Gallagher Command Centre

Mobile Connect Cloud and App - Security

Technical Information Paper

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Important: If you received this document along with your Command Centre installation media, or via another similar channel then it may be out of date with respect to the functionality/behaviour of the cloud, and of the Mobile Connect Apps, which are distributed through platform App Stores and may be more recent than your Command Centre installation.

It is recommend you refer to the latest revision of this document, which can be found here:
https://gallaghersecurity.github.io/r/mobileconnect-cloud-and-app-security

Contents

1 Background

The Gallagher Mobile Connect app for iOS and Android lets people use their mobile devices instead of, or in addition to a traditional MIFARE or similar access card.

The app has two primary features

- Using the Bluetooth® Low Energy features of mobile devices to exchange data with Bluetooth® equipped Gallagher T-Series readers (Also NFC on supported Android Devices), which in turn talk to Gallagher 6000 series controllers over HBUS to establish an access decision, and grant or deny someone access to a Command Centre system.
- Receiving broadcast notification messages via in-app Push Notifications

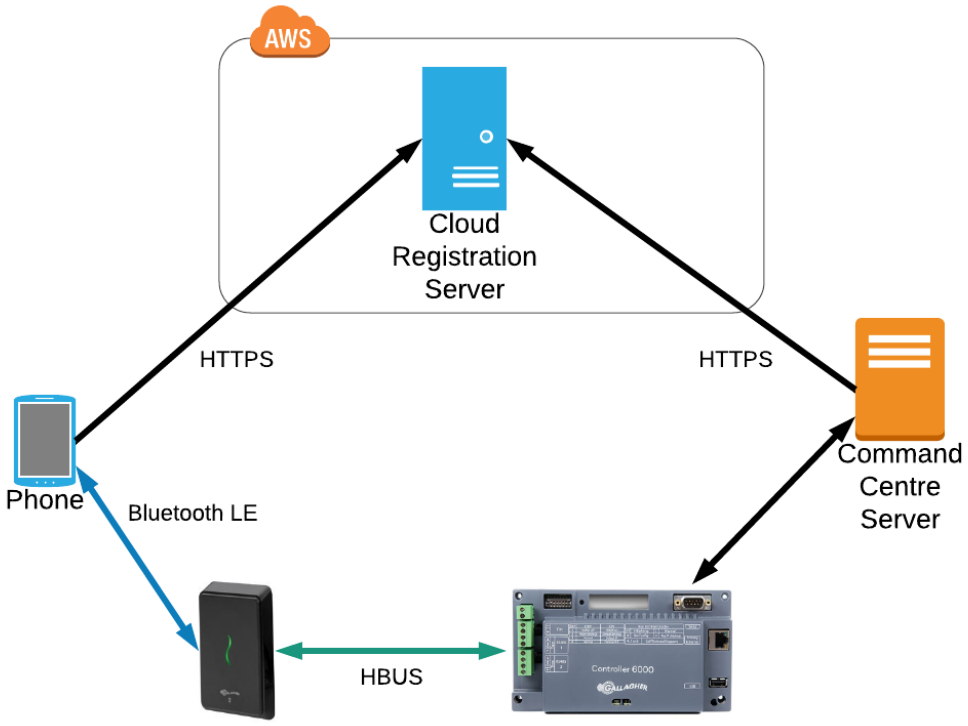
1.1 Target Audience for the Mobile Connect App

The target end user for the Mobile Connect application is anyone who might have an Access Card, including "partially-trusted" individuals such as students, contract employees, etc.

Phones are likely to be a mix of corporate and personally owned devices. Personally owned devices will probably not be monitored or controlled, and are unlikely to have access to corporate WiFi, VPN's or other secure networks.

2 Mobile Credentials

2.1 Mobile Access Overview



In order to identify a phone, Command Centre needs to exchange some information with it before any access attempts can be made using Bluetooth.

To exchange this data, there must be some way of conveying data between the phone and the Command Centre server. As phones only have WiFi or Cellular connections, a traditional approach would require the Command Centre server to be exposed to a WiFi or cellular network where the phones could communicate with it.

Allowing personal devices (whose only network connection is likely to be a generic cellular internet connection) to be used effectively means that the server would have to accept requests from the internet at large.

Anything which provides network services to personal mobile devices must be considered an attack target that will be exposed to a wide variety of potentially hostile behavior.

