Gallagher Command Centre

Mobile Wallet Access Badge

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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 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.

Document History

Edition	Date	Comment
1.0	16/09/2024	Initial release

Contents

1 Background 4

2 Compatibility 4

3 Implications 4

4 Architecture 5
- 4.1 Overview 5
- 4.2 Deployment 5

5 Apple Employee Access Badge 6
- 5.1 Solution Enablement 6
- 5.2 Access Badge In-App Provisioning 6
- 5.3 Access Badge Updates 8
  - 5.3.1 State Management Updates 9
  - 5.3.2 Badge Data Updates 11
- 5.4 Access Transaction 11

6 Data Security 13
- 6.1 Data in Transit 13
- 6.2 Data at Rest 14

7 Data Storage and Retention 14
- 7.1 Command Centre (On-Prem) 14
- 7.2 Mobile Devices 14
- 7.3 Cloud Services 15

8 Security Controls 15
- 8.1 Mobile Devices 15
- 8.2 Gallagher Cloud Services 15
  - 8.2.1 Firewall Recommendations 16
  - 8.2.2 Certifications 16
  - 8.2.3 Penetration Testing 16

9 Related Resources 17

1 Background

Mobile wallets have become vital in the digital ecosystem, transforming how users interact with their devices for payments, identification, and access control. With the advent of technologies such as Near Field Communication (NFC) and secure digital tokens, mobile wallets like Apple Wallet and Google Wallet provide a seamless and secure experience for storing credit cards, loyalty programs, and access badges.

Mobile Wallet Access Badge is a featured solution allowing Command Centre's Cardholders to securely add access badges to their phone and watch wallet apps and use them to gain access to doors, elevators, turnstiles, and other facilities at their workplaces.

The Mobile Wallet solution offers the following:

- Enhances the daily Cardholder experience using the user's smartphone or smartwatch to gain access reducing the need for plastic cards.
- Utilizes the advanced security capabilities of mobile devices, including two-factor authentication (such as fingerprint or facial recognition) and encrypted communications, to ensure that only authorized users can gain access.
- User credentials can be updated in real-time by either the Cardholder or the system operator, eliminating the need for reissuing physical cards. This improves both security and operational efficiency.

2 Compatibility

Mobile Wallet Access Badge is currently supported for Apple Wallet only.

Command Centre version 9.10 MR3 or later introduces Apple Employee Badge which at minimum requires iPhone 8 running iOS 16 or later and Apple Watch Series 6 running watchOS 10 or later.
Apple Employee Badge provisioning requires Mobile Connect app version 16.04 or later or third-party apps using Mobile Connect SDK version 17.0 or later.

