Gallagher Command Centre

Cryptography and Encryption

Technical Information Paper

Copyright © Gallagher Group Limited

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The information is indicative only and is subject to change without notice meaning it may be out of date at any given time.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

Copyright © Gallagher Group Ltd 2026. All rights reserved.

Contents

1 Introduction 5

2 Compatibility 5

3 Cryptography Process Basics 5

4 Microsoft SQL Encryption 5

5 Multi-Server 5

6 Active Directory Single Sign-On Feature 6

7 Gallagher Command Centre Certificates 6
- 7.1 Gallagher Command Centre Server Certificate 6
- 7.2 Gallagher Command Centre CA Certificate 6
- 7.3 Gallagher Command Centre Client Certificate 7
- 7.4 Gallagher OPC UA Certificate 7
- 7.5 Gallagher DCOM Certificate 7
- 7.6 Gallagher Controller ("BertBus") Certificate 8
- 7.7 Gallagher Controller ("BertBus") Signing Certificate 8
- 7.8 Gallagher Biometric Signing Certificate 8
- 7.9 Biometric Reader Signing Certificate 8
- 7.10 Gallagher Mobile Client Web Services Certificate 8
- 7.11 Gallagher REST API Certificate 9
- 7.12 FIDO2 MDS Root Certificate 9
- 7.13 Gallagher Command Centre Cardax Master Certificate and Controller 6000 factory certificates 9
- 7.14 Gallagher Command Centre Device Master Certificate and Controller 7000 factory certificates 10
- 7.15 Gallagher Controller 7000 HTTPS CA Signing certificate 10

8 Gallagher Command Centre Encryption Information 10
- 8.1 Gallagher Command Centre Database Level Encryption 10
- 8.2 Random Number Generation 11
- 8.3 Operator Password Hashing 11
- 8.4 Service Process Authentication 11
- 8.5 Gallagher Command Centre Archive File Tamper Detection 11
- 8.6 Gallagher Command Centre Software Signing 11
- 8.7 MIFARE Site Key text file 11
- 8.8 Exporting Card Layouts 11

9 Encryption of Data-at-Rest on Server 12
- 9.1 Encryption of Data-at-Rest on Controller 12

10 Gallagher Command Client Connections 12
- 10.1 Gallagher Command Centre Client 12
- 10.2 Gallagher Command Centre Configuration Client 12
- 10.3 Gallagher Visitor Management Client 13
- 10.4 Gallagher Visitor Management Kiosk 13

11 Gallagher Command Hardware Connections 13
- 11.1 Controller Encrypted Communications 13
  - 11.1.1 Controller 7000 13
  - 11.1.2 Controller 6000 14
  - 11.1.3 Port 546 UDP is open when a Controller is started with DIP switch 2 on 14
- 11.2 Controller-to-Server Communication 14
- 11.3 Controller-to-Controller Communication 14

Copyright © Gallagher Group Limited

11.4 HBUS Encryption 14
11.5 HBUS Devices without a Secure IC 14
11.6 HBUS Devices with a Secure IC 15
11.7 802.1x Support 15
12 Gallagher Command Centre PIV 16
13 Card Encryption 16
14 Web Service Connected Features 16
14.1 REST API 16
14.2 SOAP API - Cardholder Web Service 17
14.3 Active Directory Sync Feature 17
14.4 Entra ID Sync Feature 18
14.5 Gallagher Cloud Services 18
14.6 Gallagher Command Centre Mobile Client 18
14.7 Gallagher Command Centre Mobile Connect 19
14.7.1 Gallagher Apple Wallet Integration 19
14.8 Mobile Client SDK 20
14.9 Diagnostics Service 20
15 External Communications Encryption 20
15.1 IP Alarm Transmission 20
15.2 XML Import/Export 20
15.3 Gallagher IDEMIA Integration 21
15.4 Gallagher Command Centre Controller API 21
15.5 Commend Intercom 21
15.6 Gallagher Salto Integration 21
15.7 Gallagher ASSA Abloy IP-Enabled Lock Integration 21
16 OneLink (Cloud Controller Gateway) 22
16.1 Controller Registration 22
16.2 Server Discovery 22
16.3 Controller to Controller Gateway 22
16.4 Controller Gateway to Command Centre 23
17 Encryption Table 23
18 Deprecated Cryptographic Algorithm usage 24
18.1 SHA-1 24
18.2 MD5 24
18.3 RC4 24
18.4 DES/3DES 24
19 Legacy Command Centre Encryption 25
20 Glossary 26
21 References 27
21.1 Internal references 27
21.2 External references 27

Copyright © Gallagher Group Limited

1 Introduction

This document addresses questions regarding Gallagher Command Centre cryptography. It is intended to provide an overview of the encryption and authentication used by the Gallagher Command Centre Server, Controllers, and devices.

2 Compatibility

- Gallagher Command Centre vEL8.30 (or later release)
- Gallagher Controller 6000 vCR8.30 (or later release)
- Gallagher Controller 7000 vCR9.00 (or later release)
- Gallagher Controller 7000 Single Door vCR8.70 (or later release)

3 Cryptography Process Basics

Gallagher Command Centre uses industry-standard algorithms and processes.

- Asymmetric cryptography, or public-key cryptography, is an encryption scheme that uses two mathematically related keys. The public and private key pair comprise of two uniquely related cryptographic keys. The public key is what its name suggests - public. It is made available to everyone via a publicly accessible repository or directory. The private key must remain confidential to its respective owner. Because the key pair is mathematically related, anything encrypted with a public key may only be decrypted by its corresponding private key and vice versa. Gallagher uses the following asymmetric cryptography algorithms: RSA, ECC
- Symmetric cryptography, or symmetric-key encryption, is an encryption scheme that uses the same cryptographic key for both encryption and decryption. The key, in practice, is a shared secret between two or more parties that can be used to maintain a private information link. Gallagher uses the AES symmetric encryption algorithm.

4 Microsoft SQL Encryption

Encryption can be turned on for the MSSQL server communications in SQL server.

Microsoft SQL Server can use Secure Sockets Layer TLS to encrypt data that is transmitted across a network between an instance of SQL Server and a client application. The TLS encryption is performed within the protocol layer and is available to all SQL Server clients. For information on encrypting connections to SQL refer to Microsoft SQL documentation.

5 Multi-Server

Gallagher supports inter-connection of servers for enterprise-wide solutions. Servers connect to each other via TCP/IP, using the OPC UA protocol. Each Gallagher server that is enabled with a Multi-Server license can be configured to establish a secure peer-to-peer relationship with any other similarly licensed Gallagher server within an organisation.

Secure server authentication and communication makes use of the OPC UA framework. This framework implements strong open encryption algorithms, secure authentication techniques, and long key lengths. For Command Centre, these keys are 2048-bit for RSA signing and verification, and 256-bit for AES symmetric encryption.

Copyright © Gallagher Group Limited

6 Active Directory Single Sign-On Feature

The Gallagher Command Centre Active Directory Single Sign-On feature uses the Microsoft Windows Kerberos version 5 authentication protocol. Kerberos is a network authentication protocol, designed to provide strong authentication for client/server applications by using secret-key cryptography.