If a Command Centre site wishes to allow registration of devices that are not on a secure company network, it will not be possible to rely on network or endpoint level security to protect the Command Centre server.

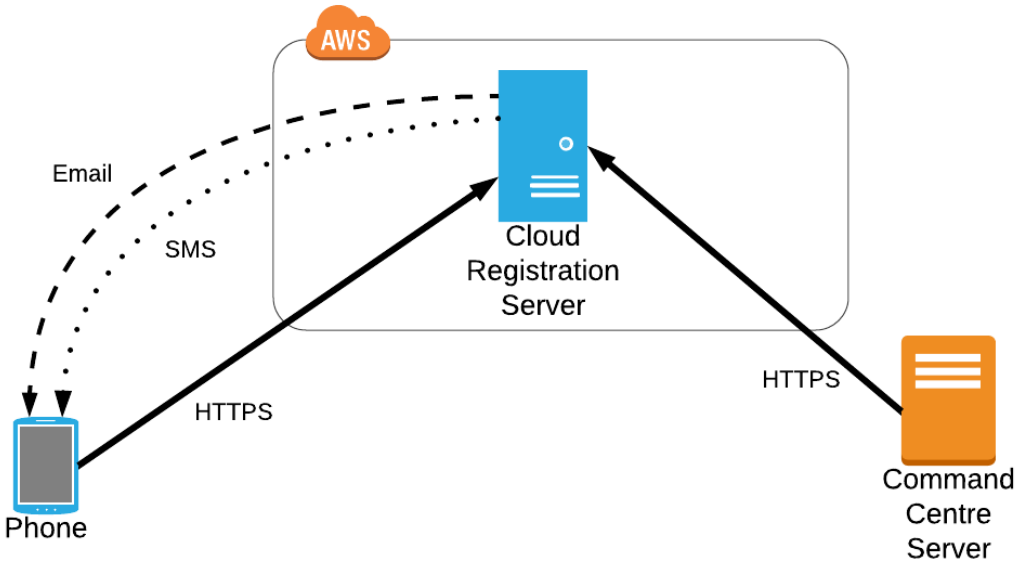
Why use the cloud for Mobile Credential Registration?

It would not be responsible to require customers to expose Command Centre servers to network traffic from such a wide variety of potentially malicious sources. As such, most IT departments are not willing to allow this kind of network traffic through company firewalls.

This means we must implement a relay of sorts, to shield the Command Centre server from direct attack. A hypothetical relay or proxy service that customers could host in their internal networks would help mitigate security risks, but it would still require Mobile Connect users to be granted access to a corporate WiFi network or VPN which would be inconvenient.

The Gallagher Cloud registration server solves the security problem and has the additional benefit that end users can register using whatever data connection they already have – from anywhere at any time.

2.2 Mobile Credential Registration Process



1. A Command Centre operator adds a Mobile Credential to a Cardholder.
2. The Command Centre server connects to the cloud registration server and sends through the minimum information needed to complete the registration.
3. The cloud sends an Email to the cardholder which contains a unique one-time-use registration code.
4. The user responds to the email, launching the Mobile Connect app. The app connects to the cloud and acknowledges the registration code.
5. The cloud sends an SMS message to the cardholder which contains a one-time-use 6 digit confirmation code.
6. The user inputs this 6 digit code into the Mobile Connect app. The app connects to the cloud and acknowledges the confirmation code.
7. The app on the phone proceeds with registering the FIDO credential, and sends the credential information to the cloud when complete.
8. The Command Centre server fetches this complete FIDO credential from the cloud, after which point it can make it available to controllers and it can be used for access.

2.3 Mobile Credential Registration Technical Details

Registration emails by default use a standard template; It is possible to customize this template, but this must be configured outside of your Command Centre software. For more information please contact your Gallagher representative.

Registration emails are sent with a from address of: **no-reply@security.gallagher.cloud**.
This is not configurable.