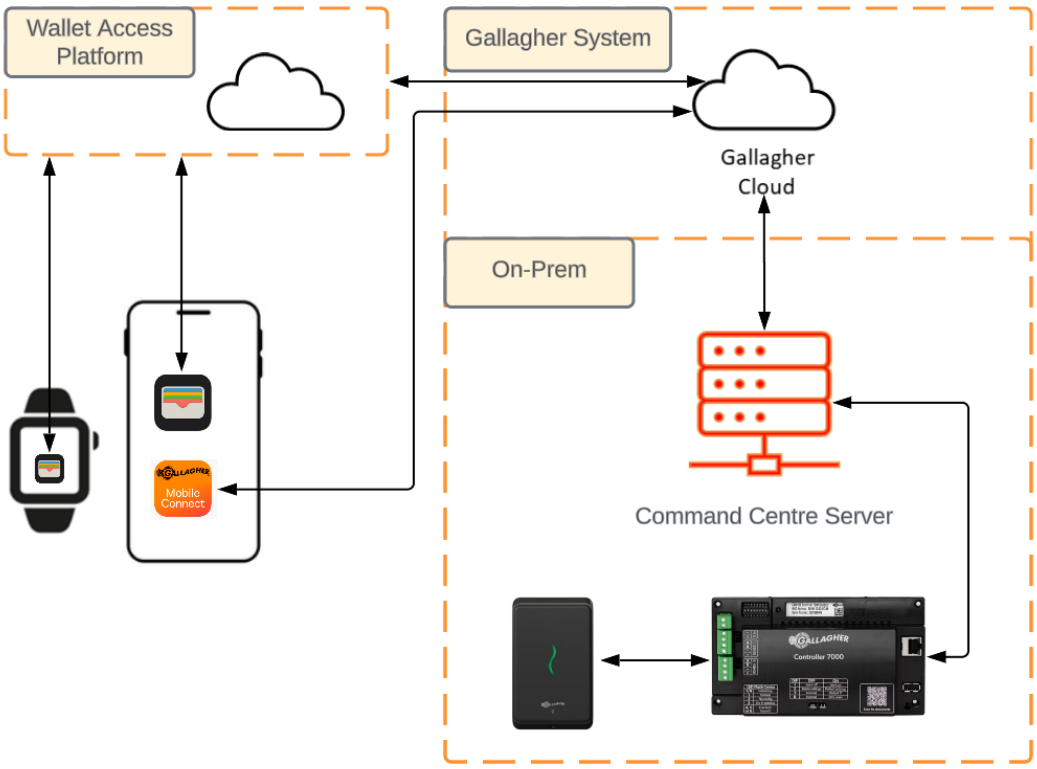
3 Implications

The Mobile Wallet Access Badge solution leverages Gallagher Cloud Services to securely store site keys, access credentials, and Cardholder information, ensuring a seamless and uninterrupted experience. Robust security measures, including encryption during transit and at rest, are implemented to protect the data. Additionally, badges and personal information are securely handled by the platform wallet provider and safeguarded by the system's secure element.

4 Architecture

4.1 Overview

The Mobile Wallet solution consists of the following main components: Command Centre server, Gallagher Cloud Services, Gallagher access hardware (controllers/readers), Smart devices, and a third-party Mobile Wallet Access platform.



4.2 Deployment

The Mobile Wallet solution is hosted in Sydney, Australia. This is the primary deployment location for the Gallagher Cloud Services. Additionally, it is deployed to Northern Virginia, US location to provide additional redundancy for availability.
Multiple redundant servers are employed internally within a region for scalability and fault tolerance.

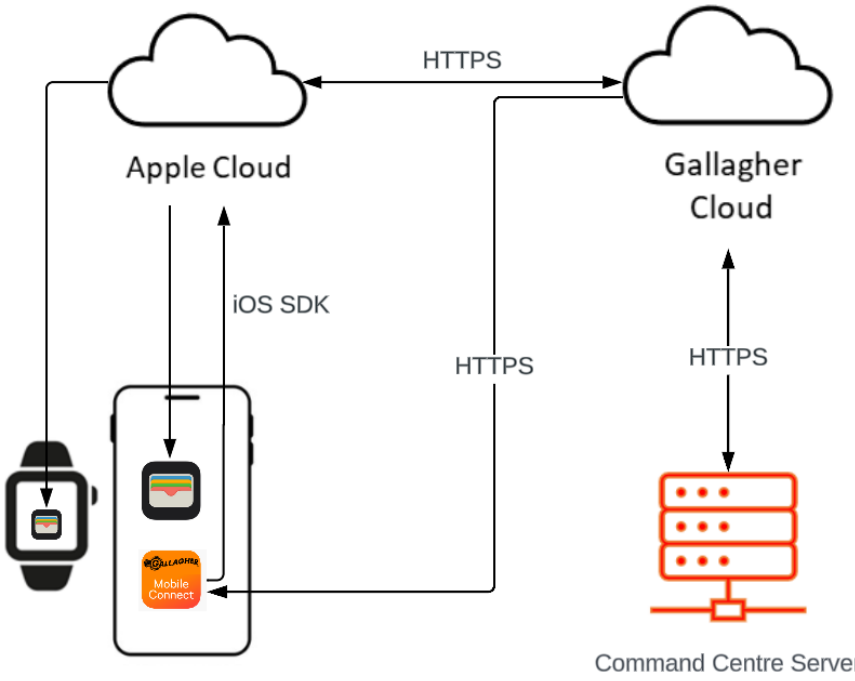
5 Apple Employee Access Badge

5.1 Solution Enablement

Apple Employee Access Badge solution requires the following:

- The Command Centre server must be licensed to use the Mobile Wallet feature.
- Active connection to the Command Centre Cloud and the Gallagher API Gateway (***REF2***).
- "Mobile Wallet" enabled as a card technology for the site's readers.
- TCI value and badge template identifier to use with Apple Employee Badge Type assigned and authorized by Gallagher.
  Note: Authorizing TCI values and approving artwork templates offers an additional layer of protection, ensuring that these are not shared between customers without explicit mutual consent.
- Command Centre server auto-generated Apple Master and Privacy keys.
- Registered Mobile Credential per Cardholder to trigger the badge provisioning flow.
  Note: A Mobile Credential is used for identifying and verifying the Cardholder when delivering the Wallet provisioning data. It provides a secure connection between the phone and the Gallagher Cloud Services. Once the Wallet Access Badge has been provisioned the Mobile Credential is no longer required.