The Microsoft Windows Server operating system implements the Kerberos version 5 authentication protocol and implements extensions for public key authentication. The Kerberos authentication client is implemented as a Security Support Provider (SSP) and can be accessed through the Security Support Provider Interface (SSPI). Initial user authentication is integrated with the Windows logon single sign-on architecture. The Kerberos Key Distribution Centre (KDC) is integrated with other Windows Server security services running on the domain controller. The KDC uses the domain's Active Directory service database as its account database. An Active Directory server is required for default Kerberos implementations.

For more information on Kerberos, see the following Microsoft web page:
https://technet.microsoft.com/pt-pt/library/cc772815(v=ws.10).aspx

7 Gallagher Command Centre Certificates

The Gallagher Command Centre Server makes use of a number of certificates to perform various functions. Three of these certificates can be found in the windows certificate store (Local Computer \ Gallagher Applications \ Certificates). The rest are stored in the server's database, with the associated private keys are secured by the database encryption described in section 8.

7.1 Gallagher Command Centre Server Certificate

Stored in: Windows Certificate Store – Computer Account (Server Only)

Certificate type: RSA2048 SHA256

Private key permissions required: Administrators, Command Centre service account

This certificate is created and bound to TCP ports 8901 and 8902 by the installer. The "recovery code" utility will fix permissions to the certificate but will NOT recreate or re-bind the certificate to the TCP ports.

The certificate is used for service authentication, (e.g. Controller service to Command Centre service).

The certificate can optionally be used for securing mobile device communications.

On upgrade, existing sites will continue using this certificate for securing mobile device communications.

7.2 Gallagher Command Centre CA Certificate

Stored in: Command Centre Database

Certificate type: RSA2048 SHA256

The certificate is used to verify the signatures of Mobile Device client certificates, to prove they have been enrolled against this server, and not another server. This only affects Mobile Device connections and as such you can ignore the Certificate Authority (CA) certificate if the site is not using Mobile Devices.

The old certificate will be left in the Windows store for upgrading sites, as Mobile Devices which enrolled prior to the 8.30 upgrade are still verified against the old CA, But for mobile devices enrolled after the site upgrades to 8.30 they will be validated by the one in the database. New sites installed from 8.30 onwards will never have this in the windows store, only in the database.

Copyright © Gallagher Group Limited

7.3 Gallagher Command Centre Client Certificate

Stored in: Windows Certificate Store – Computer Account (Server and Workstations)

Certificate type: ECDSA (P256) SHA256

Private key permissions required: Authenticated users.

This certificate is created by the server installer and client MSI installers. These installers have administrative rights during installation and are therefore able to create a machine wide client certificate for client authentication.

The Workstation Certificate installer utility can also be used to create this certificate on workstations when ClickOnce client installers are being used with strict client authentication (e.g. Workstation restrictions enabled).

The certificate may not be present on workstations where the client was installed by a ClickOnce installer. If the server is not configured for strict client authentication (e.g. Workstation Restrictions) these clients will be able to connect without a workstation certificate.

This certificate is pinned (stored in the server's database) when a workstation registers with the server. Changing this certificate will invalidate the workstation's registration, preventing the workstation from authenticating.

The Gallagher Command Centre Client Certificate is also used for authentication by some utilities, (e.g. the Bulk Configuration Tool).

7.4 Gallagher OPC UA Certificate

Stored in: Command Centre database

Certificate type: RSA2048 SHA256

This certificate is used for authenticating:

- Multi-server OPC UA communications
- Command Centre Client OPC UA communications
- Visitor Management Kiosk OPC UA communications
- Visitor Management Reception client WCF communications

This certificate is created on upgrade or installation. The certificate is also recreated when starting the Command Centre service if it is missing.

If the certificate is changed, the server's thumbprint in client configuration files will have to be updated to match. Server connections in a multi-server environment will also require the "accept certificate" override to be performed.

7.5 Gallagher DCOM Certificate

Stored in: Command Centre database

Certificate type: ECDSA (P384) SHA256

This certificate is used for authenticating the server during communications with Configuration Clients (DCOM tunneled over WebSocket).

This certificate is created on upgrade or installation. The certificate is also recreated when starting the Command Centre service if it is missing.

If the certificate's public key is changed, the server's thumbprint in client configuration files will need to be updated to match.

Copyright © Gallagher Group Limited

7.6 Gallagher Controller ("BertBus") Certificate

Stored in: Command Centre database

Certificate type: ECDSA (P384) SHA256

This certificate is used for authenticating the server during communications with Controller 6000s (version 7.80+) and Controller 7000s (version 8.70+).

This certificate is created on upgrade or installation. The certificate is also recreated when starting the Command Centre service if it is missing.

If the certificate's public key is changed, controllers will refuse communication with the server, and will require a Dip Switch 2 restart to clear the configured server thumbprint from the controller.

7.7 Gallagher Controller ("BertBus") Signing Certificate

Stored in: Command Centre database

Certificate type: ECDSA (P384) SHA256

The certificate is part of the exported "external system server" configuration and is used as a trusted authority by the FTCAPI / Middleware Framework to verify communications between the FTCAPI / Middleware and Controllers. A controller's in-field generated certificate is periodically signed by the Command Centre server, validating the controller to communicate with the FTCAPI.

This certificate is created on upgrade or installation. The certificate is also recreated when starting the Command Centre service if it is missing.

7.8 Gallagher Biometric Signing Certificate

Stored in: Command Centre database

Certificate type: RSA2048 SHA256

This is used in encrypted communications with Morpho biometric readers so the reader can verify it is communicating with a legitimate Command Centre instance (it signs Command Centre biometric comms certificates). This certificate is generated on first use if it does not already exist, then stored in the database.

7.9 Biometric Reader Signing Certificate

Stored in: Command Centre database

Certificate type: RSA2048 SHA256 (self-signed per reader)

This is used in encrypted communications with Morpho biometric readers so Command Centre can verify it is connecting to the expected/valid reader.

This certificate is created when secure reader certificates are generated/provisioned and saved against the reader record. It is replaced when reader certs are regenerated.

7.10 Gallagher Mobile Client Web Services Certificate

Stored in: Command Centre database

Certificate type: RSA2048 SHA256

This certificate is used for authenticating the server during communications with Mobile Clients.

There is an option to switch between using the Gallagher Command Centre Server Certificate in the Windows certificate store, and this certificate in the database, or to import and use your own custom certificate, which will be stored in the database.

Copyright © Gallagher Group Limited

This certificate is created on upgrade or installation. The certificate is also recreated when starting the Command Centre service if it is missing.

7.11 Gallagher REST API Certificate

Stored in: Command Centre database

Certificate type: RSA2048 SHA256

This certificate is used for authenticating the server during communications with REST clients.

There is an option to switch between using the Gallagher Command Centre Server Certificate in the Windows certificate store, and this certificate in the database, or to import and use your own custom certificate, which will be stored in the database.

This certificate is created on upgrade or installation. The certificate is also recreated when starting the Command Centre service if it is missing.

7.12 FIDO2 MDS Root Certificate

Stored in: Command Centre database

Certificate type: RSA2048 SHA256

This is a GlobalSign root CA public certificate and is used to validate the FIDO2 MDS “BLOB” file. The BLOB contains a list of metadata statements related to authenticators known to the FIDO Alliance. The integrity and authenticity of this file is verified with its digital signature, which must end its chain with the above root certificate. The contents of the BLOB are then used to determine if the FIDO2 token presented for enrolment into Command Centre is a valid token.

