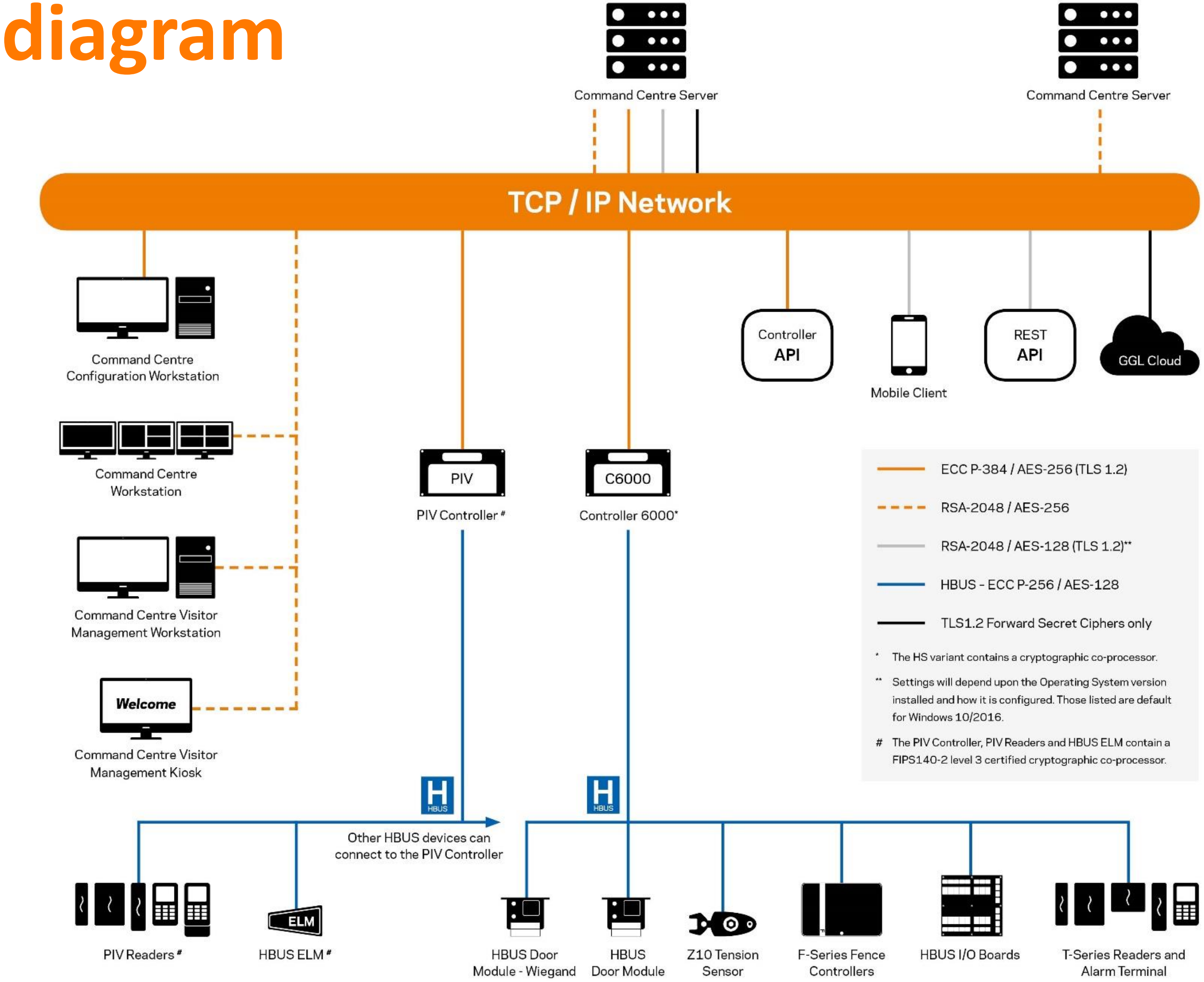
Independent 3rd party penetration testing and security reviews.

Recommended configuration settings and installation practices to ensure a highly secure Gallagher system for Command Centre, Controller, VM Kiosk, and Mobile Client.