5.2 Access Badge In-App Provisioning



Apple Employee Access Badge solution uses the Mobile Connect app to trigger the In-App Provisioning flow:

1. Once the Mobile Wallet is enabled and configured for a site, all registered Mobile Credentials linked to the Apple Employee Badge Type are sent a wallet provisioning update via the Gallagher Cloud Services.

2. The update is used by the Mobile Connect app to display the "*Add to Wallet*" button and enable the Cardholder to provision the Wallet Access Badge.
3. When the Cardholder clicks the "*Add to Wallet*" button, the Gallagher Cloud Services generates provisioning information and hands it over to the Apple Access Platform using iOS PassKit SDK.
4. The Apple Access Platform requests Gallagher Cloud Services to generate the badge data. This step generates the display and data attributes of the badge using the Cardholder information and the site's TCI, Master and Privacy keys to generate the DESFire credential, which is then encrypted and sent as a response back to Apple.
5. The Apple Access Platform delivers the badge to Apple Wallet on the devices and notifies the Gallagher Cloud Services of success or failure.
   Note: The Access Badge is only added to the Cardholder in the Command Centre server when the Gallagher Cloud Services receives a successful provisioning event from Apple.
6. If the Cardholder has an Apple Watch paired with their iPhone, an additional pass is automatically provisioned onto the Apple Watch with a distinct credential to allow the Cardholder to access locations or services with either device.
   Note: The timing and order in which badges are added to phones and paired watches are not guaranteed as the continuation of the provisioning process is dependent on the Apple Access Platform.

Note: For more details about the Access Badge provisioning in the Mobile Connect app, refer to the technical Information paper "Mobile Connect Cloud and App Security TIP" (***REF1***).

Account Binding

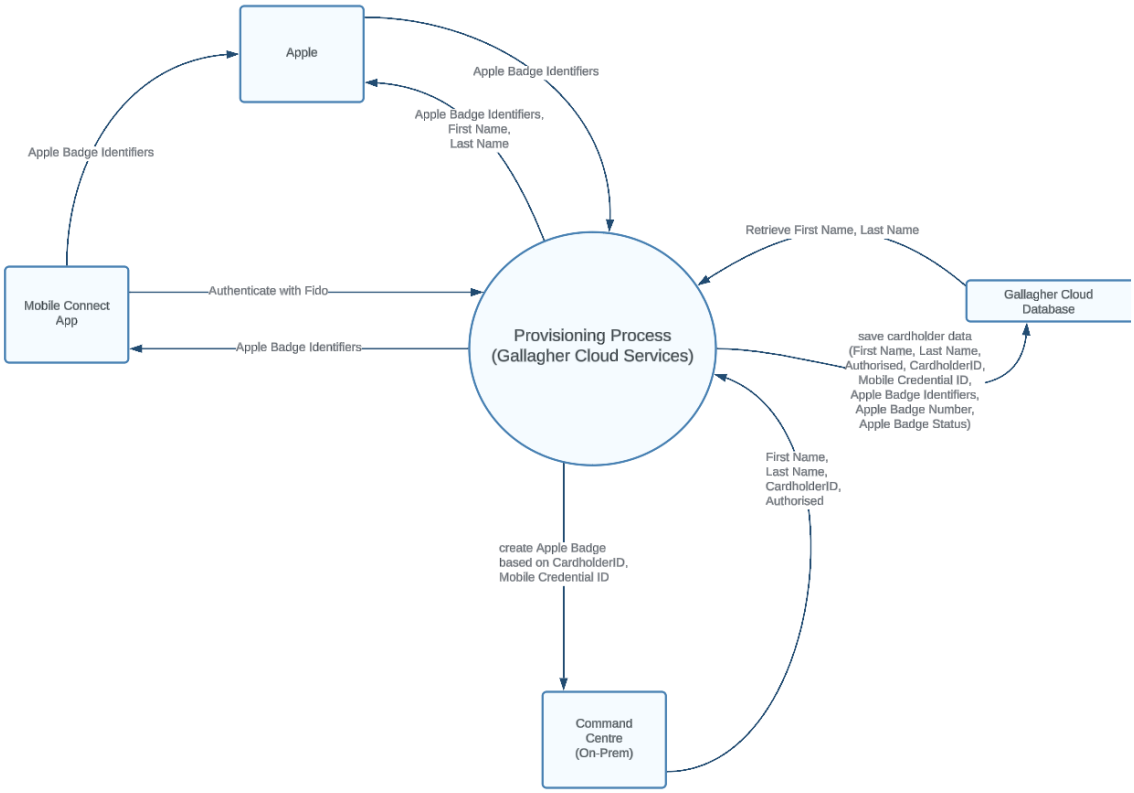
When an Access Badge is provisioned to a Cardholder for the first time, Gallagher Cloud Services binds the Cardholder's iCloud account to the badge. This process, known as strong binding, is implemented as an additional layer of security and fraud prevention.