7.13 Gallagher Command Centre Cardax Master Certificate and Controller 6000 factory certificates

Master Certificate Stored in: Command Centre License, Command Centre Database and Command Centre executable

Master key Stored in: Gallagher Group Secure production facilities

Controller Key and Certificate Stored in: Encrypted on Nand for Standard Controller 6000, Secure Integrated Circuit for High Sec Controller 6000 and Controller 6000 Enhanced

Certificate type: RSA1024 SHA1

The Cardax Master Certificate is copied from the Command Centre license into the server database and embedded in the Command Centre install as a fallback if absent from the license.

It is used to verify Controller 6000s as authentic Gallagher product when they first communicate with Command Centre (with dipswitch 2 on).

The controller must respond to a server challenge with the factory certificate and a signature from the matching factory private key before further communication allowed.

This protects against supply chain attacks with fraudulent Controllers but after first authentication and 'pinning' the controller generated certificates it is not relied upon for site security.

This authentication is repeated if the 'Revalidate certificate' override is performed on the controller to 'unpin' the controller's generated certificate.

Copyright © Gallagher Group Limited

7.14 Gallagher Command Centre Device Master Certificate and Controller 7000 factory certificates

Master Certificate Stored in: Command Centre executable

Master key Stored in: Gallagher Group Secure production facilities

Controller Key and Certificate Stored in: Secure Integrated Circuit

Certificate type: ECC-P384 SHA384

The master certificates are embedded in the Command Centre install.

They are used to verify Controller 7000s as authentic Gallagher product when they first communicate with Command Centre (with dipswitch 2 on).

The controller must respond to a server challenge with the factory certificates and a signature from the matching factory private key before further communication is allowed.

This protects against supply chain attacks with fraudulent Controllers but after first authentication and 'pinning' the controller generated certificates it is not relied upon for site security.

This authentication is repeated if the 'Revalidate certificate' override is performed on the controller to 'unpin' the controller's generated certificate.

7.15 Gallagher Controller 7000 HTTPS CA Signing certificate

Stored in: Command Centre database

Certificate type: ECDSA (P384) SHA256, 20 year expiry

This certificate and key are used as the CA to generate and sign HTTPS certificates for Controller 7000 Diagnostic webpages (9.40+). This certificate and key are first generated on demand for 9.40+ Controller 7000s and exportable from the Controller Web Server page of the Server Properties. The exported certificate can be installed on client machines as a CA to securely access the Controller 7000 Diagnostic web pages from a Web browser.

This certificate can be regenerated from the Controller Web Server page of the Server Properties, but all clients will need exported copies of the new certificate to securely authenticate Controller 7000 HTTPS certificates.

8 Gallagher Command Centre Encryption Information

8.1 Gallagher Command Centre Database Level Encryption

Sensitive data in the Command Centre database is encrypted by AES-256 (CBC mode), using the Data Encryption Key and a cryptographically random Initialisation Vector (IV). The Data Encryption Key is itself randomly generated and is encrypted in the database by AES-256 (CBC mode) using the Key Encryption Key. The Key Encryption Key is derived and stored as follows:

- Recovery Code: randomly generated at install time, necessary for data recovery.
- Key Encryption Key: PBKDF2-HMAC-SHA512(Recovery Code), 100000 iterations, encrypted by Windows DPAPI (CryptProtectData), and stored in the Command Centre Service account's registry hive.

Refer to "Recovery Code TIP" for more details.

Data that is secured by this is:

- Private keys used for communications (ref: Database stored certificates, section 7)
- Passwords used by Command Centre to access external systems (notifications, macros, archiving, DVRs and Intercoms, EDI data source passwords, and Cloud Proxy passwords).

Copyright © Gallagher Group Limited

- Card Pins (when viewable PINs are enabled)
- MIFARE Keys
- Alarm Transmitter keys
- Hashed Operator passwords
- Encrypted Changeset data (Multiserver replication)
- REST Client API keys
- Controller RAS (Dial-up) passwords.
- User codes
- GovPass configuration & application Keys

8.2 Random Number Generation

Command Centre Server uses the operating system's random number generator to generate cryptographically random data.

The High Sec Controller 7000 uses FIPS 140-3 Level 3 certified hardware and the High Sec Controller 6000 uses FIPS 140-2 Level 3 certified hardware random number generator to generate random data.

8.3 Operator Password Hashing

Operator passwords are hashed using PBKDF2-SHA512 with 100000 iterations and 16 bytes of cryptographically random salt. These hashes are encrypted (refer 8.1) before storing in the database.

8.4 Service Process Authentication

Windows services are authenticated by verifying that the service can decrypt a random nonce encrypted with the servers 2048-bit public key.

A nonce is an arbitrary number used only once in a cryptographic communication.

8.5 Gallagher Command Centre Archive File Tamper Detection

A SHA-256 hash of the content of each archive file is stored in the database to detect tampering of the archived event records.

8.6 Gallagher Command Centre Software Signing

Controller and HBUS device software are checked for authenticity by validating against SHA-384 hashes. The hashes are compared to those stored in a signed manifest. The manifest is signed by ECDSA (P384).

8.7 MIFARE Site Key text file

To protect the keys in the exported MIFARE Site Key text file (that contains exported MIFARE Site Keys) it uses AES256-wrap, and PBKDF2-SHA512 with 100000 iterations and 16 bytes of cryptographically random salt.

8.8 Exporting Card Layouts

Exporting Card Layouts using the Bulk Configuration Tool uses AES256, PBKDF2-SHA512, with 100000 iterations and 16 bytes of cryptographically random salt. This encrypts the entire card layout blob, as the blob may contain user-entered MIFARE keys.

Copyright © Gallagher Group Limited

9 Encryption of Data-at-Rest on Server

It is recommended that the server's file system is encrypted using Microsoft BitLocker.

9.1 Encryption of Data-at-Rest on Controller

The Controller's databases and event data are encrypted with AES-256-CBC. The encryption key is cryptographically random and generated when the Controller is started for the first time.

For…	the encryption key is encrypted using a…
all variants of the Controller 7000,	file encryption key which is a uniquely derived key per controller and is stored in the non-volatile storage.
High Sec Controller 6000 and Controller 6000 Enhanced,	key which is inside the secure element and is stored on the filesystem.
Standard Controller C6000,	key which is on the filesystem.

From v8.70, if the Controller is powered on with dip switch 2 set, the above encryption key is re-generated. This has the effect of making all encrypted site-specific data on the controller, including configuration database, any buffered events and site-specific encryption keys unreadable, effectively purging it.

HBus pre-shared keys are stored in NAND encrypted by the Encryption key on all devices.
Sensitive configuration is stored encrypted such as:
- Alarm Transmitter keys
- Mifare keys
- GovPass application Keys

10 Gallagher Command Client Connections

10.1 Gallagher Command Centre Client

The communication between the Gallagher Command Centre client and the Gallagher Command Centre server uses the OPC-UA binary protocol with the WS-SecurityPolicy "Basic256SHA256" algorithm suite. This consists of RSA for authentication/signing, SHA256 for hashing and AES-256 for encryption. The RSA keys are 2048 bit and are generated at the time of installation.

The server's certificate is verified against the thumbprint stored in the client's configuration file.

The client's certificate is verified against the certificate that is pinned on the server during workstation registration.

10.2 Gallagher Command Centre Configuration Client

From vEL7.90, communication between Configuration Client and Command Centre Server uses the operating system's configured TLS settings. TLS 1.2 or higher is recommended. Keys are based on NIST P-384 elliptic curve and generated at the time of installation.