If you employ a spam filter, you may need to configure it to allow messages from this address. Spam filters may also validate against the **smtp.mailfrom** header either in place of or in addition to the **from** header. Registration emails will have an smtp.mailfrom value of **<random id>@mailsender.security.gallagher.cloud**, so you may need to allow ***@mailsender.security.gallagher.cloud**.
E.g. smtp.mailfrom=01000171e6fd47ea-2cd6a766-3cf2-47dd-b207-189f0d368bf0-000000@mailsender.security.gallagher.cloud

Data sent from Command Centre to the Gallagher Cloud Services during registration consists of:

- The registration code (to uniquely identify the registration)
- The cardholder's email address (to send them the registration email message)
- The cardholder's mobile phone number (to send them the SMS confirmation code)
- Policy information such as how long the registration code should be valid before expiring

The registration code consists of cryptographically strong random data.

It expires after 7 days (by default) if not used. This expiry period is configurable individually for each site.

An SMS confirmation code expires 1 hour after being issued.

If a user enters the SMS confirmation code incorrectly more than 5 times, the invitation will be cancelled.

If the SMS confirmation code is not correctly entered within the hour, it will be reset and a second, then third confirmation code will be sent if the user re-tries the registration process.

If the user attempts to retry after the third SMS message has been sent-but-not-completed, the invitation will be cancelled.

Note: Technical details related to the cloud are subject to change. It is recommend you refer to the latest revision of this document, which can be found here:
https://gallaghersecurity.github.io/r/mobileconnect-cloud-and-app-security

2.4 Mobile Credential Invalidation Scenarios

There are several scenarios where a user can invalidate their credential by changing settings on their device. This only affects access where two-factor authentication is required by the reader.

- Android Mobile Connect: when a user is enrolled using a fingerprint for two-factor authentication and an additional fingerprint is added to the device.
- iOS Mobile Connect: when a user removes their device passcode off after enrollment.

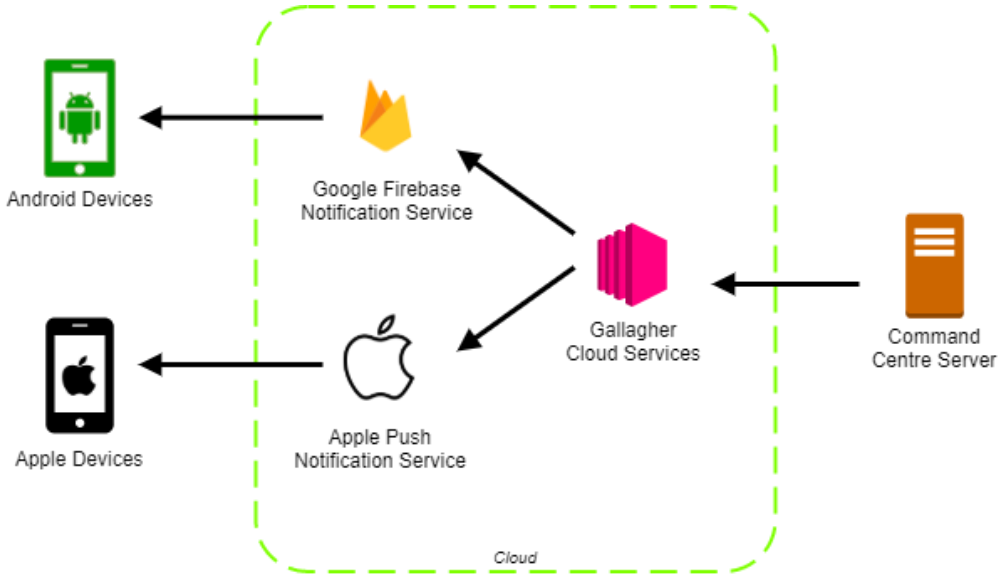
Both these scenarios require re-enrollment of the Mobile Credential.

There are also two rare scenarios in iOS Mobile Connect on Face ID capable phones, where credentials can be invalidated by revoking permission to use Face ID.

- When a user selects Face ID as their authentication method, then denies permission to the app when prompted during enrollment.
- When a user enrolls with Face ID, then disables permission to the app in the phone's settings.

When a credential is broken in this way, the app must be reinstalled before a new credential can be enrolled.

3 Broadcast Push Notifications



Android and iOS require that broadcast push notifications are sent via the respective cloud platforms controlled by Google and Apple.

Why send broadcast messages via the Gallagher Cloud?