As a result, a Cardholder cannot transfer their provisioned Access Badge to a different iCloud account.

Additionally, Gallagher Cloud Services enforces a device migration limit to prevent badge duplication fraud. A 90-day migration period allows the Cardholder to transfer the badge to a newly purchased device of the same type (phone or watch) once.

Data Flow of Personally Identifiable Information (PII)

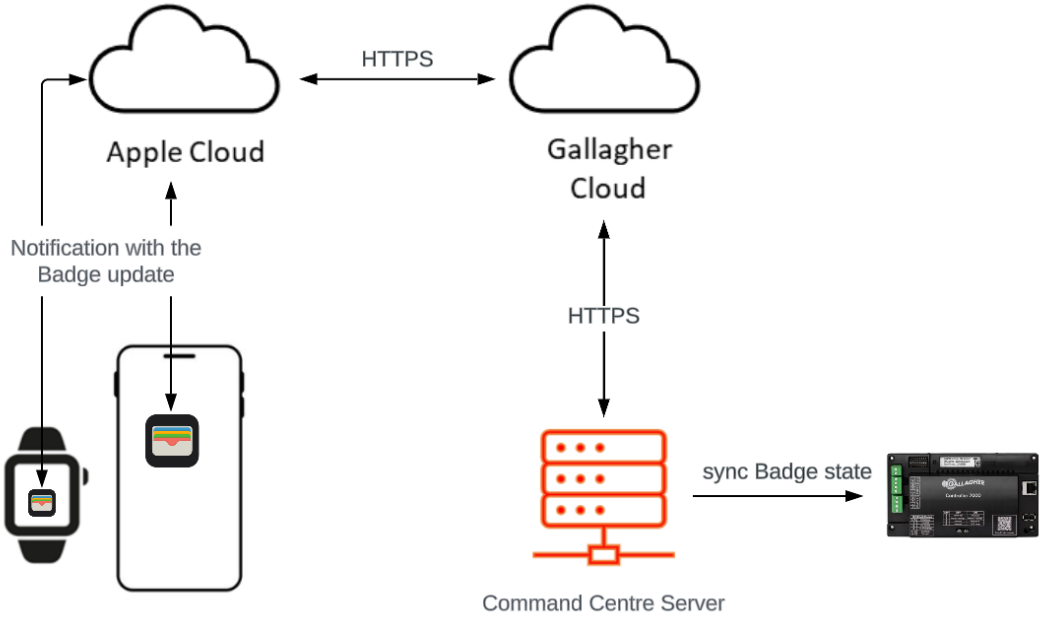
Access Badge provisioning flow requires access to Cardholder personal information for the solution to function correctly. The following diagram shows the PII flow at provisioning time:



Refer to "*Data Security*" and "*Data Storage and Retention*" sections, for more information about security measures taken by Gallagher for handling and storing the data.

5.3 Access Badge Updates

Apple Access Badge updates may include state updates, artwork changes, or underlying credential modifications. A badge can be updated on a single device or across multiple devices, such as an iPhone and its paired Apple Watch.



5.3.1 State Management Updates

Apple Access badges are access credentials which share the same infrastructure within the Command Centre as other credentials. An Access Badge state is managed separately from other credentials assigned to the Cardholder.