The server's certificate is verified against the thumbprint stored in the client's configuration file.

The client's certificate is verified against the certificate that is pinned on the server during workstation registration.

Copyright © Gallagher Group Limited

10.3 Gallagher Visitor Management Client

Communication between Visitor Management Client and Command Centre Server uses TLS 1.2. The RSA keys are 2048 bit and generated at the time of installation.

The server's certificate is verified against the thumbprint stored in the client's configuration file.

The client's certificate is verified against the certificate that is pinned on the server during workstation registration.

10.4 Gallagher Visitor Management Kiosk

Communication between Visitor Management Kiosk and Command Centre Server uses the OPC-UA binary protocol with the WS-SecurityPolicy "Basic256SHA256" algorithm suite. This consists of RSA for authentication/signing, SHA256 for hashing, and AES-256 for encryption. The RSA keys are 2048 bit and generated at the time of installation.

The server's certificate is verified against the thumbprint stored in the client's configuration file.

The client's certificate is verified against the certificate that is pinned on the server during workstation registration.

11 Gallagher Command Hardware Connections

11.1 Controller Encrypted Communications

The Controllers and Command Centre Server generate and store their own ECC keys (ECC-P384), and self-signed certificates. Both the Controller and the server generate ephemeral keys as part of TLS negotiation which results in forward secrecy. The individual controller's certificate is "pinned" in the server's database and then the server distributes these "pins" to the related controller, so connections are verified. The TLS connections are checked against the pinned public keys to prevent impersonation.

The Controller 6000 Enhanced and High Sec variants, along with all Controller 7000 variants, include increased protection for the storage of encryption keys in the form of a secure integrated circuit (IC). The secure IC on the High Sec controller is certified to FIPS 140-2 Level 3. The controller-specific ECC private key is stored encrypted on the filesystem using a key that is stored inside the secure IC.

All Controller 7000 variants include increased protection for the storage of encryption keys in the form of a secure integrated circuit (IC). The secure IC on the High Sec Controller 7000 is certified to FIPS 140-3 Level 3. The Controller-specific ECC private key is generated in this IC and cannot be exported.

The controller communication key and certificate are cleared and re-generated when configuration is reset to defaults (DIP switch 2 restart). The AES session key, which is negotiated during TLS negotiation, is re-negotiated periodically, at a random interval every 12-24 hours.

TCP port 1072 is used for communication with the Command Centre Server and other Controller devices configured on the network. TLS1.2** is required for inter-controller and controller-server communication. The host firewall blocks incoming traffic on all other TCP and UDP ports with an exception for IPv6 DHCP and Diagnostic Web Pages when enabled on demand by site configuration.

11.1.1 Controller 7000

The diagnostic webpage is server over HTTPS on port 443, using a certificate issued by Command Centre (requested on demand and stored on the Controller). It falls back to unsecured HTTP on port 80 only when HTTP is explicitly forced (ForceHttpWebServer) or while no valid certificate is yet available. Where the interface is served unsecured (Controller 6000, or the forced-HTTP fallback on Controller 7000), its use is strongly recommended against whenever possible.

Copyright © Gallagher Group Limited

11.1.2 Controller 6000

The diagnostic webpage is served only as unsecured HTTP on port 80 (no HTTPS support on this platform). Where the interface is served unsecured (Controller 6000, or the forced-HTTP fallback on Controller 7000), its use is strongly recommended against whenever possible.

11.1.3 Port 546 UDP is open when a Controller is started with DIP switch 2 on

DIP switch 2 enables all DHCP modes, which includes IPv6 DHCP, and the DHCPv6 client (dhcpcd) listens on the standard client port 546/UDP while active.

11.2 Controller-to-Server Communication

Communication between controller and Command Centre Server uses TLS 1.2** with the ECDHE-ECDSA-AES256-GCM-SHA384 cipher suite. TLS client certificates are used to provide mutual authentication.

11.3 Controller-to-Controller Communication

Communication between controllers uses TLS 1.2** with the ECDHE-ECDSA-AES256-GCM-SHA384 cipher suite. Controllers communicate with each other using the same protocol and keys that they use to communicate with the server.

** TLS1.3 from v9.20+. This also depends on the operating system version installed and how it is configured. TLS1.3 is default for Windows Server 2022.

11.4 HBUS Encryption

HBUS is a high-speed RS-485 protocol, designed specifically for the needs of field security hardware. All HBUS device communication is secured using industry leading authentication and encryption.

During manufacturing, Gallagher installs certificates and ECC-P256 keys into the HBUS device to prevent counterfeit connections to HBUS devices. When a HBUS device configured for first time or re-configured, shared keys are securely generated and stored in the Controller and HBUS device. Each time a new communications session is initiated new AES128 session keys are generated. If a session is maintained for more than a day these AES128 keys are regenerated.

Secure communication features are enforced automatically, with no additional configuration required. All HBUS devices maintain an encrypted heartbeat, the device is considered off-line when one of these are not received by the Controller.

The High Sec Controller 6000 and Controller 7000 have a security chip which stores the private keys. The Standard Controller 6000 and Controller 6000 Enhanced do not have such a security chip appropriate for these keys and stores public and private keys encrypted in non-volatile memory.

11.5 HBUS Devices without a Secure IC

When a HBUS device first communicates with a controller, the device and controller exchange certificates and verify each other's certificates are signed by Gallagher. The controller also generates an ephemeral keypair and sends the ephemeral public key to the HBUS device. The static key pairs and the ephemeral key pairs are then used to generate a shared secret, using Elliptic-curve Diffie-Hellman (ECDH).

Pre-shared key generation: The shared secret returned by the ECDH algorithm is fed into AES-CMAC based key derivation algorithm to create two 128 bit AES pre-shared keys. Pre-shared keys are 'pinned' stored encrypted on non-volatile storage using the controller's data at rest capabilities (using secure IC keys on Controller 7000, Controller 6000 Enhanced and High Sec Controller 6000). Configured HBus devices must always resume communication with the controller using the same Pre-shared key. HBus

Copyright © Gallagher Group Limited

devices securely lock their non-volatile storage or are designed to discard the key upon external attempts to access their non-volatile storage.

Session key generation: One pre-shared key is used in the Authenticated Key Exchange Protocol 2 (AKEP2) algorithm which allows the HBUS device and controller to securely determine that they do in fact have the same pre-shared keys. The second pre-shared key is used by an AES-CMAC based key derivation algorithm to generate the session keys, which are also AES-128 bit and again there are two of these, one for encryption (AES-CBC) and one for authentication (AES CMAC).

11.6 HBUS Devices with a Secure IC

All keys are protected by a FIPS 140-2 Level 3 cryptographic module. The High Sec T30 is the first HBUS device to have a FIPS 140-3 cryptographic module.

The controller pre-shared keys are not stored directly in the secure IC but are encrypted with a key stored in the secure IC.

Mutual authentication: The HBUS device and the controller exchange certificates and verify that each other's certificate is signed by Gallagher. An assurance message is then sent to the other device to be signed by that device's private key. The signed message key is then sent back to the requesting device and the signature verified.

