Gallagher | Allegion

Schlage® AD Series Locks – FIPS 201-2 integration ready networked electronic locks

The Gallagher and Allegion integration offers secure, seamlessly integrated electronic access control through hardwired and wireless electronic locks within the Gallagher system. Access is managed seamlessly regardless of the combination of Schlage® and Gallagher wired or wireless doors across a multi-building or multi-region distributed system.

AD Series electronic locks from Schlage® are designed with flexibility in mind. Its patented modular design allows the lock to be customized to fit the needs of an application now and changed to meet future needs without removing it from the door.

To simplify installation, the AD Series combines all the hardware components required at the door for a complete access control system into one integrated design that includes the electrified lock, credential reader, request-to-exit and request-to-enter sensors, door position switch, tamper switch, and more.

Factory orderable options include choices of credential technology, chassis type, network configurations, locking functions, lever styles, and finishes. It also offers a wide selection of features that can be configured in the field to customize your openings.

This product is currently available in North America only.

Integration benefits

- Exchange information in real-time between Gallagher Controller 6000 and lock
- Manage and update multiple doors centrally. without having to manually update each door
- Utilize both wired and wireless lock options for a variety of door types
- Meet changing organizational needs, both now and in the future, without needing to remove lock hardware

Integration features

- PIV, PIV-I, TWIC, and CAC compatible
- MIFARE® Classic, MIFARE® DESFire EV1/EV2, HID iClass, HID SE iClass, and 125KHz credentials
- Communication to Controller 6000 via up to two RS485 ports with the option of a proprietary 900MHz wireless comms
- Locks combine electrified lock, credential reader, request-to-exit and request-to-enter sensors, door position switch, and tamper switch
- 'Wake Up On Radio' (WOR) allowing devices to be 'woken up' remotely by the Command Centre server to allow critical mode changes e.g. lock-down
- Standard and keypad versions available

How the solution works

Integrated into Gallagher's PIV registration, validation, and authentication architecture up to 8 AD-302 wired and up to 16 AD-402 wireless PIV readers can be managed by one Gallagher 6000 HS PIV controller. In addition, the Allegion wireless communication between the AD-402 reader and the PIM400 are secured and encrypted with NIST approved encryption standards.

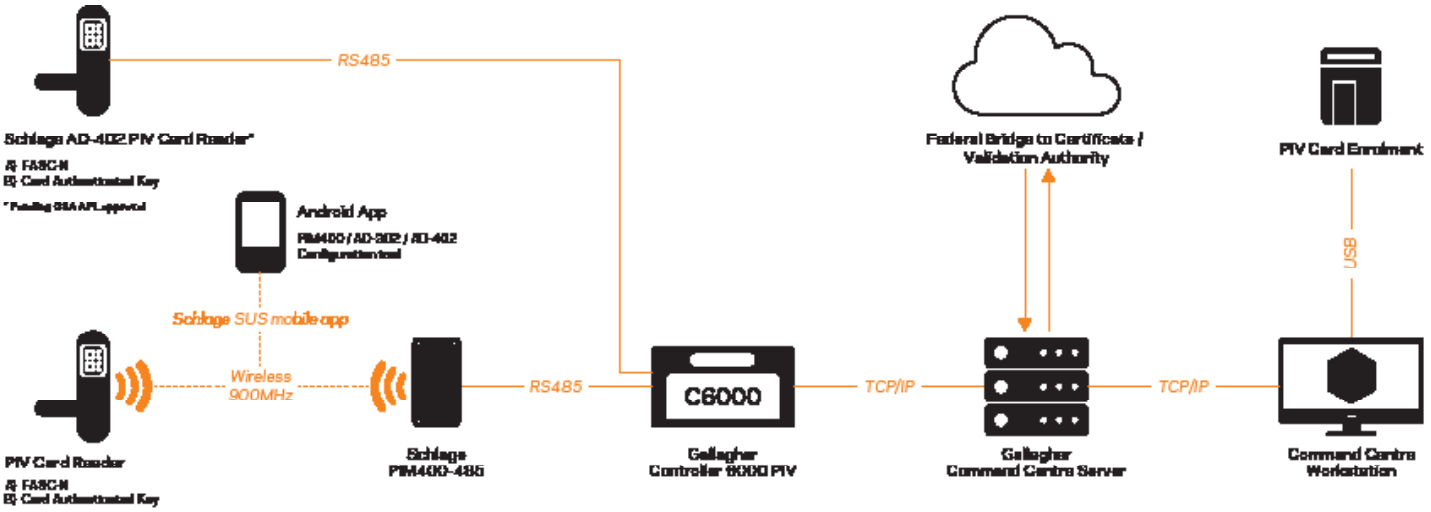
The authentication mode for PIV and PIV-I cards is configured on the AD-302 and AD-402 readers. The available authentication mode options are either "Low Security (Non FIPS201)" or High Security (FIPS201)".
FASC-N / UUID only (Non FIPS201)
CAK Authentication (FIPS201)