➢ Triggered by the Cardholder

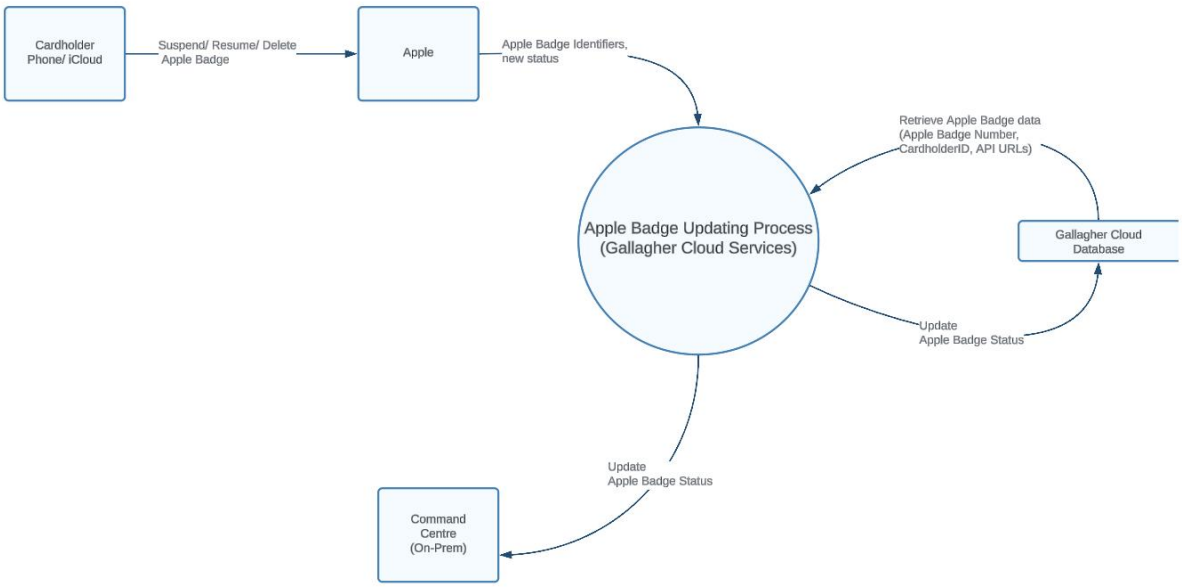
Apple Access Badges can be individually suspended, re-activated, and removed by the Cardholders using their devices' Apple Wallet app or via their iCloud account.

When a Cardholder suspends, re-activates, or deletes a badge, the Apple Access platform communicates with the Gallagher Cloud Services to perform the action for the specific badge using the badge unique identifier (UUID). The badge state change is then synced to the Command Centre server and applied to the badge accordingly.

Note: An Access Badge that is disabled by the Cardholder can be re-activated by the Command Centre operator, this however requires the operator to have "Override Card Status" privileges. Apple Access platform can choose to fail the activation request which results in de-activating the badge and setting the state to "Failed to activate" in Command Centre.

Data Flow of Personally Identifiable Information (PII)

Access Badge state update triggered by the Cardholder requires access to the Cardholder's personal information for the solution to function correctly. The following diagram shows the PII flow at badge update time:



Refer to "*Data Security*" and "*Data Storage and Retention*" sections, for more information about security measures taken by Gallagher for handling and storing the data.