Pre-shared key generation: An AES-128-bit master key is used to generate the pre-shared keys. This master key is diversified using the HBUS device's serial number. The diversified key is pre-loaded into the HBUS device's secure element at manufacture. The diversified AES master key is fed into an AES-CMAC based key derivation algorithm to create two 128 bit AES pre-shared keys. Pre-shared keys are 'pinned' stored encrypted on non-volatile storage using the controller's data at rest capabilities (using secure IC keys on Controller 7000, Controller 6000 Enhanced, High Sec Controller 6000). Configured HBus devices must always resume communication with the controller using the same Pre-shared key. HBus devices securely lock their non-volatile storage or are designed to discard the key upon external attempts to access their non-volatile storage.

Session key generation: One pre-shared key is used in the AKEP2 algorithm which allows the HBUS devices and controller to securely determine that they do in fact have the same pre-shared keys. The second pre-shared key is used by an AES-CMAC based key derivation algorithm to generate the session keys, which are also AES-128 and again there are two of these, one for encryption (AES-CBC) and one for authentication (AES-CMAC).

11.7 802.1x Support

For 802.1x we support EAP-TLS (TLS1.2 & TLS1.0) with the following Cipher Suites:
ECDHE-ECDSA-AES256-GCM-SHA384

The certificates supported are RSA 1024 - 4096, and ECC 256 - 512.

Copyright © Gallagher Group Limited

12 Gallagher Command Centre PIV

Gallagher's PIV solution is a physical access control system designed for compliance with the Personal Identity Verification (PIV) requirements of the FIPS 201-2 standard. The High Sec Controller 7000 uses FIPS 140-3 Level 3, and the High Sec Controller 6000 uses FIPS 140-2 Level 3 certified hardware random number generator to generate cryptographically random data.

Gallagher High Sec readers transfer data between PIV smart cards and the High Sec Controller 6000 and 7000 via HBUS protocol.

Gallagher High Sec readers can be configured to work with varying PIV smart card data rates and authentication modes. The solution supports authentication of PIV, PIV-I, CAC, and TWIC credentials.

PIV Cards use public key cryptography as described in the NIST FIPS 201 standard.

13 Card Encryption

MIFARE Classic® and 125kHz are legacy card formats which should no longer be utilised and therefore is not included in the paragraph below.

MIFARE Plus® and MIFARE® DESFire® EV1 / EV2 / EV3 are currently the only MIFARE high security cards supported which are a replacement for the MIFARE (classic) card, these feature multiple certified security levels, including Advanced Encryption Standard (AES) encryption. MIFARE DESFire® EV1 cards are secured by a 128bit customer-defined AES Key. Command Centre encodes MIFARE Plus cards to Security Level 3.

The MIFARE Key Seed is used by Gallagher readers to read MIFARE Plus and MIFARE DESFire cards. The MIFARE Key Seed is configured in the Command Centre Server 'Properties - Card Security'. The MIFARE Key Seed is transferred via the network connection (ethernet or dial-up) to all configured Controller 6000's and 7000's.

The Controller 6000 and 7000 store the MIFARE Key Seed along with the MIFARE Enhanced site key if configured. When a card is presented at a reader, the reader asks the controller for a diversified key specific to that card, which it uses to read the card.

14 Web Service Connected Features

In a web service, web technology such as HTTP is utilized for machine-to-machine communication, more specifically for transferring machine-readable file formats such as XML and JSON.

The various Gallagher web services provide an object-oriented web-based interface to Command Centre Server. There are two types of web services used by Gallagher Command Centre, Representational State Transfer (REST) and Simple Object Access Protocol (SOAP).

SOAP API is deprecated from vEL7.80 onwards and going forward, Gallagher web service development will be focused the REST API. Therefore, we recommend the REST web service for any client application development.

14.1 REST API

REST describes a set of architectural principles by which data can be transmitted over a standardized interface (such as HTTP). REST does not contain an additional messaging layer and focuses on design rules for creating stateless services. A client can access the resource using the unique Uniform Resource Identifier (URI) and a representation of the resource is returned. With each new resource representation, the client is said to transfer state. While accessing RESTful resources with HTTP protocol, the URL of the resource serves as the resource identifier and GET, DELETE, POST, and PATCH are HTTP operations that Command Centre Server performs on a resource.

Copyright © Gallagher Group Limited

A REST API is independent of the language used by each system; hence it promotes longevity and evolution of both systems. It allows a site to use independent developers to quickly integrate systems. All data is securely transferred using a secure token and a pinned certificate with optional IP filtering. Cardholder data can be exported from or imported into Command Centre Server.

All data transfer with the REST API takes place over HTTPS. The operating system determines the cryptography supported (TLS 1.3 recommended). Older protocols like IPSEC can be used but are not recommended, due to encryption-related security risks. Communication with Command Centre Server is authenticated and secured using TLS client certificates (RSA-2048 by default, but an installer can upload certificates of other types). The certificate pinning can be disabled.

14.2 SOAP API - Cardholder Web Service

Note: The SOAP services are no longer officially supported and are obsoleted by the REST API.

SOAP defines a standard communication protocol (set of rules) specification for XML-based message exchange. The standard protocol HTTP makes it easier for SOAP model to tunnel across firewalls and proxies without any modifications to the SOAP protocol. A SOAP client works like a custom desktop application, tightly coupled to the server. There's a rigid contract between client and server, and everything is expected to break if either side changes anything. You need constant updates following any change.

The SOAP services (Cardholder web service) use their own web server. The operating system determines the cryptography supported (TLS 1.3 recommended). The Web Service Certificate Deployment utility is used to create the Server Certificate. It installs the Server Certificate (HTTPS Certificate) on the web server machine. This certificate is used for authenticating the web server and encrypting its traffic, and for verifying the Client Certificate.

SOAP requires the username and password of an operator. The client passes those to the SOAP server over HTTPS and then SOAP checks that it has a pinned certificate that matches the one coming from the client.

14.3 Active Directory Sync Feature

The Gallagher Active Directory Sync Service communicates with the Command Centre Service using HTTPS, secured using TLS 1.2.

The Active Directory Sync UI application (configuration app) communicates with the Gallagher Active Directory Sync Service via COM, limited to the same host (i.e. inbound network connections are not allowed).

The Windows user running the Active Directory Sync UI application is verified against the Windows username of any Command Centre operator in a designated Operator Group (i.e. all operators in the group are checked for a matching username). If such an operator is not found, but the Windows user running the application is a member of the local Administrators group, limited access is granted to the application so that the designated Operator Group can be specified/changed. Any other Windows user is denied all access to the application.

The Gallagher Active Directory Sync Service communicates with Active Directory Domain Controllers using LDAP or LDAPS. Gallagher recommends using LDAPS which secures the connection using TLS 1.2. The Gallagher Active Directory Sync Service is the origin of connection. Active Directory authenticates the service with an Active Directory user's credentials, which are specified in the Active Directory Sync configuration. Replication to and from Active Directory is limited to the user's level of privilege to view and make changes in the Active Directory domain.

Copyright © Gallagher Group Limited

14.4 Entra ID Sync Feature

The Gallagher Entra ID Sync Service communicates with the Command Centre Service using HTTPS, secured using TLS 1.3.

The Entra ID Sync UI application (configuration app) communicates with the Gallagher Entra ID Sync Service via COM, limited to the same host (i.e. inbound network connections are not allowed).

The Windows user (or Entra user in Entra ID Sync v2) running the Entra ID Sync UI application is verified against the Windows username of any Command Centre operator in a designated Operator Group (i.e. all operators in the group are checked for a matching username). If such an operator is not found, but the user running the application is a member of the local Administrators group, limited access is granted to the application so that the designated Operator Group can be specified/changed. Any other user is denied all access to the application.