The readers may be configured for a low security read of the PIV and PIV-I cards for maximum access speed, however this mode does not meet FIPS 201-2 compliance requirements. In this mode only the FASC-N / UUID is transmitted from the reader to the controller which will grant access if the card has privileges.

For a fully FIPS 201-2 Approved Products List (APL) solution the system can authenticate the PIV Card Authentication Key (CAK). When a PIV card is presented, the unique identifier (FASC-N / UUID) is read by the reader and transmitted to the Gallagher 6000 HS PIV controller. The controller will send a "Challenge" (an array of bytes with randomly generated data) to the reader that then passes it to the card for signing with the private key of the CAK, the result is then returned to the Gallagher 6000 HS PIV controller where the cryptographic challenge is validated using the public key stored in the controller database.

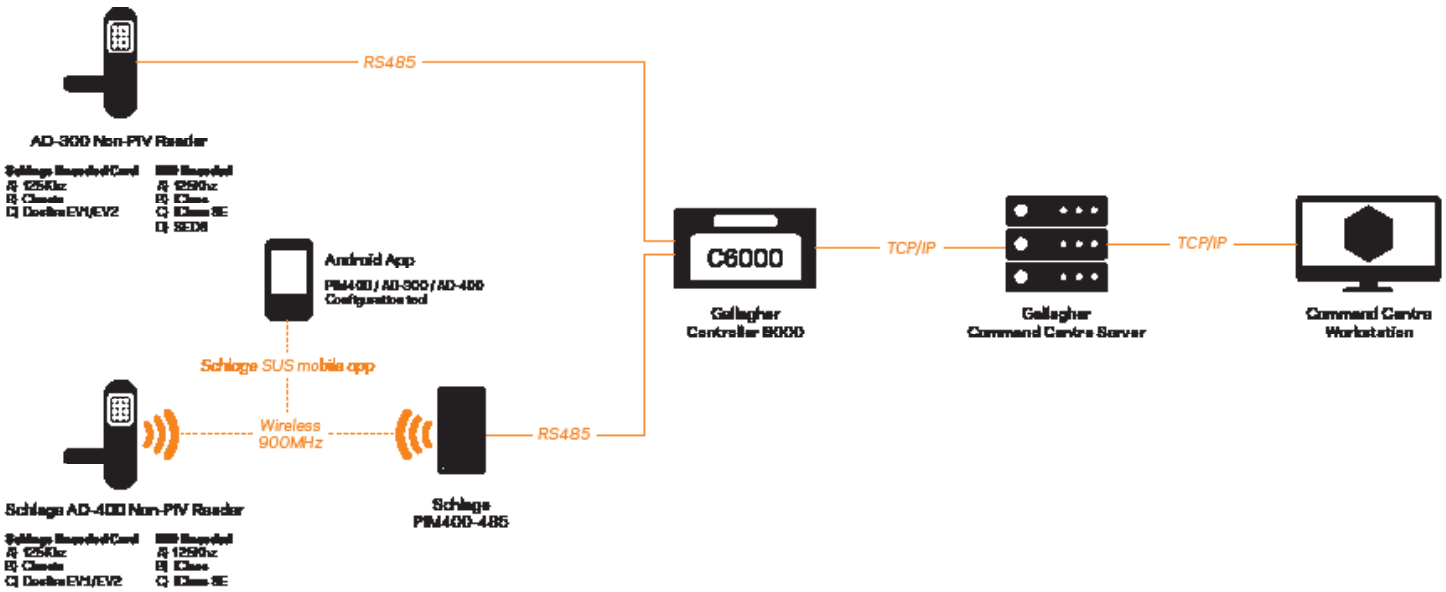
The person is granted access if the card has privileges. The card's expiry date is checked in both authenticated modes. When a PIV or PIV-I card is presented the FASC-N (PIV) or UUID (PIV-I) is transmitted from the reader to the Controller. The expiry date and CAK certificate are already known by the controller as they are captured by Command Centre during enrollment.