➢ Triggered by the Command Centre Operator

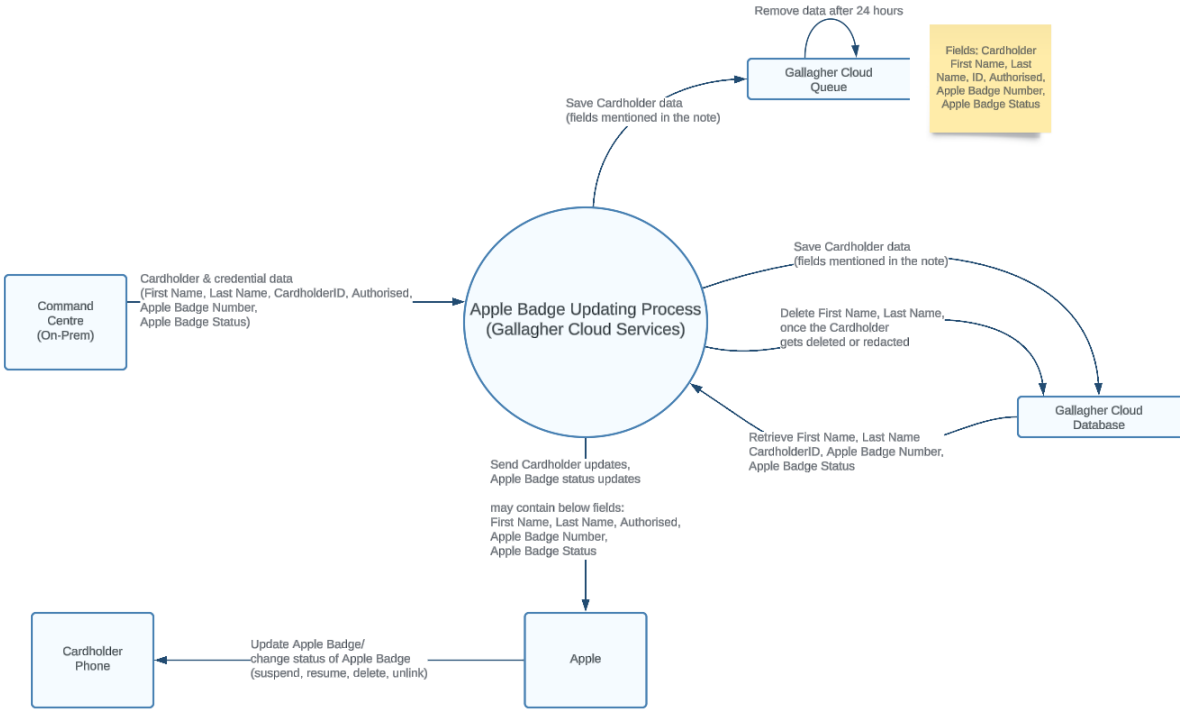
Access Badges are represented as other access credentials in the Command Centre. As such, they can be marked as Active, Expired, Pending, or Disabled.

When a Command Centre operator disables, re-activates, or removes a badge, the update is sent to the Gallagher Cloud. The state update is then sent as a request to the Apple Access Platform to perform the action for the specific badge using the badge unique identifier (UUID). Apple Access Platform then delivers the update to the device when possible, and a success or failure notification is sent back to the Gallagher Cloud Service.
Apple attempts its best efforts to deliver the update notification to the device. If not online, the Apple Access Platform will try for up to 30 days to deliver the update notification to the device.

Note: An Access Badge that is disabled by a Command Centre operator cannot be re-activated by the Cardholder. However, a Cardholder can remove the disabled badge and re-provision it again. It is recommended to de-authorize the Cardholder, delete, or disable the provisioning Mobile Credential to revoke access.

Data Flow of Personally Identifiable Information (PII)

Access Badge state update triggered by the Command Centre operator requires access to Cardholder personal information for the solution to function correctly. The following diagram shows the PII flow at badge update time:



Refer to "*Data Security*" and "*Data Storage and Retention*" sections, for more information about security measures taken by Gallagher for handling and storing the data.

5.3.2 Badge Data Updates

Attributes of an Access Badge in the Wallet app can be updated by the Gallagher Cloud Services. Display attributes (such as Cardholder first and last names, badge artwork change) and data attributes (the underlying badge credentials).

Command Centre operator can trigger an individual display attribute change to a Cardholder badge by changing the first or last names. An operator can also trigger site-wide badge change which will be applied to all provisioned badges when changing the badge template identifier or rolling the Apple Wallet Master and Privacy keys.

Note: Gallagher can trigger artwork badge updates on behalf of the site when configuring/updating the badge artwork template in the Apple Business Register portal. This update will be applied to all provisioned badges and will be delivered to each device by the Apple Access Platform when possible.

5.4 Access Transaction

Gallagher HBUS Multi-Tech devices/readers support Enhanced Contactless Polling (ECP v2.3) to read MIFARE DESFire Apple Access Badges.
The ECP protocol allows the readers to broadcast site configuration and capability information in the contactless polling loop to Apple devices before the transaction initiates. The polling loop contains Terminal Capabilities Identifier (TCI) used for Express Mode and Terminal Requested Authentication (TRA) used to request second-factor authentication on a transaction.

Note: Gallagher Readers are Apple IOT certified. Gallagher and Apple have conducted extensive interoperability testing before launching the solution to ensure consistent reader performance across multiple Apple devices and device generations.