The Gallagher Entra ID Sync Service communicates with Entra ID using HTTPS, secured using TLS 1.2 or higher. The Gallagher Entra ID Sync Service is the origin of connection. Entra ID authenticates the service either by a shared secret configured for the Entra ID application in the Entra ID management screens, or by selecting a client certificate. A client certificate can be generated or purchased from a certificate authority and then imported into the Entra ID Sync machine's Windows certificate store and uploaded to the Entra ID application registration. The thumbprint is then known to Entra ID and must be entered in the Entra ID Sync UI application.

14.5 Gallagher Cloud Services

Gallagher Cloud Service is the routing service for both the Gallagher Command Centre Mobile Connect, and Gallagher Command Centre Mobile Client. Gallagher Cloud Service 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. Command Centre Cloud Services supports TLS 1.2 and TLS 1.3.

14.6 Gallagher Command Centre Mobile Client

The Mobile Client application communicates over HTTPS using a REST based protocol. In order to ensure only authorised users can connect, the app requires both device and user authentication.

All data transferred to Cloud Services takes place over HTTPS. TLS 1.2 and TLS 1.3 are supported. The communication with Command Centre servers is authenticated and secured using TLS client certificates (RSA-2048). TLS1.3 will negotiate the best settings that are supported by both the server and phone. For most mobile phones this means AES256 with forward secrecy ciphers. The Command Centre Server and clients use an RSA-2048 certificate to authenticate against the cloud. The certificate is stored encrypted in the Command Centre Central Database.

The Gallagher cloud server uses an RSA-2048 certificate, stored securely in AWS. Mobile devices (client) also use RSA-2048 client certificates, stored in the secure operating system storage (equivalent of windows certificate store or better).

The Gallagher Command Centre mobile application is designed to store as little data as possible, relying on Command Centre Server to provide secure storage.

Copyright © Gallagher Group Limited

14.7 Gallagher Command Centre Mobile Connect

Gallagher Mobile Connect app is equivalent to a traditional access card.

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 Mobile Connect app also stores secure credential information, which consists of the FIDO credential information and private keys. 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.

At registration, the Mobile Device generates a public and private key pair (ECC P-256). The public key is sent from the Mobile Device to Command Centre, which saves it, and makes it available to controllers for later use.

All data transfer takes place over HTTPS. Command Centre Mobile Connect supports TLS 1.2 and TLS 1.3. Communication with Command Centre Server is authenticated and secured using TLS client certificates (RSA-2048).

To prevent replay attacks over Bluetooth, Gallagher implement a random Server Challenge as per the FIDO Specification:

https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-protocol-v1.1-ps-20170202.html#replay-attack-protection

The Gallagher Controller is the FIDO server, and the Mobile Device is the FIDO client. When a Mobile Device attempts to authenticate against a Gallagher Bluetooth reader, the controller creates a cryptographically secure random sequence of bytes, and uses this as the FIDO Server Challenge data. It validates that the mobile device response contains the correct Server Challenge, and signature thereof.

This random Server Challenge is cleared after every access attempt, and re-generated every time a new request for access is made, because the challenge is reset on every request, there is no time-based factor or window for attack.

If an attacker were to capture the challenge data from one transaction and replay it, even immediately after, the Server Challenge would be different and thus the replay attack is prevented.

For more information on Gallagher Command Centre Mobile Connect, please refer to the “Mobile Connect Cloud and App Security TIP” and “Mobile End to End Encryption TIP” documents, both available on the Gallagher Command Centre install media.

14.7.1 Gallagher Apple Wallet Integration

Apple Wallet credentials are provisioned in our Mobile Wallet Cloud Service. To allow this, a Mobile Wallet DESFire seed key and privacy key are generated in the Command Centre Server. These are both 16-byte AES keys. They are stored in an encrypted format as defined in section 8.1.

We diversify 8 keys based on the DESFire seed key and send down the first key to Gallagher Controllers. This leaves keys 2-7, which can be shared to a third party for integration (i.e. Aperio).

The DESFire seed and privacy keys are encrypted (ECC P-256) using a public key from the Mobile Wallet Service cloud component. The bundle is sent to the Mobile Wallet Service as a site update. The bundle is stored in this encrypted format. When an Apple Pass is to be provisioned, the bundle is decrypted last-minute and used to diversify the 8 seed keys, and then the 8 card keys. The credentials are DESFire format. The card data is then encrypted (ECC P-256) using a public key from Apple and is sent to an Apple server, which forwards the credential to the user’s phone via its own paths.

For more information, please refer to the "Mobile Wallet Access Badge TIP" document, available on the Gallagher Command Centre install media.

Copyright © Gallagher Group Limited

14.8 Mobile Client SDK

Client certificates are stored in the Mobile Device certificate store with the site facility ID. Client certificates are shared between apps with the same developer account. Therefore, two apps written with the same developer account cannot both have credentials for the same site. The later will overwrite the previous apps certificate.

This should not be a problem, but just noting it here in case it comes up. The event details will show "FIDO Result: Incorrect Signature" if this does occur. This might happen if a site using the SDK decides to scrap their current app and rewrite it and a user keeps both apps.

14.9 Diagnostics Service

The Diagnostics Service acts a broker for receiving and forwarding diagnostic telemetry provided by other applications.

It communicates with the Command Centre Service using HTTPS, secured using TLS 1.2.

The service accepts requests using HTTPS, OTLP/HTTPS and OTLP/gRPC, and connects to external observability platforms using OTLP/gRPC. The service certificate is used for server and client authentication respectively in these cases.

The Diagnostics Service validates certificates using the following criteria:

- Self-Signed - SHA-384 public key hash must match, must not be expired, must contain the Server Authentication enhanced key usage.
- CA-Signed - Same criteria as above however the certificate chain must be valid according to the Windows Certificate Store.

Gallagher Diagnostics Service Certificate

Stored in: Windows Certificate Store - Computer Account

Certificate type: ECDSA (P384) SHA384

This certificate is used for authenticating the Diagnostics Service for the purposes of receiving telemetry, forwarding telemetry, communicating with the Command Centre Service and providing a configuration interface to operators.

This certificate is created on upgrade or installation. It can be replaced with a self-signed or CA-signed certificate via the configuration interface.

15 External Communications Encryption

15.1 IP Alarm Transmission

IP Alarm Monitoring messages are transmitted using the Offsite Alarm Transmission Protocol. This protocol uses the Contact ID ANSI\SIA DC-09 message format. Encryption can be enabled or disabled. If encryption is disabled the alarm receiver will still accept encrypted messages. If encryption is enabled, outgoing message traffic will be encrypted with AES-256 and the alarm receiver will accept only encrypted messages. Default is disabled.

15.2 XML Import/Export

From Gallagher Command Centre vEL7.80 DCOM native encryption which is based on Windows accounts can be enabled. For vEL7.80 and vEL7.90 DCOM encryption is disabled by default. From Command Centre vEL8.00 onwards DCOM encryption is enabled by default.

Copyright © Gallagher Group Limited

If a password was set prior to vEL7.80, it will still be protected using MD5/RC4 which is considered obsolete cryptography. After upgrading to vEL7.80 (released Nov 2017) or later, the password must be changed to bring the storage up to current standards.

15.3 Gallagher IDEMIA Integration

The Gallagher integration with IDEMIA is supported exclusively on Native 5th Generation (MA5G) IDEMIA biometric devices.