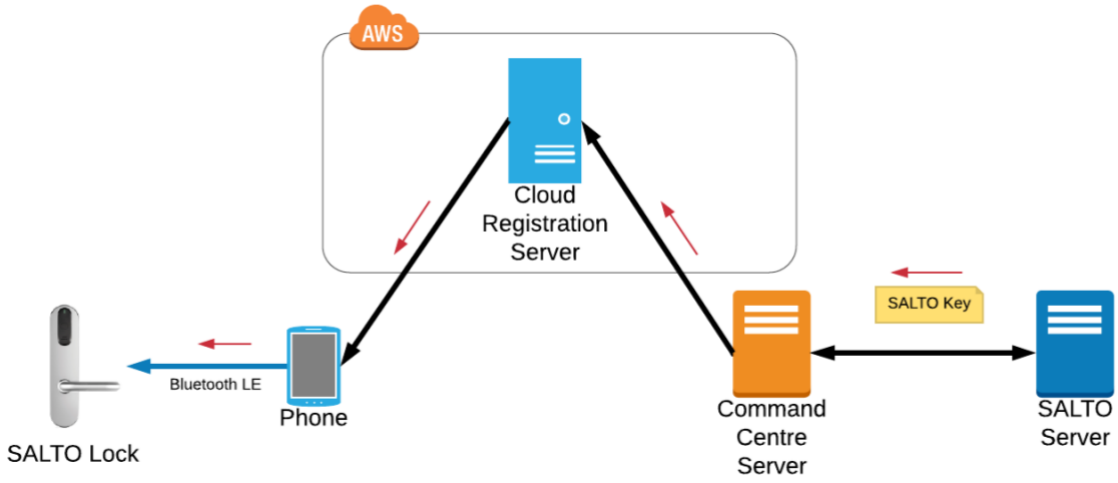
Command Centre servers could communicate directly with Google and Apple, but in practice this would have major drawbacks

- Google/Apple push notification services require security keys and a development account for their respective platforms. It would be a significant burden to require each individual Command Centre customer to create and manage these things
- Google/Apple cloud services have a huge range of dynamic IP addresses, which makes controlling outbound access through corporate firewalls very difficult.
- Mobile push notifications are not guaranteed to be reliable. If (for example) multiple messages are sent while a phone is powered off, Google/Apple reserve the right to drop some messages and only send the most recent one. By sending messages through the Gallagher cloud, we can ensure that no data is lost.

3.1 Broadcast Notification Process

1. Command Centre sends broadcast notifications to the target cardholders
2. Command Centre queues these messages internally, and delivers them to the Gallagher Cloud as quickly as it is able (determined by the network)
3. The Gallagher Cloud delivers the messages to Google Firebase, which delivers them to Android devices, or forwards them to Apple for delivery to iOS devices
4. The user receives a notification on their phone containing a summary of the message
5. When the user opens the notification, they will be taken to the Notification List screen in mobile connect.
6. Mobile Connect will use the user's FIDO credential to securely authenticate to the Gallagher Cloud, and then download the full message details, along with any other messages that may have been delivered but that Google/Apple have dropped. Dropped messages are rare, and generally only occur if the user has had their device powered off for a long period of time, or has manually disabled notifications using their system settings.

4 SALTO Mobile Access integration



If your site has SALTO Bluetooth-capable wired or wireless locks, and you have integrated your SALTO server with Command Centre, then you can use the Gallagher Mobile Connect App to open Bluetooth-capable SALTO doors. This requires Command Centre version 8.10 or newer.

In order to communicate with SALTO hardware, the Gallagher Mobile Connect App incorporates SALTO's JustIN Mobile SDK. The JustIN Mobile SDK handles Bluetooth communication with SALTO locks, but it does not account for delivery and maintenance of SALTO access keys used to open those locks.

Mobile Connect solves this by attaching the SALTO key to Gallagher's existing Mobile Credential. We use the Mobile Credential to securely deliver the SALTO key to the correct phone. As such, Gallagher Mobile Credentials are a pre-requisite for using SALTO BLE locks with the Mobile Connect app.

If you do not have any SALTO integration, this part of Command Centre and the Mobile Connect App is deactivated

Licensing Note: While no additional license is required by Command Centre, SALTO may require an additional Salto BLE site license in addition to the purchase of Salto BLE hardware.

Security Note: SALTO keys are less secure than FIDO-based Gallagher Mobile Credentials.
It is also not possible to use SALTO locks in PINs or Two-factor mode.
It is recommended that you use Mobile/FIDO credentials for security-sensitive areas.