PIV



When using one of the non-PIV card technologies, the connections of the Schlage® AD-300 and AD-400 series readers is unchanged from the PIV solution described above. When one of the support credential technologies is presented to the reader, the unique identifier is sent from the reader to the Controller 6000 which will look up the persons privileges in the onboard database and grant access by telling the reader to release the door.

Non-PIV



Technical specifications

	AD-300	AD-302	AD-400	AD-402
Modulation	900 MHz spread spectrum, direct sequence, 10 channels			
Frequency range	902-928 MHz			
Transmission / encryption	AES-128 bit key			
Credential verification time	< 1 second*	< 2 seconds in FASC-N mode; card certificate validated by the Controller 6000 only 2-4 seconds in full authentication mode.	< 1 second*	< 2 seconds in FASC-N mode; card certificate validated by the Controller 6000 only 2-6 seconds in full authentication mode.
Wake-Up on Radio	Responds to lock/unlock command from host in less than 10 seconds in battery powered applications (per field configuration)			
Communication range	Up to 200 ft with obstructions (normal building construction), up to 1000 ft clear line of sight			
RF interference avoidance	Configurable dynamic channel switching			
Data rate	RS-485 : 9.6 kbps		RF: 40 kbps	
Visual / audible communications	Tri-colored LED's and audible indicators			
System interface	RS-485 directly	RS-485 directly	RS-485 via PIM400 to host	RS-485 via PIM400 to host
Power supply	12 VDC or 24 VDC		4AA, 8AA, 12 VDC or 24 VDC	
Voltage range	4 VDC to 26 VDC			
Max current requirement	Up to 250 mA			
Battery life			Up to 2 yrs with 4AA	FASC-N mode: 18-24 months (4AA) Full authentication mode: 10-12 months (4AA
Cable specifications for power	18AWG, 2 conductor (Belden 8760 or equivalent)			
Cable distance for power	AD-300 to power supply: up to 1000 ft (303 m)	AD-302 to power supply: up to 1000 ft (303 m)		
Cable specifications for data	24AWG, 2 or 4 conductor shielded (Belden 9841, 9842 or equivalent)			
Cabling distance for data	RS-485: up to 4000 ft (1219 m)	RS-485: up to 4000 ft (1219 m)		
Operating temperature	-31° to 151°F (-35° to 66°C)		Exterior = -31° to 151°F (-35° to 66°C) Interior = 32° to 120°F (0° to 49°C) (battery)	
Operating humidity	0 - 100% non-condensing			
Certifications	ANSI/BHMA A156.25, ANSI/BHMA Grade 1, UL 294, UL10 C, FCC Part 15, ADA, RoHS			
Accessories	Schlage Utility Software (SUS) Mobile App (Android only), SUS-A cable		Panel Interface Module (PIM400), SUS-A cable, remote antennas for PIM400 to extend range, Schlage Utility Software (SUS) Mobile App (Android only), Dry Contact Relay Board (RLBD) may be required for supervised inputs (Wiegand systems)	Panel Interface Module (PIM400) and SUS-A cable
Supported credential technologies	MIFARE Classic, MIFARE DESFire, HID iClass, HID SE iClass, and 125KHz	PIV (FIPS 201-2), TWIC/CAC, MIFARE Classic, MIFARE DESFire, HID iClass, HID SE iClass, HID SEOS, and 125KHz	MIFARE Classic, MIFARE DESFire, HID iClass, HID SE iClass, and 125KHz	PIV (FIPS 201-2), TWIC/CAC, MIFARE Classic, MIFARE DESFire, HID iClass, HID SE iClass, and 125KHz