Apple Access Badge access transaction flow:

1. The Cardholder presents the Apple device to the reader, which is broadcasting the site TCI allowing the Apple Wallet app to select and present the correct Access Badge.
2. The reader will then authenticate the badge.
   Note: If a second factor is required to access a door, then the reader will request a second factor (Face ID, Fingerprint, PIN) and access the secure application of the badge. The secure application part of the credential is only available upon a successful 2FA authentication.
3. The credential information is passed to the controller, which makes the final access decision.
   Note: The outcome reflected in the Apple Wallet app, indicates whether the read was successful or not, without conveying the access decision itself.

6 Data Security

6.1 Data in Transit

Communication between Command Centre and Gallagher Cloud Services

All data transfer between Gallagher Command Centre, Gallagher API Gateway, Gallagher Mobile Wallet Service, and Mobile Apps uses encrypted HTTPS.

We support only TLS 1.2 and TLS 1.3; older protocols are disallowed, which mitigates most encryption-related security risks.

Communication between Command Centre and Command Centre Cloud and Gallagher API Gateway is authenticated using TLS client certificates (2048-bit RSA).

Command Centre Mobile Wallet DESFire site seed keys are bundled and encrypted (ECC P-256), using a public key from the Gallagher Mobile Wallet Cloud Service.

Communication between internal Cloud Services

Inter-service communication between Gallagher Cloud Services uses HTTPS / TLS 1.3 with certificate pinning.

Communication between Gallagher and Apple Access Platform

Communication between the Gallagher Cloud Services and the Apple Access Platform is encrypted using HTTPS/ Mutual Transport Layer Security (mTLS with 2048-bit RSA certificates). Additionally, inbound and outbound network Access Control Lists (ACLs) have been set up to enhance networking security.

EC v3 encryption scheme is used to encrypt and decrypt the data sent between the Gallagher Cloud services and the Apple Access Platform. The encryption scheme uses the following to encrypt data:

- Elliptic-curve Diffie–Hellman (ECDH) generated private and public key pairs. This scheme uses Elliptic Curve **secp256r1**.
  Other aliases for this curve are **NIST P-256**, **1.2.840.10045.3.1.7**, **prime256v1**, and **secp256r1**.
- ANSI X9.63 Key Derivation Function (KDF) used to derive the shared secret.
- AES-128 encryption algorithm in Galois/Counter Mode (GCM) used to encrypt the data.

Communication between Apple Wallet and Gallagher Readers uses the Apple device core Near Field Communication (NFC). The underlying credential is presented as a MIFARE DESFire credential consisting of a privacy application, encrypted with a shareable AES128 key, and two payload applications which contain the actual credential information; one for single factor and a secure one used for the second factor. The privacy key is first used to access the card's real UID, which allows diversification of the read key, that is then used to read the payload. This key is one of the 8 diversified shareable keys generated from the site's Mobile Wallet 16-byte seed key. All keys are stored and diversified at the Gallagher controllers.

6.2 Data at Rest

The Mobile Wallet solution stores site-wide and Cardholder data in the Gallagher Cloud Services in Amazon Aurora databases, using industry-standard AES-256 encryption for data and metadata at rest.

Refer to the “Data Storage and Retention” section below for more information about the data retained by the solution.

7 Data Storage and Retention

For the Mobile Wallet solution to function properly and deliver a seamless user experience, data must be retained on-premises, in the Gallagher Cloud Services, and on mobile devices.

7.1 Command Centre (On-Prem)

- Site’s Apple Wallet DESFire 16-byte Master and Privacy keys. Keys are encrypted at rest using an AES key generated using the database recovery code.
- Site’s TCI which is assigned by Gallagher to the site.
- Site’s badge template identifier (UUID generated by Apple when configuring the site with the badge artwork).
- Actively provisioned Apple Access Badges.

7.2 Mobile Devices

- Mobile Connect App (currently iOS only) stores wallet provisioning data, which is unencrypted at rest. However, this is stored on the private app database and is protected by the device operating system sandboxing.
  - Cardholder first and last names.
  - Cardholder global identifier unique within a Command Centre system (UUID).
  - The linked Apple Employee Badge Type global identifier unique within a Command Centre system (UUID).
  - Random Apple user identifier (UUID).
- The Wallet Access Badge is stored on the Secure Element (SE) of the device by Apple, which is isolated from the main operating system, adding an additional layer of security. Security of the badge data is managed and maintained by the Apple eco-system.

Removing Stored Device Data

A Cardholder can remove persisted mobile wallet data associated with a site by deleting the Mobile Credential from the Mobile Connect App or by deleting the app.