Communications between Gallagher Command Centre and IDEMIA biometric devices are protected using encryption and certificate-based authentication. Each IDEMIA device is provisioned with a unique digital certificate and its own public and private key pair, helping to secure data transmitted across the IP network. TLS 1.3 is supported and preferred where device configuration permits.

Communications between Gallagher Controllers and IDEMIA biometric readers are secured using Secure OSDP (Open Supervised Device Protocol) over RS-485. Secure OSDP provides an encrypted and authenticated communication channel between the controller and reader, helping protect credential and control data from interception or tampering while addressing the security limitations of legacy Wiegand communications. Secure OSDP is enabled by default for supported IDEMIA MA5G devices.

15.4 Gallagher Command Centre Controller API

The Gallagher Command Centre Controller API is designed to run on a middleware machine and look after all communications, protocol, licensing, and encryption details so as to make it simple for middleware engineers to interface to the Command Centre system. Communications between Middleware/FTCAPI and the Command Centre system uses TLS 1.2 or 1.3 with the ECDHE-ECDSA-AES256-GCM-SHA384 cipher suite.

15.5 Commend Intercom

The Gallagher integration with Commend requires the use of the Commend ICX interfaces and protocol. The most secure method of communicating via this protocol involves a nonce challenge/response that utilises two bytes of an MD5-based hash.

15.6 Gallagher Salto Integration

From vEL9.20 onwards, the Gallagher Salto Integration can utilize HTTPS to communicate with the Salto SHIP API. This secures the communication between Command Centre and Salto Server with TLS. The TLS version is dependent on system configuration. Please see the Command Centre Hardening Guide for more information.

Salto Legacy Card migration is available from vEL9.30 onwards, which uses encryption to secure the migration data during transfer. This is a password-based encryption scheme, with key derivation using PBKDF2-SHA384 with 100,000 iterations, and encryption with AES-256-CBC.

15.7 Gallagher ASSA Abloy IP-Enabled Lock Integration

The Gallagher ASSA Abloy Integration communicates with ASSA Abloy Door Service Routers (DSRs) exclusively over HTTPS, using SOAP/WCF as the transport protocol. This secures all management, access control, and support communications between Command Centre and the DSR with TLS. The DSR itself runs on Apache Tomcat, and the integration includes tooling to provision TLS certificates for the DSR (either self-signed or CA-issued) using RSA 4096-bit keys stored in PKCS12 keystores. Callbacks from the DSR back to Command Centre are also delivered over HTTPS and are authenticated using a token-based scheme, where the token is a deterministic identifier derived from a SHA-256 hash of the DSR identity. Cardholder PIN codes (user codes) stored by the integration are encrypted at rest using ASP.NET Core Data Protection with a purpose-scoped key.

Copyright © Gallagher Group Limited

Communications between the DSR and connected IN120/IN220 locks are managed by ASSA Abloy components rather than by the Gallagher integration. ASSA Abloy documentation indicates that PoE and Wi-Fi locks support optional AES 128-bit encryption at the lock protocol level, in addition to any Wi-Fi network encryption; for IN120 Wi-Fi locks, supported wireless security/authentication options include WPA/WPA2 Personal with AES/TKIP and WPA/WPA2 Enterprise with 802.1X options such as PEAPv0, EAP-TLS, and EAP-TTLS. Because this encryption is configured and enforced within the ASSA Abloy DSR/LCT/lock ecosystem, deployment-specific settings should be verified against ASSA Abloy documentation and the installed lock firmware/radio generation.

16 OneLink (Cloud Controller Gateway)

OneLink utilises Gallagher Cloud services to enable controllers to connect to the on-premises Command Centre Server over the internet. Communications between Command Centre and Cloud Services take place solely using HTTPS over the standard port **443**. This is described in more detail in section ***14.5 Gallagher Cloud Services*** earlier.

16.1 Controller Registration

To allow the server discovery mechanism to determine which server URL a controller should connect to, the server URL must have been assigned to the controller during the Controller Registration process.

Like other Gallagher cloud services, communication between Command Centre server and the Controller Registration Service takes place using HTTPS over port 443. RSA-2048 TLS client certificates are used to securely and uniquely identify each individual Command Centre Server.

16.2 Server Discovery

When a Controller 7000 boots with DIP switches 2 and 7 ON, the controller will begin the server discovery process. This allows the controller to determine the server URL to connect to and the preferred authentication method to use.

It will retrieve the trusted issuer information from the HTTP host:

controller-onboarding.security.gallagher.cloud

The trusted issuer information is downloaded over unauthenticated HTTP and contains lists of trusted CA certificates, CRLs and revoked signing certificates.

The controller will authenticate the attached CMS signature of the trusted issuer information using a Gallagher Production Root certificate stored on the Controller 7000 Edgelock.

The trusted issuer list signature must be SHA384 or SHA512.

The controller will authenticate the Server Discovery TLS connection using the trusted issuer certificates and CRLs from the trusted issuer list.

16.3 Controller to Controller Gateway

The Controller Gateway application uses an ECDSA (P384) SHA256 certificate for authenticating itself during communications with C7000 controllers. This certificate is securely stored in AWS.

The controller will authenticate the Controller Gateway WebSocket TLS connection using the trusted issuer certificates and CRLs from the trusted issuer list.

The controller enforces that all certificates, CRLs and signatures must be of ECC256/SHA256/RSA3072 strength or greater.

Copyright © Gallagher Group Limited

16.4 Controller Gateway to Command Centre

Communication between the Controller Gateway and a Command Centre server is carried out via the Gallagher API Gateway. The HTTPS connection between the Controller Gateway and the Gallagher API Gateway is authenticated using private ECDSA (P384) SHA256 client TLS certificates and the WSS connection between the Gallagher API Gateway and a Command Centre instance is authenticated using RSA-2048 client TLS certificates using HTTPS/TLS 1.3 with certificate pinning.

17 Encryption Table

Gallagher Command Centre Server Communication Encryption	Key Strength	Encryption Algorithm Strength	Key Storage Location
Command Centre Server (Multi-Server) to Command Centre Server	RSA-2048	AES-256	Command Centre Database
Command Centre Client to Command Centre Server	RSA-2048	AES-256	Command Centre Database
Command Centre Configuration Client to Command Centre Server	ECC P384	AES-256	Command Centre Database
Command Centre Visitor Management Workstation to Command Centre Server	RSA-2048	AES-256	Command Centre Database
Command Centre Visitor Management Kiosk to Command Centre Server	RSA-2048	AES-256	Command Centre Database
GGL Cloud (Mobile) to Command Centre Server	Not Applicable	TLS1.3 Forward Secret ciphers only	Command Centre Database
Command Centre Mobile Client to Command Centre Server	HTTPS: RSA-2048	AES-256 (TLS1.3)	Command Centre Database
Gallagher REST API to Command Centre Server	HTTPS: RSA-2048	AES-256 (TLS1.3)	Command Centre Database
Controller to Command Centre Server	ECC P384	AES-256 (TLS1.3)	Command Centre Database

Gallagher Controller Communication Encryption	Key Strength	Encryption Algorithm Strength
Controller to Controller	ECC P-384	AES-256 (TLS1.3)
Controller to Controller API	ECC P-384	AES-256 (TLS1.2)