Automated testing:

- Dedicated automated testing team
- Automated test scripts for all new software
- Virtual hardware – Enterprise size stress testing
- 1,000’s of automated tests run every night

Encryption diagram


Command Centre Server
Command Centre Server
TCP / IP Network
Command Centre Configuration Workstation
Command Centre Workstation
Command Centre Visitor Management Workstation
Welcome
Command Centre Visitor Management Kiosk
PIV
PIV Controller #
C6000
Controller 6000*
Controller API
Mobile Client
REST API
GGL Cloud
H HBUS
H HBUS
Other HBUS devices can connect to the PIV Controller
PIV Readers #
ELM
HBUS ELM #
HBUS Door Module - Wiegand
HBUS Door Module
Z10 Tension Sensor
F-Series Fence Controllers
HBUS I/O Boards
T-Series Readers and Alarm Terminal

— ECC P-384 / AES-256 (TLS 1.2)

- - - RSA-2048 / AES-256

— RSA-2048 / AES-128 (TLS 1.2)**

— HBUS - ECC P-256 / AES-128

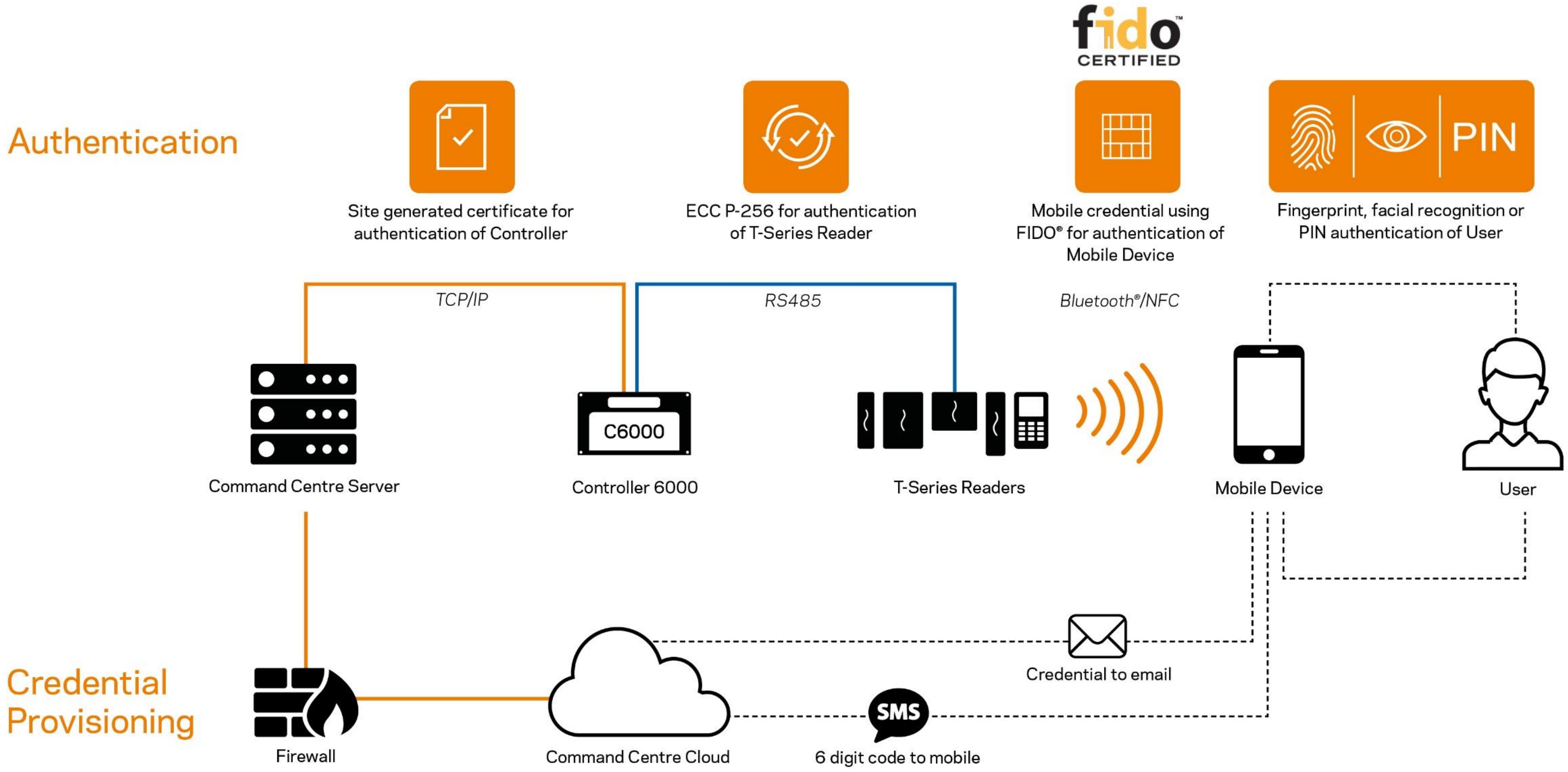
— TLS1.2 Forward Secret Ciphers only

* The HS variant contains a cryptographic co-processor.

** Settings will depend upon the Operating System version installed and how it is configured. Those listed are default for Windows 10/2016.