*Lock requires less than 100 msec, response time does not include latency time of ACP.

Device allocations

The Schlage® Lock Interface allows one Gallagher Controller 6000 to manage the below allocations:

- A maximum of 8 Schlage® PIM's (Panel Interface Modules) per Controller 6000 and up to 16 Schlage® AD-40X locks.
- A maximum of 8 Schlage® AD-30X locks per Controller 6000 (each AD-30X lock has a virtual PIM).

The devices will consume allocations as per the table below:

AD-300	AD-302	PIM400	AD-400	AD-402
1 x Controller 6000 Lock allocation (Includes Virtual PIM) *Max 8 per Controller*	1 x Controller 6000 Lock allocation (Includes Virtual PIM) *Max 8 per Controller*	1 x Controller 6000 PIM allocation *Max 8 per Controller*	Lock allocation is to PIM400 (Max 16 AD-400's per PIM) *Max 16 per Controller*	Lock allocation is to PIM400 (Max 16 AD-402's per PIM) *Max 16 per Controller*

The AD-40x locks are connected to a PIM400, which will connect to the Controller 6000. A single PIM400 can have up to 16 Schlage® AD-40x devices connected to it.

In Command Centre, a Schlage® PIM400 is attached to one of the two RS-485 buses on the Controller 6000, and a Schlage® AD-40X Lock is assigned to a Schlage® PIM400. The Schlage® AD-30x is attached directly to one of the two RS-485 busses on the Controller 6000.

Physically, a Schlage® PIM400 is wired to one of the two RS-485 ports on a Controller 6000. If more than two PM400s need to be connected, they can be wired together into the RS-485 bus, or an extension board can be used. A Schlage® AD-40x lock talks to a Schlage® PIM400 via 900 MHz wireless communication. The Schlage® AD-30x lock is wired directly into one of the two RS-485 buses. They can also be wired together, or an extension board used, if more than two Schlage® AD-30x devices need to be connected to a single controller.

If the site wishes to use both Gallagher and the Schlage® AD series of locks, an HBUS can be connected to a free RS-485 bus.

Note: If the site is using the PIV functionality available in the Schlage® AD-302 and AD-402 locks, a Gallagher PIV Controller 6000 is required.

Supported Products

A wide range of Schlage®AD series products can be deployed easily with the Gallagher solution. A selection of supported products are displayed below. For more detail on Schlage®AD series products, please contact your nearest Gallagher representative.

AD-400 - Networked wireless electronic lock

AD-402 - FIPS 201-2* integration ready networked wireless electronic lock

pending GSA APL approval

AD-302 - FIPS 201-2 integration ready networked hardwired electronic lock

AD-300 - Networked hardwired electronic lock

Gallagher World Headquarters
181 Kahikatea Drive, Melville, Hamilton 3204
New Zealand

Phone +64 7 838 9800
Email security@gallagher.com

Regional Offices

Americas	+1 877 560 6308
Asia	+852 3468 5175
Australia	+61 3 9308 7722
India	+91 98 458 92920
Middle East	+971 4 566 5834
South Africa	+27 11 974 4740
United Kingdom / Europe	+44 2476 64 1234

3E5482 - 10/21