Gallagher Controller (HBUS) Devices Communication Encryption	Key Strength	Encryption Algorithm Strength
Controller to T-Series Reader and Alarm Terminal	ECC P-256	AES-128 (HBUS)
Controller to Door Module	ECC P-256	AES-128 (HBUS)
Controller to Wiegand Door Module	ECC P-256	AES-128 (HBUS)
Controller to HBUS I/O Devices	ECC P-256	AES-128 (HBUS)
Controller to F-Series Fence Controller	ECC P-256	AES-128 (HBUS)
Controller to Z10 Tension Sensor	ECC P-256	AES-128 (HBUS)

Gallagher High Sec Controller 6000/7000 (HBUS) Devices Communication Encryption	Key Strength	Encryption Algorithm Strength
High Sec Controller 6000/7000 to T-Series High Sec Reader	ECC P-256	AES-128 (HBUS)
High Sec Controller 6000/7000 to Class 5 ELM	ECC P-256	AES-128 (HBUS)

DESFire Encryption	Encryption Algorithm Strength	Key Storage Location
DESFire Encryption	AES-128	Command Centre Database

Copyright © Gallagher Group Limited

18 Deprecated Cryptographic Algorithm usage

18.1 SHA-1

- SHA-1 is required as a part of the upgrade process when upgrading a pre 8.20 WindowsCE Controller 6000 to a later, Linux based version.
- SHA-1 is used to obfuscate calls from the FTCPAI into the licensing DLL.
- Command Centre uses SHA-1 to store already validated certificates in a hash table during a PIV certificate validation cycle to avoid unnecessary work.
- SHA-1 is used to hash the public key in X.509 certificates to form the unique Subject Key Identifier and is used by Command Centre during PIV certificate validation to differentiate certificates with the same name but different public keys. This is a non-cryptographic use of SHA-1.
- Command Centre makes use of SHA-1 as per RFC 4122 when creating UUIDs for COM references. This is a non-cryptographic use of SHA-1.
- SHA-1 is used as per RFC 6455 as part of the websockets protocol. This is not used for security purposes.

18.2 MD5

- MD5 may be used when reading older Mifare key export files.
- MD5 is used in license file validation.
- MD5 is used in a licensing context for some additional resources such as language translations.
- MD5 is used in the Security Health Check when performing some password checks on operator accounts whose passwords were set in older versions of Command Centre and have not been updated.

18.3 RC4

- RC4 may be used to validate passwords set in earlier versions of Command Centre. Once a password has been changed it will no longer be used.
- RC4 is used to decrypt factory keys loaded from the license file. These are used for confirming hardware authenticity.

18.4 DES/3DES

DES/3DES can be used for various legacy card types.

Copyright © Gallagher Group Limited

19 Legacy Command Centre Encryption

These methods and protocols have been superseded as the underlying cryptography has become weak by modern standards. They are not recommended to be used in current security infrastructure and are only here for historical reference.

Communication between the Command Centre Server and 3000/5000GL Controllers use TLS1.0. The 3000 and 5000 legacy controllers are unable to use newer protocols and higher levels of encryption.

Gallagher Command Centre V7.80 and before - Configuration Client used the Distributed Component Object Model (DCOM) for communication between the client and server. However, DCOM by default is not encrypted.

Gallagher Local Bus

Currently supported for backwards and third-party compatibility:

- RS485 GBUS protocol
- RS485 Local Bus protocol
- Weigand protocol
- 125kHz Card Technologies
- MIFARE® Classic Card Technologies

Copyright © Gallagher Group Limited

20 Glossary

- **AES** (Advanced Encryption Standard) is an algorithm used in symmetric key cryptography. The cipher has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Due to the fixed block size of 128 bits, AES operates on a 4×4 array of bytes.
- **CBC** (Cipher Blocker Chaining) is a mode of operation for a block cipher, where one sequence of bits is encrypted as a single unit or block with a cipher key applied to the entire block.
- **DH** (Diffie-Hellman) is an algorithm used to establish a shared secret between two parties. It is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES.
- **DPAPI** (Data Protection Application Programming Interface) is a simple cryptographic application programming interface available as a built-in component of Microsoft Windows operating systems.
- **ECC** (Elliptic-Curve Cryptography). The primary benefit promised by elliptic curve cryptography is a smaller key size, reducing storage and transmission requirements.
- **FIDO** (Fast IDentity Online) 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, and Visa.
- **FIPS 201** (Federal Information Processing Standard Publication 201) is a United States federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.
- **HTTPS** (Hypertext Transfer Protocol Secure) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection.
- **IV** (Initialization Vector) is an arbitrary number that can be used along with a secret key for data encryption. The IV length is usually comparable to the length of the encryption key or block of the cipher in use.
- **NIST** (National Institute of Standards and Technology) is a non-regulatory federal agency under the Department of Commerce. NIST is the United States National Measurement Institute.
- **OPC UA** (OPC Unified Architecture) is a machine-to-machine communication protocol for industrial automation developed by the OPC Foundation and focuses on communicating with industrial equipment and systems for data collection and control. OPC UA binary protocol is a TCP-based binary protocol and a common transport layer where general concepts translate to HTTP and SOAP-based communication.
- **PBKDF2** (Password-Based Key Derivation Function 2) are key derivation functions with a sliding computational cost, aimed to reduce the vulnerability of encrypted keys to brute force attacks. PBKDF2 is part of RSA Laboratories' Public-Key Cryptography Standards.
- **REST** (Representational State Transfer) is an architectural style and approach to communications and is often used in web services development.
- **RSA** (Rivest–Shamir–Adleman) is a relatively slow asymmetric algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.
- **SHA-1** (Secure Hash Algorithm 1) is a cryptographic hash function that when applied to the provided input results in a 40-digit hexadecimal number.
- **SHA-256** (Secure Hash Algorithm 256) is a cryptographic hash function that when applied to the provided input results in a 64-digit hexadecimal number.

Copyright © Gallagher Group Limited

- **SHA-512** (Secure Hash Algorithm 512) is a cryptographic hash function that when applied to the provided input results in a 128-digit hexadecimal number.
- **SOAP** (Simple Object Access Protocol) is a messaging protocol specification for exchanging structured information in the implementation of web services.
- **SSL/TLS** uses asymmetric encryption for client and server to verify the identity (certificate) of the remote host, the encryption key is derived from a securely negotiate a shared session key that is used to encrypt application data. E.g. RSA, DSA, Elliptic Curve. SSL/TLS also uses symmetric encryption for transmitting and receiving application data. e.g. AES, 3DES, RC4.
- **TIP** (Technical Information Paper) are technical publications by Gallagher Group to inform Channel Partners and customers of the operation and underlying architecture of Command Centre and associated products.
- **TLS** (Transport Layer Security) is a successor to Secure Sockets Layer protocol. TLS provides secure communications between server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.
- **UAF** (Universal Authentication Framework) 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.
- **WS-Security** (Web Services Security) The WS-Security Policy is a web services specification, that extends the fundamental security protocols specified by WS-Security, WS-Trust, and WS-SecureConversation by offering mechanisms to represent the capabilities and requirements of web services as policies.

21 References

21.1 Internal references

- Gallagher Command Centre Hardening Guide
- Command Centre Mobile App Security TIP
- Mobile Connect Cloud and App Security TIP

21.2 External references

Microsoft SQL document repositories

https://technet.microsoft.com/pt-pt/library/cc772815(v=ws.10).aspx

https://en.wikipedia.org

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/sql-server-encryption?view=sql-server-2017

Copyright © Gallagher Group Limited