A Cardholder can remove Apple Access Badge data of the device by deleting the badge from the Wallet app on the Apple device.

7.3 Cloud Services

- Site's server serial number.
- Encrypted (ECC P-256) bundle of the site's Apple Wallet DESFire seed keys (Master and Privacy keys). Decrypted for key diversification of the underlying credential for a badge at provisioning time.
- Site TCI value used when generating the underlying credential data for a badge at provisioning time.
- Site's badge template identifier (UUID).
- Mobile Credential ID (UUID) used by the Mobile Connect app/SDK, FIDO credential information, and encrypted un-downloaded provisioning Mobile Wallet updates.
  Note: For more details about the data stored in the Mobile Connect app, refer to the technical Information paper "Mobile Connect Cloud and App Security TIP" (***REF1***).
- Random Apple Badge identifiers (UUID) unique to the Apple system.
- Cardholder first and last names.
- Cardholder authorised flag.
- Cardholder global identifier unique within a Command Centre system (UUID).
- The Apple Employee Badge Type global identifier unique within a Command Centre system (UUID).
- Apple badge number (8 bytes) unique within the Command Centre site.
- Apple Badge state.
- API update URLs for Apple Employee Badge type, Cardholders, and Access Badges used for syncing updates between the Gallagher Cloud Services and the on-premise Command Centre server.
- Minimal active count and usage data for Access Badges per site, this is collected for licensing purposes and to satisfy Apple's reporting requirement.

Removing Stored Cloud Services Data

For removing Mobile Credential data stored in the Gallagher Cloud, refer to the section "Data Storage and Retention" of the technical Information paper "Mobile Connect Cloud and App Security TIP" (***REF1***).

Individual Cardholder first and last names can be requested by the Cardholder and removed by the Command Centre operator by deleting or redacting the Cardholder from the Command Centre server.

Access Badge information is kept even when the badge is deleted from the Cardholder Wallet App or the Command Centre serve, This information is the minimum required for the solution to function, and it is retained until you no longer wish to use the Gallagher Mobile Wallet solution.

8 Security Controls

8.1 Mobile Devices

Security, access control, and data isolation are managed by the mobile device's operating system and hardware platform. It is recommended to always keep users' devices updated to the latest operating system version for optimal security.

8.2 Gallagher Cloud Services

Our cloud services are securely hosted using Amazon Web Services and isolated from external services using an AWS Virtual Private Cloud.

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

All administrative users accessing our cloud infrastructure require a Security Technician Certificate of Approval issued by the New Zealand Private Security Personnel Licensing Authority.

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 daily where required. We employ automated scanning tools that 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.

Notice of any incidents or outages that may affect customers will be provided via our Gallagher Cloud Services status page (https://status.gallagher.com/), Channel Partners, or a direct email alert system, which customers may sign up to by contacting their Channel Partner.

8.2.1 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 following DNS or IP addresses.
Note: There is no need to allow any inbound traffic to your Command Centre server.

If you are configuring firewall rules based on IP address, please allow the following static IP addresses:

Australian Command Centre Cloud

DNS address: **commandcentre-ap-southeast-2.security.gallagher.cloud**

IP addresses: **52.62.211.7** and **54.79.91.203,**

Australian Gallagher Gateway Region:

DNS address: **commandcentre-api-au.security.gallagher.cloud**

IP Addresses: **3.106.1.6** and **3.106.100.112**

United States Gallagher Gateway Region:

DNS address: **commandcentre-api-us.security.gallagher.cloud**

IP Addresses: **44.193.42.111** and **3.209.194.103**

Global Cloud Services API Gateway:

DNS address: **services.security.gallagher.cloud**

IP Addresses: **15.197.141.103** and **76.223.78.39**

8.2.2 Certifications

Gallagher is committed to data security and privacy. Our cloud-hosted solutions are SOC 2 Type 2 certified.

8.2.3 Penetration Testing

Gallagher employs internal security and penetration testing staff, who hold several 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 is engaged to do a comprehensive review annually, or more frequently with each major release as required. 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.

9 Related Resources

ID	Document Title	Location
REF1	Mobile Connect Cloud and App Security TIP	https://gallaghersecurity.github.io/r/mobileconnect-cloud-and-app-security
REF2	Command Centre Cloud Api Gateway TIP	https://gallaghersecurity.github.io/r/commandcentre-cloud-api-gateway