4.1 SALTO key issuing and delivery

When your SALTO access changes, the following occurs:

1. Command Centre asks the SALTO server to encode a new key, containing your new access
2. Command Centre associates the new key with your mobile credential, and sends it to Gallagher Cloud Services
3. Gallagher Cloud Services store the key (in encrypted form) until the Mobile Connect app on your phone connects and retrieves the new key
   Note: If the key is not retrieved within 7 days, it will be deleted from the cloud.
4. Gallagher Cloud Services will send a "background" push notification to your phone.
5. When your phone receives this push notification, the Mobile Connect app launches invisibly in the background. It will retrieve the new SALTO key from the cloud, and store it locally on your phone, attached to your Mobile Credential.

6. Google and Apple do not guarantee instant or reliable delivery of "background" notifications; so, whenever the Mobile Connect app is opened, it will also connect to the cloud and check for SALTO key changes in case a new key is available and a notification was not received for it.

   Note: While background notifications are not guaranteed, in practice we find that in almost all cases the background notification is delivered, and the phone receives the new key within 5-10 seconds after the cloud sends the push notification.

4.2 SALTO key refresh

SALTO keys (as issued by your SALTO server) are valid for up to 7 days, at which point your key must be refreshed. This is a behavior of SALTO's system and is not under the control of Gallagher.

If you are familiar with SALTO's traditional access-card based system, this is analogous to the situation where you must badge on a wired update point periodically to refresh your card.

Command Centre and Mobile Connect transparently manages this refresh process for you. Six days (possibly earlier, see below) after issuing a SALTO key, Command Centre will ask the SALTO server for a refreshed key, and silently send this through the cloud and to the target mobile phone(s)

If, for some reason the refreshed key cannot be delivered to the phone (for example if the phone has no internet connection) then, after the key has expired, the Mobile Connect App will show a warning in the user interface and ask you to connect your phone to the internet to receive a refreshed key.

4.3 SALTO key revocation

If you make a change in Command Centre to remove SALTO access from a cardholder (for example you remove all their SALTO access groups), Command Centre will send a message via the cloud to the target phone(s) to instruct them to immediately delete their SALTO keys.

4.4 SALTO encoding performance management

If you make a large number of SALTO access changes at once - for example, you assign 5,000 cardholders to a SALTO access group that they did not previously have - this will cause Command Centre to immediately ask the SALTO server for 5,000 new keys so that they can be sent to the cloud and delivered to phones.

This may cause the SALTO server to be busy while it encodes all these new keys. Command Centre does not attempt to delay or spread this load *when you make an access change* as the priority is making sure the cardholders have their correct access as soon as possible

SALTO key refresh, however, is a background process and may not be expected. To reduce the performance impact on the SALTO server, when Command Centre is doing key refresh, it will deliberately spread out the refresh process, such that the key refreshes for those 5,000 cardholders do not all occur at the same time.

To spread out the load, Command Centre will deliberately refresh some credentials earlier than strictly required. It spreads them out across the entire 6-day period so some credentials may get refreshed after 1 or 2 days. Because the refresh process is transparent to the user, so this should not affect access or performance for any individual user.
Command Centre will never delay the refresh of a credential past the 6-day point as that could affect the user's access.

5 Gallagher Cloud Services Technical Details

Currently, there is a single (logical) endpoint, located in Sydney, Australia.
Internally we employ multiple redundant servers for failover and scalability.

It has the DNS address **commandcentre-ap-southeast-2.security.gallagher.cloud**

It has two static IP addresses: **52.62.211.7** and **54.79.91.203**

Communications with cloud services take place solely using HTTPS over the standard port **443**

Gallagher cloud services use TLS client certificates to securely and uniquely identify each individual Command Centre server. The client certificates are issued by the cloud to each Command Centre server the first time it connects.

Note: The same Gallagher Cloud Services also provide Mobile Push Notifications functionality for the Command Centre Mobile Application. For more information, please refer to the document titled **"Gallagher Command Centre Mobile App – Security Technical Information Paper"**

5.1 Firewall Recommendations

Configure your firewall to allow TCP outbound traffic on port 443 with a source of your internal Command Centre server, and destination of the above DNS or IP addresses. If you are configuring firewall rules based on IP address, please allow **both** static IP addresses.