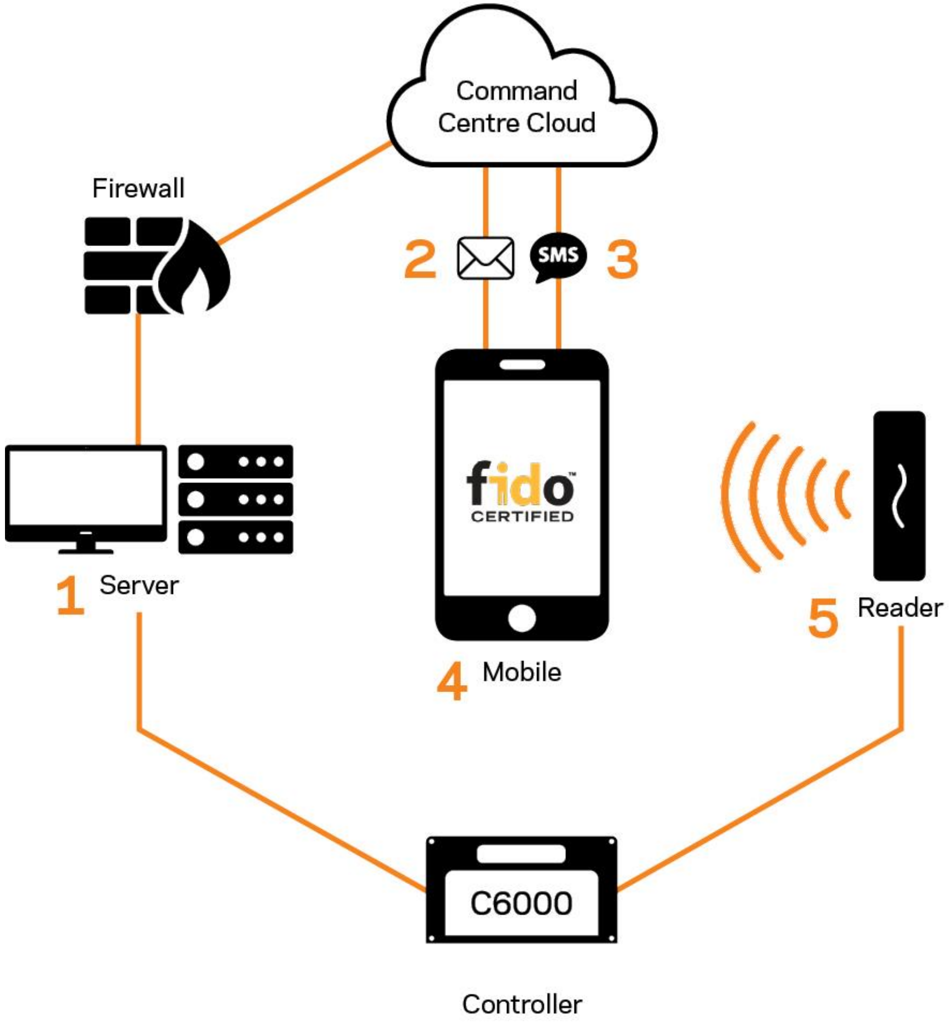
The PIV Controller, PIV Readers and HBUS ELM contain a FIPS140-2 level 3 certified cryptographic co-processor.

Authentication diagram



fido CERTIFIED
Authentication
Site generated certificate for authentication of Controller
ECC P-256 for authentication of T-Series Reader
Mobile credential using FIDO® for authentication of Mobile Device
PIN
Fingerprint, facial recognition or PIN authentication of User
TCP/IP
RS485
Bluetooth®/NFC
C6000
Command Centre Server
Controller 6000
T-Series Readers
Mobile Device
User
Credential Provisioning
Firewall
Command Centre Cloud
Credential to email
SMS
6 digit code to mobile

Mobile credential provisioning diagram



1 An operator registers a mobile credential to a cardholder in Command Centre. When registered, a request is sent from Command Centre to the Cloud. Command Centre sends the user's email address, phone number, invitation expiry time, and mobile credential identifier.

2 The Cloud sends an invitation email to the user's email address. This email contains a link to the Mobile Connect App. The user must download and install the app. The email also contains an 'Accept Credential' button.

3 The Cloud then sends an SMS containing a six digit confirmation code to the user's phone number. The user must enter the six digit confirmation code to the user's phone number. The user must enter the six digit code into the app in order to authorise their device.

4 The user must specify their second authentication factor, either PIN or fingerprint. If the door requires a second authentication factor, this must be entered using the device, not the keypad on a reader.

5 The user can now request access at a Gallagher reader.

Note: The credential identified is stored on the Controller. Internet connectivity is not required for a user to request access at a Gallagher reader.

High security standards

High security standards Gallagher manufactures to are:

- Type A (New Zealand)
- Type 1A (Australia)
- FIPS 201 (USA)
- CPNI standards (UK)

Even if you don't need to meet these standards, your system benefits from the expertise and in-depth knowledge of the Gallagher team behind your security solution.