You do not need to allow any inbound traffic to your Command Centre server.

6 Data Storage and Retention

6.1 Mobile Devices

The Mobile Connect app stores the following data locally on the phone:

1. Mobile Credential Display/Diagnostic Information:
   - The name of the site a cardholder has registered against
   - The date they registered.
   - The authentication method they selected for second factor

   This information is not encrypted at rest. Mobile operating systems provide sandboxing which prevents other applications and most casual attackers from reading it.
   Note: The displayed site name is configurable. It can be altered or left blank if a site does not wish this information to be shown or saved.
2. Secure Mobile Credential Information, which consists of the FIDO credential information and private keys.
   This information is stored by NokNok labs' FIDO certified authenticator components. It is stored using hardware secure storage and encryption on devices which support this, or otherwise the best available encryption and storage option for a given device.
3. Received Broadcast notification messages.
   - The notification message text
   - The date and time the notification was received
   - The name of the site which sent the notification.

   This information is not encrypted at rest. Mobile operating systems provide sandboxing which prevents other applications and most casual attackers from reading it.
   Note: The displayed site name is configurable. It can be altered or left blank if a site does not wish this information to be shown or saved.
4. SALTO Key data If configured

Data is retained on the mobile device until the cardholder deletes it.

To delete mobile credential data, a cardholder can use the Settings screen in the app to delete a credential for a specific site, or they can uninstall the entire app.

To delete broadcast notification messages, a cardholder can delete the messages by swiping them on the notifications list screen within the app, or they can uninstall the entire app.
Note: Deleting a mobile credential does not delete the broadcast notification messages that were received while the credential was active. The cardholder may delete these manually.

Note: Technical details related to the Mobile Connect Apps are subject to change. It is recommend you refer to the latest revision of this document, which can be found here:
https://gallaghersecurity.github.io/r/mobileconnect-cloud-and-app-security

6.2 Cloud Services

Gallagher Cloud Services encrypt Broadcast Notification contents, and SALTO keys at rest. Other data is not encrypted at rest.

The credential information pertaining to registrations is secure without needing encryption due to FIDO's use of public key cryptography (refer to the FIDO section for more information on this.)

For each Command Centre server that connects to the cloud, the cloud retains the following:

- Server serial number (note the server name is NOT retained)
- Server licensing information
- A TLS client certificate used to authenticate connections from that server.
- Information about any in-progress or successful mobile device registrations, consisting of:
  - Random credential identifier UUIDs
  - FIDO Public Key(s)
  - *Note: Expired or failed mobile device registration information is deleted after the configurable expiry period*
  - *Note: registered mobile credential data is retained until it is requested to be deleted by either the Mobile Connect app, or the Command Centre server. It needs to be stored to enable broadcast notifications to work securely.*
- Any un-downloaded broadcast notification messages or SALTO keys for any valid mobile credentials associated with the Command Centre site.
  The Mobile Connect app downloads notification messages and SALTO keys every time it is launched, and once downloaded they are removed from the cloud. If the Mobile Connect app is never launched, they will be purged from the cloud after 7 days.
- Command Centre also periodically sends a count of active mobile credentials for licensing purposes.

This information is the minimum required for the solution to function, and it is retained until you no longer wish to use the Gallagher Cloud Services.

6.2.1 Removing individual mobile credential data from Gallagher Cloud Services

When you use Command Centre to remove a mobile credential from a cardholder, the Command Centre server will queue a request to instruct the cloud to delete the credential, and anything associated with it (FIDO public keys, Broadcast Notification messages, SALTO keys).
Your Command Centre server must have an active internet connection for this delete request to be delivered to the cloud, otherwise it will be queued until an internet connection is available.

When a cardholder deletes their Mobile Credential using the settings screen in the Mobile Connect app, their phone will tell the cloud to also delete the corresponding credential and associated data. The delete function requires an internet connection.

Note: If you uninstall the Mobile Connect app, it is not given the opportunity by the mobile operating systems to contact our cloud. As such you will need to remove the credential through Command Centre if you are concerned about this.

6.2.2 Removing all information about your site from Gallagher Cloud Services

It was previously the case that deleting the Cloud FT Item from within the Command Centre configuration client would request the Gallagher Cloud services to remove all data related to the site. After July 2018, this is no longer the case – regardless of the Command Centre server version installed on a given site.

Deleting the Cloud FT Item within Command Centre will now send a message informing the Gallagher Cloud to release the license serial number (to allow for server migrations and upgrades) however all other data is retained.

Command Centre 8.00 adds a "Delete Cloud and Purge Data" feature, accessible on the "Advanced" tab of the Cloud FT Item configuration dialog. You can use this to request that all information referred to by this document about the site is removed from Gallagher Cloud Services. The purge data feature does not work if the Command Centre server does not have an active internet connection.

Important Note: If you use the purge data feature to remove the cloud connection, and then later re-establish a connection to the cloud, then any mobile credentials issued before the purge will not be known to the cloud. **This means those credentials will fail to receive broadcast notification messages and SALTO keys**. If you wish to correct this, you must re-issue those credentials.

Note for older sites: The purge data feature is available in version 8.00 or newer of the Command Centre software. If you have not or are not able to upgrade your server to version 8.00 or newer but would still like your data to be deleted from the Gallagher Cloud Services, please contact privacy@gallagher.com or by using any of the methods listed on the Gallagher website at https://www.gallagher.com/privacy

If you email, please use a subject line containing the terms "Mobile Connect Cloud Services" in order to help us process your request more quickly.

Note: Technical details related to the cloud are subject to change. It is recommend you refer to the latest revision of this document, which can be found here: https://gallaghersecurity.github.io/r/mobileconnect-cloud-and-app-security

6.2.3 Cardholder Personal Information

Cardholder email addresses are never persisted by the cloud. It receives them from Command Centre and immediately discards them after sending an email.

Cardholder mobile phone numbers are stored for the minimum amount of time to allow for registration.

- When a cardholder completes the registration process using the Mobile Connect app, the cloud immediately deletes the corresponding mobile number.
- When a registration expires, the cloud immediately deletes the corresponding mobile number.
- When a registration is cancelled, the cloud immediately deletes the corresponding mobile number.

Note: *The above is the deletion policy for the active database, however mobile numbers may be persisted in database backups for longer periods than this.*

7 Data Transmission

Data transfer between Mobile devices and Reader hardware is not encrypted as no private information is sent. Authentication is secured by FIDO.

All other data transfer between Command Centre, the Cloud and Mobile devices uses encrypted HTTPS. We support only TLS 1.2; Older protocols are disallowed which mitigates most encryption-related security risks. You can view the SSL Labs industry standard report here:

https://www.ssllabs.com/ssltest/analyze.html?d=commandcentre%2dap%2dsoutheast%2d2.security.gallagher.cloud&latest

Communication between Command Centre and the Cloud servers is authenticated using TLS client certificates (2048-bit RSA).

Communication between Mobile devices and the Gallagher Cloud is authenticated using FIDO (P256 Elliptic Curve).

8 Security Controls

8.1 Mobile Devices

Security, Access Controls and Isolation are provided by mobile operating systems and hardware.

8.2 Cloud Services

Our cloud services are securely hosted using Amazon Web Services. They are isolated from other Gallagher or external services using an AWS Virtual Private Cloud.

The cloud services themselves are not exposed directly to the internet, all traffic is routed through a dedicated Security Gateway component, which employs OWASP standard rules and techniques for mitigating attacks, as well as application-specific URL allow-listing and appropriate rate limiting.

Strict firewall and access control rules are in place protecting all Administrative functions and other endpoints.

All administrative users accessing our cloud infrastructure require two-factor authentication and strong passwords.

Services within the cloud environment are only allowed access to the minimum set of resources they require to function (e.g. they are only allowed to fetch and connect to the sole database / key storage they require, and cannot access resources for any other services).

Platform updates (for example Operating System security patches) are applied on a daily basis where required. We employ automated scanning tools which alert if any third-party software components we use are identified in a vulnerability database such as (but not limited to) the public CVE database.

9 Monitoring and Response

We employ automated analysis of both application and database logs, continuous monitoring of CPU, Disk and network resource usage and application-specific health monitoring.

Alerts are automatically generated and immediately sent to Gallagher. These alerts, along with service status, are monitored 24 hours per day.

Notice of any incidents or outages that may affect customers will be provided via our Channel Partners, or a direct email alert system, which customers may sign up to by contacting their Channel Partner.

10 Security and Penetration Testing

Gallagher employ internal security and penetration testing staff, who hold a number of security certifications.

Our internal security staff hold a key role in the development of our cloud services, providing expertise, security reviews and internal penetration testing.

An external specialist security company will be engaged to do a comprehensive review annually, or more frequently with each major release as required. Prior reviews have been conducted by Insomnia Security, and executive summaries of the findings are available by request.

We are open to customer or otherwise externally arranged penetration testing, however we require advance notice and approval from Gallagher to avoid disruption of our services which may impact other customers.

11 FIDO and public key cryptography based security

In order to provide a secure solution:

- Phones must be able to identify themselves to Controllers (via a reader)
- Controllers must be able to prove that the phone's identity is legitimate
- Controllers must be able to prove that data sent from the phone has not been tampered or misused.

11.1 FIDO

Gallagher Mobile Connect uses the FIDO UAF protocol for identification and authentication to provide security when access is attempted by a cardholder using their mobile device.

FIDO is an acronym for **F**ast **ID**entity **O**nline. It represents a set of open, interoperable and secure specifications for online authentication. It is managed by the FIDO alliance (https://fidoalliance.org/) which is an open group consisting of companies including Microsoft, Google, Intel, MasterCard, Visa and many others.

UAF is an acronym for **U**niversal **A**uthentication **F**ramework, and is a FIDO protocol designed to authenticate users to services using public key cryptography instead of traditional methods such as passwords. It aims to provide improved security and usability through support for biometric, PIN and other convenient forms of authentication.

The FIDO UAF protocol has gained wide acceptance as being secure, reliable and resistant to many forms of attack. As an open protocol, the specifications are publicly available, and as such have been scrutinised and reviewed in great detail by many parties.

11.2 Public Key Cryptography

The full details of public key cryptography are outside the scope of this document, but it can be summarised roughly as follows.

- To identify something, a pair of large numbers is generated which are mathematically linked together. These are called **keys**.
- Each of the keys can be used to encrypt, or generate a signature for a set of data, which the other key can be used to decrypt or verify.
- The mathematics is such that given one key, it is not practically possible to discover the other, so one key is safe to distribute without requiring additional encryption.
- Given this property, one key is designated as the **private key** and kept safe. The other is designated as the **public key**. Copies of the public key are sent to other parties we wish to communicate with.
- The private key can be used to generate a signature for a piece of data, which is sent along with that data. The public key can be used to verify the data. The mathematics formally prove that the data originated with the private key, and that it has not been tampered with.
- Encryption can also be performed, but this is not needed by FIDO, so does not warrant further explanation.

Public Key Cryptography is also known as asymmetric cryptography, referring to the two sides of the conversation both holding different keys.

11.3 Cryptography principles applied by Gallagher Mobile Connect

The FIDO UAF protocol applies these principles as follows:

At registration time:

- The phone generates a public and private key pair (Elliptic Curve P-256).
- The public key is sent from the phone to Command Centre, which saves it, and makes it available to controllers for later use.
  Sending the public key to the controller is the primary reason for having a registration process.

At access time:

- The phone signs some data with its private key and sends the data and the signature.
- The Controller uses the corresponding public key (which it obtained during registration) to verify the signature and the data. This securely proves that the phone is the correct one and the data is legitimate.

A number of points arise from this approach:

1. An attacker being able to clone the credential depends on their obtaining a copy of the private key. It is important to keep it safe.
2. The public key can only verify the phone, not impersonate it. As such, it is not considered sensitive information, and if it happens to get copied, intercepted or otherwise made available to malicious third parties, the credential still remains secure.
3. Only the public key needs to be transmitted. The private key can remain securely on the device. This greatly reduces the ability for any malicious third parties to intercept or gain access to it.
4. If hardware secure storage is available, the private key can be stored in this secure hardware. In these situations, the private key never leaves this secure hardware chip for any reason.
5. For an attacker to clone or compromise a credential, they must:
    a. At bare minimum have physical access to your phone
    b. Modify its operating system to circumvent the phone's built in security defenses.
    c. If hardware secure storage is used, even this will not reveal the private key. An attacker must resort to physical attack methods such as removing the secure hardware chip and physically opening it, which may destroy the chip entirely.